Extraordinary SANS certified instructors

200+
Training events globally, plus multiple online options

See inside for
SANS training events across Europe and Middle East

SANS training curriculum
About SANS

SANS is the world’s largest and most trusted provider of cyber security training. Founded in 1989, SANS operates globally and has over 200,000 alumni.

For over twenty-five years, we have worked with many of the world’s more prominent companies, military organisations, and governments.

Technology may have changed in that time, but our core mission has remained constant: to protect people and assets through sharing cutting-edge cyber-security skills and knowledge.

Strength from people
SANS Instructors are, first and foremost, industry professionals with a wealth of real-world experience – experience that they bring into the classroom.

Across our roster of instructors are many active security practitioners who work for high profile organisations. The list includes red team leaders, information warfare officers, technical directors, CISOs, and research fellows.

Along with respected technical credentials, SANS Instructors are also expert teachers. Their passion for their subject shines through, making the SANS classroom efficient and effective.

Cutting edge training
Cybercrime evolves constantly. SANS prepares students to meet today’s dominant threats and tomorrow’s challenges.

We do this through constantly updating and rewriting our courses and support material. This process is steered by an expert panel that draws on the global community’s consensus regarding best practice.

Focussed training
SANS training is job and skill-specific. We offer more than 60 courses, designed to align with dominant security team roles, duties, and disciplines.

The SANS Curriculum spans Digital Forensics, Audit, Management, Pen Testing, ICS, Secure Software Development and more (see pages 14-19). Each curriculum offers a progression of courses that can take practitioners from a subject’s foundations right up to specialist skills and knowledge.

Our training is designed to be practical; students are immersed in hands-on lab exercises built to let them rehearse, hone and perfect what they’ve learned.

The SANS Promise
At the heart of everything we do is the SANS Promise: Students will be able to deploy the new skills they’ve learned immediately.

The global community
SANS Institute is a prominent member of the global cyber security community. We operate the Internet Storm Centre – the internet’s early warning system.

SANS also develops, maintains, and publishes a large collection of research papers about many aspects of information security. These papers are made available for free.

The GIAC Advantage
GIAC validates the skills of information security professionals, proving that those certified have the technical knowledge necessary to work in key areas of cyber security.

GIAC certifications are respected globally because they measure specific skill and knowledge areas. GIAC offers the only cyber security certifications that cover advanced technical subject areas.

There are over 30 specialised GIAC certifications. Several GIAC certifications are accepted under the ANSI/ISO/IEC 17024 Personnel Certification program.

Many SANS training courses align with GIAC certifications. As such, SANS Training is an ideal preparation for a GIAC certification attempt.

Why SANS is the best training and educational investment
SANS’ immersion training is intensive and hands-on and our courseware is unrivalled in the industry.

SANS Instructors and course authors are leading industry experts and practitioners. Their real-world experience informs their teaching and SANS’ training content.

SANS training strengthens a student’s ability to achieve a GIAC certification, with both SANS and GIAC placing an emphasis on learning practical skills.

How to register for SANS training
SANS runs public training events globally, including multiple events across Europe and the Middle East, offering students the opportunity to take a SANS course across an intensive 5 or 6 days.

SANS training events provide the perfect learning environment and offer the chance to network with other security professionals, as well as SANS Instructors and staff.

Students should register online by visiting www.sans.org/emea.

SANS Training can also be delivered online through our OnDemand product, as a private class within an organisation, and through other mediums, including classroom training in French, German, Italian and Spanish. See page 6 for details of all our training delivery options or visit www.sans.org/emea.

Contact SANS
Email: emea@sans.org
Tel: +44 20 3384 3470
Address: SANS EMEA, PO Box 124, Swansea, SA3 9BB, UK
www.sans.org
### Contents

#### SANS Cyber Defence Courses
- SEC301 Intro to Information Security ........................................... 20
- SEC401 Security Essentials Bootcamp Style .................................. 21
- SEC487 Open-Source Intelligence Gathering (OSINT) and Analysis .......... 22
- SEC503 Intrusion Detection In-Depth ............................................. 24
- SEC505 Securing Windows and PowerShell Automation ....................... 25
- SEC506 Securing Linux/Unix .................................................. 26
- SEC511 Continuous Monitoring and Security Operations .................... 27
- SEC530 Defensible Security Architecture .................................... 28
- SEC545 Cloud Security Architecture and Operations ....................... 29
- SEC555 SIEM with Tactical Analytics ....................................... 30
- SEC579 Virtualization and Software Defined Security ...................... 31
- SEC599 Defeating Advanced Adversaries - Implementing Kill Chain Defenses 32

#### SANS Penetration Testing & Vulnerability Courses
- SEC460 Enterprise Threat and Vulnerability Assessment .................. 34
- SEC504 Hacker Tools, Techniques, Exploit ................................... 35
- SEC542 Web App Penetration Testing and Ethical Hacking .................. 36
- SEC560 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking 38
- SEC561 Immersive Hands-on Hacking Techniques .......................... 39
- SEC573 Automating Information Security for Python ....................... 40
- SEC575 Mobile Device Security and Ethical Hacking ...................... 41
- SEC617 Wireless Ethical Hacking, Penetration Testing, and Defenses ...... 42
- SEC642 Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Tech. 43
- SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking 44
- SEC760 Advanced Exploit Development for Penetration Testers ........... 45

#### SANS Forensics and Incident Response Courses
- FOR500 Windows Forensic Analysis .......................................... 46
- FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting 47
- FOR518 Mac Forensic Analysis ................................................ 48
- FOR526 Memory Forensics In-Depth ......................................... 49
- FOR572 Advanced Network Forensics and Analysis .......................... 50
- FOR578 Cyber Threat Intelligence ........................................... 51
- FOR585 Advanced Smartphone Forensics .................................... 52
- FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques 53

#### SANS Management and Audit Courses
- SEC566 Implementing and Auditing the Critical Security Controls In-Depth 54
- MGT414 SANS Training Program for CISSP® Certification ................ 55
- MGT433 Securing The Human: How to build, maintain, and measure a high-impact awareness programme .................................. 56
- MGT512 SANS Security Leadership Essentials For Managers with Knowledge CompressionTM .................................................. 58
- MGT514 IT Security Strategic Planning, Policy, and Leadership .......... 59
- MGT517 IT Project Management, Effective Communication, and PMP® Exam Prep 60
- MGT525 IT Project Management, Effective Communication, and PMP® Exam Prep 61
- AUD507 Auditing & Monitoring Networks, Perimeters, and Systems .... 62
- LEG523 Law of Data Security and Investigations ............................ 63

#### SANS Secure Software Development Courses
- DEV522 Defending Web Applications Security Essentials ................ 64
- DEV541 Secure Coding in Java/JEE: Developing Defensible Application 65
- DEV544 Secure Coding in .NET: Developing Defensible Applications .... 66

#### SANS Industrial Control Systems Courses
- ICS410 ICS/SCADA Security Essentials .................................... 67
- ICS456 Essentials for NERC Critical Infrastructure Protection .......... 68
- ICS515 ICS Active Defense and Incident Response ........................ 69

---

**About SANS** ........................................... 2
**Contents** ........................................... 3
**Training Roadmap** .................................. 4
**Training Formats** .................................... 6
**Securing Budget Approval** ................................ 8
**Build a High-Performing Security Organization** ....................... 9
**GIAC** ........................................... 10
**SANS Summits** ....................................... 11
**Partnerships & Solutions** .................................. 12
**SANS Curricula** ....................................... 14
**Course Descriptions** ................................... 20
**NetWars** ........................................... 33
**Security Awareness Training** .................................... 57
**The SANS Portal Account** .................................. 71
**Upcoming SANS Events** ................................... 72

---

**For course descriptions**

Are you taking your first course or career move? Turn to page 4 for our Career Roadmap and see where SANS training could take you.

---

**Are you taking your first SANS training course?** Turn to page 14 for our curriculum guides and page 20 onwards for course descriptions.
New to cyber security?

SEC 301
Intro to Information Security
GSF Certification - Information Security Fundamentals

You are experienced in technology, but need to learn hands-on, essential security skills and techniques

Core Security Techniques
Defend & Maintain

The defence-in-depth techniques taught in SEC401 are essential for every security professional. SEC504 provides additional “offence informs defence” knowledge, teaching defence specialists how attacks occur and how to respond. Students with existing core defence skills could begin their training journey with SEC504.

SEC 401
Security Essentials Bootcamp Style
GSF - Security Essentials

SEC 504
Hacker Tools, Techniques, Exploits, and Incident Handling
GOH - Certified Incident Handler

You will be responsible for managing security teams or implementations, but do not require hands-on skills

Security Management

MGT 433
Securing The Human: How to Build, Maintain & Measure a High-Impact Awareness Program
Security Leadership

MGT 512
SANS Security Leadership Essentials For Managers (with Knowledge Compression™)
GSF - Security Leadership

SEC 566
Implementing and Auditing the Critical Security Controls - In-Depth
GCCC - Critical Security Controls

You are experienced in security, preparing for a specialised job role or focus

Security Monitoring & Detection

SEC 503
Intrusion Detection In-depth
GCI - Certified Intrusion Analyst

SEC 511
Continuous Monitoring and Security Operations
GMON - Continuation Monitoring

Penetration Testing and Vulnerability Analysis

SEC 560
Network Penetration Testing and Ethical Hacking
OPEN - Penetration Tester

SEC 542
Web App Penetration Testing and Ethical Hacking
GWAPT - Web Application Penetration Tester

SEC 460
Enterprise Threat and Vulnerability Assessment

Incident Response and Enterprise Forensics

FOR 508
Advanced Digital Forensics, Incident Response, and Threat Hunting
GCFA - Forensic Analyst

FOR 572
Advanced Network Forensics and Analysis
GNFA - Network Forensic Analyst
You are a candidate for specialised or advanced training

SANS’ comprehensive curriculum enables professionals to deepen their technical skills in key practice areas. It also directly addresses software developers, industrial control engineers, and non-technical personnel in management, legal, and audit.

<table>
<thead>
<tr>
<th>Cyber Defence Operations</th>
<th>Industrial Control Systems Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SEC487</strong> Open-Source Intelligence Gathering (OSINT) and Analysis</td>
<td><strong>ICS410</strong> ICS/SCADA Security Essentials - GICSP</td>
</tr>
<tr>
<td><strong>SEC555</strong> SIEM with Tactical Analytics - GCAD</td>
<td><strong>ICS456</strong> Essentials for NERC Critical Infrastructure Protection - GICSP</td>
</tr>
<tr>
<td><strong>SEC501</strong> Advanced Security Essentials Enterprise Defender - GCED</td>
<td><strong>ICS515</strong> ICS Active Defence and Incident Response - GRID</td>
</tr>
<tr>
<td><strong>SEC530</strong> Defensible Security Architecture</td>
<td></td>
</tr>
<tr>
<td><strong>SEC545</strong> Cloud Security Architecture and Operations</td>
<td></td>
</tr>
<tr>
<td><strong>SEC505</strong> Securing Windows and PowerShell Automation - GCWN</td>
<td></td>
</tr>
<tr>
<td><strong>SEC506</strong> Securing Linux/Unix - GCUX</td>
<td></td>
</tr>
<tr>
<td><strong>SEC566</strong> Implementing and Auditing the Critical Security Controls - In-Depth - GICC</td>
<td></td>
</tr>
<tr>
<td><strong>SEC579</strong> Virtualization and Private Cloud Security</td>
<td></td>
</tr>
<tr>
<td><strong>SEC599</strong> Defeating Advanced Adversaries - Implementing Kill Chain Defences</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Penetration Testing and Ethical Hacking</th>
<th>Software Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SEC561</strong> Immersive Hands-On Hacking Techniques</td>
<td><strong>DEV522</strong> Defending Web Applications Security Essentials - GWED</td>
</tr>
<tr>
<td><strong>SEC573</strong> Python for Penetration Testers - GPMC</td>
<td><strong>DEV540</strong> Secure DevOps and Cloud Application Security</td>
</tr>
<tr>
<td><strong>SEC575</strong> Mobile Device Security and Ethical Hacking - GWDG</td>
<td><strong>DEV541</strong> Secure Coding in Java/JEE: Developing Defensible Applications - GSSP-JAVA</td>
</tr>
<tr>
<td><strong>SEC617</strong> Wireless Ethical Hacking, Penetration Testing, and Defences - GAWN</td>
<td><strong>DEV544</strong> Secure Coding in .NET: Developing Defensible Applications - GSSP.NET</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Digital Forensics &amp; Incident Response</th>
<th>Audit / Legal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FOR500</strong> Windows Forensic Analysis - GCFE</td>
<td><strong>AUD507</strong> Auditing &amp; Monitoring Networks, Perimeters &amp; Systems - GSNA</td>
</tr>
<tr>
<td><strong>FOR518</strong> Mac Forensic Analysis</td>
<td><strong>SEC566</strong> Implementing and Auditing the Critical Security Controls - In-Depth - GICC</td>
</tr>
<tr>
<td><strong>FOR526</strong> Memory Forensics In-Depth</td>
<td><strong>LEG523</strong> Law of Data Security &amp; Investigations - GLEG</td>
</tr>
<tr>
<td><strong>FOR578</strong> Cyber Threat Intelligence - GCTI</td>
<td></td>
</tr>
<tr>
<td><strong>FOR585</strong> Advanced Smartphone Forensics - GASF</td>
<td></td>
</tr>
<tr>
<td><strong>FOR610</strong> Reverse-Engineering Malware: Malware Analysis Tools and Techniques - GREM</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Management</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MG514</strong> IT Security Strategic Planning, Policy and Leadership - GSTRT</td>
<td></td>
</tr>
<tr>
<td><strong>MG525</strong> IT Project Management, Effective Communication, &amp; PMP® Exam Prep - GCPM</td>
<td></td>
</tr>
<tr>
<td><strong>MG517</strong> Managing Security Operations: Detection, Response, and Intelligence</td>
<td></td>
</tr>
</tbody>
</table>
SANS Training Formats

Established in 1989, SANS is the world’s largest and most trusted source of cyber security training

**SANS Training Events**

Instruction in a classroom setting from a qualified SANS Instructor. These are multi-course events located centrally in major cities and hosted at quality hotels or event centres with excellent facilities.

Training Events are a popular method for taking SANS training as they provide an opportunity to learn, network, and socialise with peers, colleagues, and SANS staff.

Training fees also include break refreshments, lunch, and evening functions (where advertised), but not accommodation.

2018 EMEA region Training Events take place across Europe and the Gulf Region. Courses at Training Events are led in English, French, German, Italian and Spanish.

See the back cover of this brochure or www.sans.org/emea for the latest schedule.

**SANS Summits**

Summits are one- or two-day events that take the form of keynote speeches and panel sessions, led by respected thought-leaders and industry practitioners.

A SANS Summit is an invaluable source of targeted learning and typically takes place before or after a SANS Training Event with attendance available at a discounted rate for those attending training.

**SANS Security Awareness Training**

SANS Security Awareness provides computer-based security awareness training for end users, ICS engineers, developers, and the utilities and healthcare industries. Modular videos deliver expert and impactful training to large numbers of employees, with measurable results. SANS training goes beyond compliance and focuses on changing behaviour.

[www.sans.org/security-awareness-training](http://www.sans.org/security-awareness-training)
SANS On-Demand

SANS courses available anytime via E-learning. Includes course books, CD/DVDs / Toolkits, as applicable, and four months of online access to SANS’ OnDemand e-learning platform. For students who wish to study on their own at their own pace.

www.sans.org/ondemand

SANS Private Training

Training delivered directly to an organisation’s security team in a classroom setting at the employer’s premises or training facility. Private training is suitable for organisations that need to train 25 or more staff and/or require an entirely confidential training experience. Private training allows a SANS Instructor to concentrate on areas directly relevant to that organisation and provides financial advantages across staff travel, subsistence, and accommodation.

Contact SANS for further information:
emea@sans.org

Bespoke Training Solutions and Cyber Academy

SANS creates bespoke training programmes that answer specific operational and organisational needs. Training content is drawn from across SANS’ Curriculum, and programmes often include assessment phases using SANS CyberTalent.

SANS Cyber Academy identifies candidates with the potential to succeed, then provides intensive training before deploying them as GIAC Certified professionals.

To find out more about SANS partnerships email emea@sans.org

SANS Residency

A tailored programme of training for organisations that may require several courses to be run in succession, in order to quickly train large existing teams and/or new recruits.

Contact SANS for further information:
emea@sans.org
Securing Approval and Budget for Training

**Packaging matters**

**Write a formal request**

- All organizations are different, but because training requires a significant investment of both time and money, most successful training requests are made via a written document (short memo and/or a few Powerpoint slides) that justifies the need and benefit. Most managers will respect and value the effort.
- Provide all the necessary information in one place. In addition to your request, provide all the right context by including the summary pages on Why SANS?, the Training Roadmap, the instructor bio, and additional benefits available at our live events or online.

**Clearly state the benefits**

**Be specific**

- How does the course relate to the job you need to be doing? Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context for the decision.
- Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled “You Will Be Able To.” Be sure to include this in your request so that you make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

**Set the context**

**Establish longer-term expectations**

- Information security is a specialized career path within IT with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense—not a once-and-done item.
- Take a GIAC Certification exam to prove the training worked. Employers value the validation of skills and knowledge that a GIAC Certification provides. Exams are psychometrically designed to establish competency for related job tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expenses into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.
Build a High-Performing Security Organization

Every professional entrusted with hands-on work should be trained to possess a common set of capabilities enabling them to secure systems, practice defense-in-depth, understand how attackers work, and manage incidents when they occur. Set a high bar for the baseline set of skills in your security organization.

Four job roles typically emerge as organizations grow in size, risk, and/or complexity:

• **Security Monitoring & Detection Professionals** – The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Vendor training all too often teaches to the tool, and not how or why the tool works, or how it can be best deployed. Identifying security anomalies requires increased depth of understanding to deploy detection and monitoring tools and interpret their output.

• **Pen Testers & Vulnerability Analysts** – The professional who can find weaknesses is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires a different way of thinking and different tools, but is essential for defense specialists to improve defenses.

• **Forensic Investigators & Incident Responders** – Whether you’re seeking to maintain a trail of evidence on host or network systems, or hunting for threats using similar techniques, larger organizations need specialized professionals who can move beyond first-response incident handling in order to analyze an attack and develop an appropriate remediation and recovery plan.

• **Security Managers** – With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. Those managers will not necessarily perform hands-on work, but they must know enough about the underlying technologies and frameworks to help set strategy, develop appropriate policies, interact with skilled practitioners, and measure outcomes.

Within (or beyond) these four areas, high-performing security organizations will develop individual professionals to either utilize advanced skills generally, or to meet specialized needs. Along the entire spectrum, from Active Defense to Cloud Defense to Python for Pen Testers to Malware Reverse Engineering, SANS offers more than 30 courses for specialized roles or more advanced topics, meeting the needs of nearly all security professionals at every level.

**People & Skills = f (Size of Organization, Value at Risk)**

![Advanced Skills & Specialized Roles, including:](image)

- **Blue Team Operations**
- **Threat Hunting**
- **ICS-SCADA**
- **Secure Development**
- **Active Defense**
- **Mobile**
- **Malware Reverse Engineering**
- **Legal & Audit**

**Professionals with Baseline Defensive Security Capabilities**

**Vulnerability Analysis & Pen Testing**

**Incident Response & Forensic Investigations**

**Monitoring & Detection**

**Security Managers**

Practical strategies for building an information security group, based on our research and observations globally:

- **Use practical organizing principles** to design your plan and efforts. Nearly all of the more complex frameworks may be reduced to a few simpler constructs, such as “Build and Maintain Defenses – Monitor and Detect Intrusion – Proactively Self-Assess – Respond to Incidents.”

- **Prioritize** your efforts within these areas using the **CIS Critical Controls** as you mature your own organization.

- **Determine the number** and type of professionals you require to perform the hands-on work. Engage in a persistent campaign to develop professionals with the appropriate skills and capabilities. Cybersecurity is a specialized practice area within IT and demands specialized training.
Job-Specific, Specialised Focus
Today’s cyber attacks are highly sophisticated and exploit specific vulnerabilities. Broad and general InfoSec certifications are no longer enough. Professionals need the specific skills and specialised knowledge required to meet multiple and varied threats. That’s why GIAC has more than 30 certifications, each focused on specific job skills and each requiring unmatched and distinct knowledge.

Deep, Real-World Knowledge
Theoretical knowledge is the ultimate security risk. Deep, real-world knowledge and hands-on skills are the only reliable means to reduce security risk. Nothing comes close to a GIAC certification to ensure that this level of real-world knowledge and skill has been mastered.

Most Trusted Certification Design
The design of a certification exam impacts the quality and integrity of a certification. GIAC exam content and question design are developed through a rigorous process led by GIAC’s on-staff psychometrician and reviewed by experts in each area. More than 78,000 certifications have been issued since 1999. GIAC certifications meet ANSI standards.

“I think the exam was both fair and practical. These are the kind of real-world problems I expect to see in the field.”
– Carl Hallberg, Wells Fargo, GIAC Reverse Engineering Malware (GREM)
At SANS we have made it our mission to share knowledge with all who will listen, to make the world a safer place. And it starts with you. Learn from the industries’ experts at SANS Summits, network with your peers and discover how best practices are applied directly in the field.

SANS
Cyber Security Summits

Elevate your skills
Learn something new
Hear remarkable stories
Meet people like you
Get new ideas
Be inspired
Find answers

28-29 NOV 2018
European Security Awareness Summit
LONDON

24 JUNE 2019
ICS Europe Summit 2019
MUNICH

22 JULY, 2019
PenTest Summit
BERLIN

COMING SOON
CyberThreat2

To stay up to date with all SANS Events, visit
www.sans.org/information-security-training/by-location/emea
Partnerships and Solutions

SANS works with businesses and governments, creating bespoke training and development solutions that directly support specific operational requirements.

SANS frequently works with organisations to create bespoke skills development solutions. We consult, advise, and then build tailored packages for corporate and government partners looking to enhance their cyber security capability. We also provide tools and solutions that allow organisations to measure and model the effectiveness of these unique solutions.

SANS has the experience and knowledge to deliver solutions across employee assessment, recruitment selection, team development, and intense technical training.

“We work with governments and enterprises across different countries, cultures, and continents,” explains Jan Pieter Spaans, Managing Director Mainland Europe. “Our services include direct solutions, like providing SANS training courses privately.”

All of SANS’ cyber security training courses can be delivered privately, in an organisation’s training facility or HQ. SANS Private Training is delivered by a qualified SANS Instructor with the utmost of discretion. SANS can, of course, provide security cleared Instructors as required.

“Our services go beyond training, though. We also assist security managers in ensuring their team’s skills are kept up to date,” says Jan Pieter Spaans. “We can build and deploy programmes that increase staff retention through skills development or assess an organisation’s needs and then deliver bespoke solutions that deliver across recruitment, on boarding and training.”

Begin a discussion with SANS

For an initial discussion with a SANS Institute Director, contact SANS via emea@sans.org or +44 203 384 3470. Alternatively contact:

Stephen M Jones
Managing Director
UK & Nordics
sjones@sans.org

Ned Baltagi
Managing Director
ME & GCC Regions
nbaltagi@sans.org

Jan-Pieter Spaans
Managing Director,
Mainland Europe
jspaans@sans.org

HMG Cyber Schools Programme

SANS and its delivery partners were selected to devise and run the UK’s first extracurricular cyber security learning programme for schools in England. Cyber Discovery is a multi phase programme that uses an assessment tool and gamified learning platform developed by SANS as well as online and face to face initiatives to enhance the cyber security skills and knowledge of young people.

Stephen Jones, SANS Managing Director for UK and Nordics says, “We are proud to be delivering this vital training programme in support of the UK’s National Cyber Security Strategy and look forward to seeing a great increase in the number of young people taking an interest in cyber security as a future career choice. By assessing, selecting and training students with a natural flair for cyber we intend to help close the skills gap that remains a challenge to all nations.”

HMG’s Cyber Schools Programme launched in Autumn 2017 and falls within the UK government’s CyberFirst initiative. SANS is delivering the programme as Cyber Discovery alongside partner organisations BT, FutureLearn and Cyber Security Challenge UK.

SANS has experience of delivering similar training programmes for school students in other nations.
Bespoke Training Solutions

Private training is ideal for organisations that need an entire team to take a particular SANS course. However, often an organisation needs to implement a bespoke training programme that incorporates several SANS training courses.

SANS works closely with organisations, taking time to understand their specific training needs. After a consultation process, a unique training and development solution is created that meets these needs – based on courses from across the SANS Cyber Security Training Curriculum and additional SANS products.

Uniquely, we are able to provide training recommendations, and then deliver that programme ourselves.

Assessment and Candidate Selection

SANS works regularly with organisations, helping them to streamline their recruitment processes and procedures.

“The traditional mode of candidate selection generally relies on sifting CVs,” explains Ned Baltagi, Director, SANS ME & GCC Regions. “Organisations tell us regularly that this is time consuming and doesn’t provide the reliable - and predictable - results they need when selecting front-line cyber security staff.”

SANS CyberTalent is one such selection product. It is a suite of assessment tools that improves the effectiveness of a cyber security recruitment and selection process.

SANS CyberTalent products use psychometric and skills testing to assess candidates’ aptitude and suitability for particular roles. The online assessments leverage SANS’ experience in the field of cyber security training and GIAC certification to gauge technical skills and knowledge.

CyberTalent provides managers and HR teams with a deeper understanding of candidates’ technical and conceptual makeup.

Assessing Team Strengths and Weaknesses

SANS CyberTalent and other bespoke solutions extend beyond candidate selection. SANS works closely with many organisations, helping them to ensure their security team keeps developing and evolving.

“Security teams must change and adapt – new attack vectors emerge, technologies evolve and businesses themselves change,” states Jan Pieter Spaans. “Training is an integral part of this development process... but training needs vary across a team. Training just isn’t a one size-fits-all business.”

To support managers in developing and improving their team, SANS provides assessment products such as SANS NetWars, SANS CyberCity and SANS CyberTalent.

These allow Security and HR managers to achieve a clear understanding of their team’s strengths, weaknesses and training needs.

SANS then builds a unique training programme that focusses on addressing a team or individual’s specific requirements.

Career development also aids staff retention and ensures a security team remains effective. SANS helps employers create bespoke training programmes using the extensive SANS training curriculum.

Following a consultation process, SANS delivers programmes that meet business needs and also offer security professionals a career roadmap.

Training Programmes

SANS is experienced in building residential training programmes for many different types of organisation – governments, enterprises, and military bodies - spanning different geographic regions and business cultures.

These programmes vary in scale and focus, and are designed to precisely meet a client’s requirements. SANS Cyber Academy is a cyber security training programme that demonstrates this capability.

“Cyber Academy programmes identify, train, and deploy new cyber security talent. The success of the UK Cyber Academy and HMG Cyber Retraining Academy in delivering expertly trained, GIAC qualified security personnel into the workforce demonstrated SANS’ capabilities in creating bespoke training solutions,” says Stephen Jones, SANS Managing Director for UK and Nordics. “The Cyber Retraining Academy in partnership with HM Government was delivered as part of the UK’s National Cyber Security Strategy”

“SANS first identifies candidates with the potential to succeed in cyber security. Those candidates are then assessed using SANS’ CyberTalent.”

“Successful applicants then enrol into Cyber Academy and are invested with intensive residential cyber security training – the content being drawn from across SANS’ Curricula.”

As with UK Cyber Academy 2015, the Cyber Retraining Academy graduates are being deployed into key cyber security roles with UK organisations.
SANS Cyber Defence Courses

Learn the hands-on, practical skills needed to defend and protect networks, people, and infrastructure.

SANS Cyber Defence curriculum teaches the cyber security skills necessary to prevent, detect, and respond to digital threats. Two sub curricula comprise the full Cyber Defence Curriculum: Core Security and Network and Security Operations.

SANS Cyber Defence Curriculum explores how to perform the following core cyber defence duties:

- Detect, prevent and respond to attacks
- Design and build secure business procedures
- Identify, assess, and remediate exposures in existing networks
- Model a threat and plan a defence
- Communicate a cyber attack - and its ramifications - to managers
- Build security solutions that are scalable
- Secure and protect an organisation’s intellectual property

SANS Cyber Defence Curriculum teaches all of these skills, and more.

“This was the best and most well-presented course I ever attended.”
London
SEC401

Equipped to defend
SANS training is hands-on. Rather than just sharing well-known theories, SANS courses place an emphasis on opening a command line prompt and working through an attack or defence situation.

SANS’ success is rooted in the quality of its people, specifically our Instructors’ experience.

SANS Instructors are experts in their respective fields. They are security practitioners who work on the frontline. They’re acquainted with the dominant threats organisations face, and understand the prevailing defences.

SANS also equips students with a wealth of supplementary learning resources. Students are, for example, provided with a library of textbooks. The books are created by the same experts who created the course they support. We also provide students with posters, cheat sheets and software tool kits. All of our training content is updated regularly.

“I got a real insight into the mind of the adversary.”
London
SEC401
SANS Penetration Testing & Vulnerability Courses

Hands-on penetration testing security training that teaches how to think, work and attack like a hacker.

SANS Pen Test courses focus on equipping students with the technical skills, knowledge and tools they need to make a difference, as soon as they get back to the office.

SANS Pen Test training is hands on. Students can expect in-depth lab exercises, simulations, cryptographic challenges and war games.

At the heart of our penetration testing training curriculum is a belief in high-value testing. This encompasses:

- Modelling the activities of real-world attackers.
- Finding vulnerabilities in target systems.
- Exploiting them under controlled circumstances.
- Determining and documenting business risk.
- Applying technical excellence.
- Working in a professional, safe fashion according to a carefully designed scope and rules of engagement.
- Helping an organisation prioritise its resources to improve the security stance.

SANS Penetration Testing Instructors bring expert technical and industrial experience into the classroom. Many Instructors hold prominent positions in high-profile, global organisations. Others run pen test consultancies and work with prominent businesses. SANS Instructors bring this experience into the classroom.

Real World Experience
SANS Penetration Testing Instructors bring expert technical and industrial experience into the classroom. Many Instructors hold prominent positions in high-profile, global organisations. Others run pen test consultancies and work with prominent businesses. SANS Instructors bring this experience into the classroom.

“Overall a well presented and comprehensive course that I would recommend to any information security professional.”
London
SEC560
SANS Forensics and Incident Response

Courses

Hands-on and intensive digital forensics and incident response training delivered by acknowledged security and forensics experts.

SANS Digital Forensic and Incident Response curriculum (DFIR) helps organisations investigate and respond effectively to IT security breaches.

SANS DFIR Curriculum offers a great deal of scope for specialisation. SANS offers courses that hone in on Windows, smartphone, Apple operating systems, network and memory forensics, and more.

SANS DFIR Curriculum helps organisations deploy the correct responses - responses designed to minimise financial and reputation loss, and to help businesses recover strongly from an attack.

Resources

SANS DFIR Instructors are industry practitioners who spend the majority of their professional lives working on security’s front line. They bring this real-world experience into the classroom.

Many SANS Instructors are prominent members of the DFIR community. They write, blog, speak, and contribute to the global consensus.

Along with their technical credentials, our DFIR Instructors are skilled teachers. They understand how to get the best from their students.

SANS supplies students with courseware and supplementary resources. We provide every student with a library of textbooks that relate directly to the course – books that are written by the course’s author.

SANS also supplies students with licences for software tools explored in class. This means students can deploy the skills they’ve learned as soon as they get back to their desk.

“Intense, nothing can prepare you for learning from a true master of their art.”

London

FOR508
SANS Management and Audit Courses

Hands-on training designed to equip advancing managers and auditors with the skills needed to build the right policies and processes, and to make the best IT security decisions.

SANS Management Curriculum teaches students how to manage security. Courses are ideal for newly appointed information security officers, skilled administrators who are stepping up to a management role, and seasoned managers who find themselves managing technical people.

Training for IT Security Auditors
SANS Audit training equips students to audit many business critical technologies such as applications, databases, networks and perimeter defences. Our curriculum teaches risk-based methodologies that yield far better enterprise security.

SANS Audit training also teaches the practical skills and techniques needed to perform a comprehensive IT audit. With a hands-on approach to training, SANS exposes students to the best tools – and best practices – needed to add business value through their audits.

Our courses develop and expand students’ knowledge of audit’s Critical Security Controls.

Training For Security Managers
Two SANS Management Courses that run at Training Events in the EMEA region are ‘MGT433: Securing the Human – How to Build, Maintain, and Measure a High-Impact Awareness Program’, and ‘MGTS12: SANS Security Leadership Essentials for Managers with Knowledge Compression™.

MGTS12 is a hands-on course designed to impart the skills and knowledge necessary to lead a project or product’s security components.

The course empowers managers and auditors to speak the same language as technical staff, including system, security, and network administrators.

MGTS433 focusses on helping managers to create, deploy, and access the efficacy of a high-impact security awareness campaign.

All SANS Management Courses are taught by SANS Instructors. Our Management Instructors are, primarily, practicing cyber security management professionals. They bring this real-world experience into the classroom.

Students are equipped with a wealth of courseware and resources to supplement their learning. We supply, for example, a library of expertly written textbooks.

“The course helped me sharpen up my awareness programme planning for next year.”

London
MGT433

“...excellent as it covers most of the technical auditing techniques and tools used for the auditing.”

Dubai UAE
AUD507

PAGE 54
PAGE 55
PAGE 56
PAGE 58
PAGE 59
PAGE 60
PAGE 61
PAGE 62
PAGE 63

SANS TRAINING CATALOGUE, 2018
SANS Secure Software Development Courses

Placing secure software development practice and principles at its heart, sans teaches how to architect defensible applications.

SANS Secure Software Development courses are built with two outcomes in mind: firstly, to equip programmers with the skills and knowledge to write secure code; secondly, alumni are able to recognise the security shortcomings in existing code.

The SANS Secure Software Development Curriculum covers secure coding across C and C#, .NET, Java/JEE and web applications. We also offer deep-dive courses that focus on developing and architecting defensible applications.

Organisations looking to further enhance their software and product security can also access SANS’ penetration testing curriculum. Specifically, SANS offers a course designed to teach web application pen testing.

At the heart of SANS Secure Software Development curriculum is a promise: as soon as students return to their team from their training they’ll be able to deploy what they’ve learned.

“A very knowledgeable instructor who demonstrates very well the issues and solutions in modern web apps security.”

London
DEV522

“DEV522 really covers the security aspects every web developer must know.”

London
DEV522

Architect Securely
SANS Secure Software Development is designed to foster safety by design. Our developer security training courses teach students to:

• Build securely – Our courses teach development’s defining security principles.
• Hunt for flaws – Learn to find security issues in existing code.
• Secure across different languages – Courses address .NET, C & C++, JAVA/JEE.
• Stay current - SANS Software Security Curriculum exemplifies our drive to stay one step ahead of criminals.
• Engineer with security in mind – SANS Instructors are real-word practitioners who specialise in architecting defensible applications.
• Be prepared – Students receive a wide selection of textbooks, tools, and learning resources, all of which they can keep and refer back to.

Outside of the classroom our Secure Software Development Instructors are respected practitioners and proponents in the field of defensive programming.

SANS training is designed to be hands-on. Expect a long list of live, code based lab exercises.
SANS Industrial Control Systems Courses

Learn the skills and knowledge needed to defend industrial control systems from cyber attack.

SANS ICS Curriculum has been created to assist two groups of professionals: Control system engineers who need to learn more about security best practice and securing their infrastructure, and IT security practitioners who need a clearer understanding of ICS’ key technologies.

SANS ICS training curriculum is hands-on. Courses feature many live lab based exercises and simulations. Students can, for example, gain experience of network capture forensics, spoofing Modbus-TCP control signals, and finding passwords in EEPROM dumps.

SANS ICS training provides:
- Real world training – A panel of experts with an intimate understanding of ICS cyber security and SCADA principles create course content.
- Training for engineers – Specialised training is designed to help engineers understand security.
- Training for security professionals – Training helps security staff understand SCADA security and embedded systems, their functions and their limitations.
- Courses led by experts – Training classes are taught by respected experts in the ICS field.
- Extensive courseware – ICS students are equipped with a library of textbooks and extra material.

“Valuable course for engineers, IT and physical security consultants for Industrial Control Systems.”
London
ICS410

“I think IT Security personnel and engineers from any company using ICS should attend this course.”
London
ICS410

“Valuable course for engineers, IT and physical security consultants for Industrial Control Systems.”
London
ICS410

“I think IT Security personnel and engineers from any company using ICS should attend this course.”
London
ICS410

SANS TRAINING CATALOGUE, 2018
To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

• Do you have basic computer knowledge, but are new to information security and in need of an introduction to the fundamentals?
• Are you bombarded with complex technical security terms that you don’t understand?
• Are you a non-IT security manager (with some technical knowledge) who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o’clock news?
• Do you need to be conversant in basic security concepts, principles, and terms, even if you don’t need “deep in the weeds” detail?
• Have you decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification?

If you answer yes to any of these questions, the SEC301: Intro to Information Security training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised, five-day comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles. This course is designed for students who have a basic knowledge of computers and technology but no prior knowledge of cybersecurity. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You’ll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

Written by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next course up the line, SEC401: Security Essentials Bootcamp Style. It also delivers on the SANS promise: You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.

“\textquote{I very much appreciate the passion of the instructors. Their knowledge is incredible and the presentation of their knowledge is down-to-earth and helpful. SANS training is far better than privacy-related certification.}”

Ron Hoffman,
MUTUAL OF OMAHA
This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques you can directly apply when you get back to work. You’ll learn tips and tricks from the experts so you can win the battle against the wide range of cyber adversaries that want to harm your environment.

STOP and ask yourself the following questions:
• Do you fully understand why some organisations get compromised and others do not?
• If there were compromised systems on your network, are you confident that you would be able to find them?
• Do you know the effectiveness of each security device and are you certain they are all configured correctly?
• Are proper security metrics set up and communicated to your executives to drive security decisions?

If you do not know the answers to these questions, SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

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. Our course will show you how to prevent your organisation’s security problems from being headline news in the Wall Street Journal!

Prevention is ideal but detection is a must.
With the rise in 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 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:
• What is the risk?
• Is it the highest priority risk?
• 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.

“\textit{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

Who should attend?
• Security professionals who want to fill the gaps in their understanding of technical information security
• Managers who want to understand information security beyond simple terminology and concepts
• Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
• IT engineers and supervisors who need to know how to build a defensible network against attacks
• Administrators responsible for building and maintaining systems that are being targeted by attackers
• Forensic specialists, penetration testers, and auditors who need a solid foundation of security principles to be as effective as possible at their jobs
• Anyone new to information security with some background in information systems and networking

You will be able to...
• Design and build a network architecture using VLANs, 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 operate a virtual lab to test and evaluate the tools/security of systems
• Create an effective policy that can be enforced within an organisation and prepare a checklist to validate security, creating metrics to tie into training and awareness
• Identify visible weaknesses of a system utilising various tools including dumpsec and OpenVAS, and once vulnerabilities are discovered cover ways to configure the system to be more secure
Immeasurable amounts of personal, potentially incriminating data is currently stored in the websites, apps, and social media platforms that people access and update via their devices daily. That data can become evidence for citizens, governments, and businesses to use in solving real financial, employment, and criminal issues with the help of a professional information gatherer.

SEC487 will teach students legitimate and effective ways to find, gather, and analyse this data from the Internet. You’ll learn about reliable places to harvest data using manual and automated methods and tools. Once you have the data, we’ll show you how to ensure that it is analysed, sound, and useful to your investigations.

This is a foundational course in open-source intelligence (OSINT) gathering and, as such, will move quickly through many areas of the field. The course will teach you current, real-world skills, techniques, and tools that law enforcement, private investigators, cyber attackers, and defenders use to scour the massive amount of information across the Internet, analyse the results, and pivot on interesting pieces of data to find other areas for investigation. Our goal is to provide the OSINT knowledge base for students to be successful in their fields whether they are cyber defenders, threat intelligence analysts, private investigators, insurance claims investigators, intelligence analysts, law enforcement personnel, or just someone curious about OSINT.

Throughout the course week, students will participate in numerous hands-on labs using the tools and techniques that are the basis for gathering free data from the Internet. The 20 labs in this course use the live Internet and dark web to help students gain real-world confidence. You’ll leave the course knowing not just how to use search features on a website, but all of the scenario-based requirements and OSINT techniques needed to gather truly important OSINT data.
Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage.

SEC501: Advanced Security Essentials – Enterprise Defender builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

It has been said of security that “prevention is ideal, but detection is a must.” However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

Despite an organisation’s best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organisations need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, looking for indications of an attack, and performing penetration testing and vulnerability analysis against your organisation to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

“By far the best course I have ever attended. Every day I have learnt things that can be applied at work”

Stuart Long,
BANK OF ENGLAND

“Great course content very interesting and comprehensive.”

John O’Brien,
AIRBUS DEFENCE & SPACE
Intrusion Detection In-Depth

Reports of prominent organisations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?

Preserving the security of your site in today’s threat environment is more challenging than ever before. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and sometimes vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in SEC503: Intrusion Detection In-Depth is to acquaint you with the core knowledge, tools, and techniques to defend your networks with insight and awareness. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

Mark Twain said, “It is easier to fool people than to convince them that they’ve been fooled.” Too many IDS/IPS solutions provide a simplistic red/green, good/bad assessment of traffic and too many untrained analysts accept that feedback as the absolute truth. This course emphasises the theory that a properly trained analyst uses an IDS alert as a starting point for examination of traffic, not as a final assessment. SEC503: Intrusion Detection In-Depth is to acquaint you with the core knowledge, tools, and techniques to defend your networks with insight and awareness. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

SEC503: Intrusion Detection In-Depth delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to master different open-source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material.

“In order to defend a network you need to understand how it works, this course is both enjoyable and challenging”

Holly C
MOD UK

Who should attend?
- Intrusion detection (all levels), system, and security analysts
- Network engineers/administrators
- Hands-on security managers

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
- Craft packets with Scapy
- Use the open-source network flow tool SiLK to find network behavior anomalies
- Use your knowledge of network architecture and hardware to customise placement of IDS sensors and sniff traffic off the wire

“I loved the course. I had big expectations, because I have also taken the 401 security essentials course and it was amazing too. All my expectations have been completed. I had great classmates and we had a lot of fun during the day and the evenings.”

Diana Moldovan
BETFAIR
Hackers know how to use PowerShell for evil. Do you know how to use it for good? In SEC505 you will learn PowerShell and Windows security hardening at the same time. SecOps requires automation, and Windows automation means PowerShell.

You've run a vulnerability scanner and applied patches – now what? A major theme of this course is defensible design: we have to assume that there will be a breach, so we need to build in damage control from the beginning. Whack-a-mole incident response cannot be our only defensive strategy – we’ll never win, and we’ll never get ahead of the game. By the time your monitoring system tells you a Domain Admin account has been compromised, IT’S TOO LATE.

For the assume breach mindset, we must carefully delegate limited administrative powers so that the compromise of one administrator account is not a total catastrophe. Managing administrative privileges is a tough problem, so this course devotes an entire day to just this one critical task.

Learning PowerShell is also useful for another kind of security: job security. Employers are looking for people with these skills. You don't have to know any PowerShell to attend the course; we will learn it together. About half the labs during the week are PowerShell, while the rest use graphical security tools.

PowerShell is free and open source on GitHub for Linux and Mac OS, too. This course is not a vendor show to convince you to buy another security appliance or to install yet another endpoint agent. The idea is to use built-in or free Windows and Active Directory security tools when we can (especially PowerShell and Group Policy) and then purchase commercial products only when absolutely necessary.

If you are an IT manager or CIO, the aim for this course is to have it pay for itself 10 times over within two years, because automation isn’t just good for SecOps/DevOps, it can save money, too.

This course is designed for systems engineers, security architects, and the Security Operations (SecOps) team. The focus of the course is on how to automate the NSA Top 10 Mitigations and the CIS Critical Security Controls related to Windows, especially the ones that are difficult to implement in large environments. This is a fun course and a real eye-opener, even for Windows administrators with years of experience. We don’t cover patch management, share permissions, or other such basics – the aim is to go far beyond that! Come have fun learning PowerShell and agile Windows security at the same time!
Securing Linux/Unix

SEC506: Securing Linux/Unix provides in-depth coverage of Linux and Unix security issues that includes specific configuration guidance and practical, real-world examples, tips, and tricks. We examine how to mitigate or eliminate general problems that apply to all Unix-like operating systems, including vulnerabilities in the password authentication system, file system, virtual memory system, and applications that commonly run on Linux and Unix.

The course will teach you the skills to use freely available tools to handle security issues, including SSH, AIDE, sudo, Isol, and many others. SANS’ practical approach uses hand-on exercises every day to ensure that you will be able to use these tools as soon as you return to work. We will also put these tools to work in a special section that covers simple forensic techniques for investigating compromised systems.

Topics
- Memory Attacks, Buffer Overflows
- File System Attacks, Race Conditions
- Trojan Horse Programs and Rootkits
- Monitoring and Alerting Tools
- Unix Logging and Kernel-Level Auditing
- Building a Centralised Logging Infrastructure
- Network Security Tools
- SSH for Secure Administration
- Server Lockdown for Linux and Unix
- Controlling Root Access with sudo
- SELinux and chroot() for Application Security
- DNSSEC Deployment and Automation
- mod_security and Web Application Firewalls
- Secure Configuration of BIND, Sendmail, Apache
- Forensic Investigation of Linux Systems

Course Author Statement
A wise man once said, “How are you going to learn anything if you know everything already?” And yet there seems to be a quiet arrogance in the Unix community that we have figured out all of our security problems, as if to say, “Been there, done that.” All I can say is that what keeps me going in the Unix field, and the security industry in particular, is that there is always something new to learn, discover, or invent. In 20 plus years on the job, what I have learned is how much more there is that I can learn. I think this is also true for the students in my courses. I regularly get comments back from students who say things like, “I have been using Unix for 20 years, and I still learned a lot in this class.” That is really rewarding.
- Hal Pomeranz

“i have been a unix systems administrator for a couple of decades, but in SEC506 I learned something new every day”
Sheryl Coppenger, NCI INC.

Who should attend?
- Security professionals looking to learn the basics of securing Unix operating systems.
- Experienced administrators looking for in-depth descriptions of attacks on Unix systems and how they can be prevented.
- Administrators needing information on how to secure common Internet applications on the Unix platform.
- Auditors, incident responders, and information security analysts who need greater visibility into Linux and Unix security tools, procedures, and best practices.

You will be able to...
- Significantly reduce the number of vulnerabilities in the average Linux/Unix system by disabling unnecessary services.
- Protect your systems from buffer overflows, denial-of-service, and physical access attacks by leveraging OS configuration settings.
- Configure host-based firewalls to block attacks from outside.
- Deploy SSH to protect administrative sessions, and leverage SSH functionality to securely automate routine administrative tasks.
- Use sudo to control and monitor administrative access.
- Create a centralized logging infrastructure with Syslog-NG, and deploy log monitoring tools to scan for significant events.
- Use SELinux to effectively isolate compromised applications from harming other system services.
- Securely configure common Internet-facing applications such as Apache and BIND.
- Investigate compromised Linux/Unix systems with Sleuthkit, Isol, and other open-source tools.
- Understand attacker rootkits and how to detect them with AIDE and rkhunter/chkrootkit.
Continuous Monitoring and Security Operations

We continue to underestimate the tenacity of our adversaries! Organisations are investing significant 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. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed 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 victimized 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 (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organisation or Security Operations Center (SOC) to analyse threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach will be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and this course will greatly increase your understanding and enhance your skills in implementing CM utilising the NIST framework.

SEC511 will take you on quite a journey. We start by exploring traditional security architecture to assess its current state and the attacks against it. Next, we discuss and discover modern security design that represents a new proactive approach to such architecture that can be easily understood and defended. We then transition to how to actually build the network and endpoint security, and then carefully navigate our way through automation, NSM/CDM/CSM. For timely detection of potential intrusions, the network and systems must be proactively and continuously monitored for any changes in the security posture that might increase the likelihood that attackers will succeed.

Your SEC511 journey will conclude with one last hill to climb! The final day (Day 6) 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. Course authors Eric Conrad and Seth Misenar have designed the Capture-the-Flag competition to be fun, engaging, comprehensive, and challenging. You will not be disappointed!

Who should attend?
• Security architects
• Senior security engineers
• Technical security managers
• Security Operations Center (SOC) analysts, engineers, and managers
• CND analysts
• Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)

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 Center (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 robust Network Security Monitoring/Continuous Security Monitoring (NSM/CSM)
• Utilise tools to support implementation of Continuous Monitoring per NIST guidelines SP800-137
• Determine requisite monitoring capabilities for a SOC environment
• Determine capabilities required to support continuous monitoring of key Critical Security Controls

“Very comprehensive, hands-on and can be applied to working environment.”
Ewa Konkolska
PRUDENTIAL, PGDS
SEC530: Defensible Security Architecture is designed to help students build and maintain a truly defensible security architecture. “The perimeter is dead” is a favourite saying in this age of mobile, cloud, and the Internet of Things, and we are indeed living in a new world of “de-parameterisation” where the old boundaries of “inside” and “outside” or “trusted” and “untrusted” no longer apply.

This changing landscape requires a change in mindset, as well as a repurposing of many devices. Where does it leave our classic perimeter devices such as firewalls? What are the ramifications of the “encrypt everything” mindset for devices such as Network Intrusion Detection Systems?

In this course, students will learn the fundamentals of up-to-date defensible security architecture. There will be a heavy focus on leveraging current infrastructure (and investment), including switches, routers, and firewalls. Students will learn how to reconfigure these devices to better prevent the threat landscape they face today. The course will also suggest newer technologies that will aid in building a robust security infrastructure.

While this is not a monitoring course, this course will dovetail nicely with continuous security monitoring, ensuring that security architecture not only supports prevention, but also provides the critical logs that can be fed into a Security Information and Event Management (SIEM) system in a Security Operations Center.

Hands-on labs will reinforce key points in the course and provide actionable skills that students will be able to leverage as soon as they return to work.

Who should attend
- Security Architects
- Network Engineers
- Network Architects
- Security Analysts
- Senior Security Engineers
- System Administrators
- Technical Security Managers
- CND Analysts
- Security Monitoring Specialists
- Cyber Threat Investigators

You will be able to...
- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Determine appropriate security monitoring needs for organizations of all sizes
- Maximize existing investment in security architecture by reconfiguring existing assets
- Determine capabilities required to support continuous monitoring of key Critical Security Controls
- Configure appropriate logging and monitoring to support a Security Operations Center and continuous monitoring program

36 CPE/CMU CREDITS
As more organisations move data and infrastructure to the cloud, security is becoming a major priority. Operations and development teams are finding new uses for cloud services, and executives are eager to save money and gain new capabilities and operational efficiency by using these services. But, will information security prove to be an Achilles’ heel? Many cloud providers do not provide detailed control information about their internal environments, and quite a few common security controls used internally may not translate directly to the public cloud.

The SEC545 course, Cloud Security Architecture and Operations, will tackle these issues one by one. We’ll start with a brief introduction to cloud security fundamentals, and then cover the critical concepts of cloud policy and governance for security professionals. For the rest of day one and all of day two, we’ll move into technical security principles and controls for all major cloud types (SaaS, PaaS, and IaaS). We’ll learn about the Cloud Security Alliance framework for cloud control areas, then delve into assessing risk for cloud services, looking specifically at technical areas that need to be addressed.

The course then moves into cloud architecture and security design, both for building new architectures and for adapting tried-and-true security tools and processes to the cloud. This will be a comprehensive discussion that encompasses network security (firewalls and network access controls, intrusion detection, and more), as well as all the other layers of the cloud security stack.

We’ll visit each layer and the components therein, including building secure instances, data security, identity and account security, and much more. We’ll devote an entire day to adapting our offense and defence focal areas to cloud. This will involve looking at vulnerability management and pen testing, as well as covering the latest and greatest cloud security research. On the defence side, we’ll delve into incident handling, forensics, event management, and application security.

We wrap up the course by taking a deep dive into SecDevOps and automation, investigating methods of embedding security into orchestration and every facet of the cloud life cycle. We’ll explore tools and tactics that work, and even walk through several cutting-edge use cases where security can be automated entirely in both deployment and incident detection-and-response scenarios using APIs and scripting.

**Who should attend?**
- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- Security monitoring analysts
- Cloud security architects
- DevOps and DevSecOps engineers
- System administrators
- Cloud administrators

**You will be able to...**
- Revise and build internal policies to ensure cloud security is properly addressed
- Understand all major facets of cloud risk, including threats, vulnerabilities, and impact
- Articulate the key security topics and risks associated with SaaS, PaaS, and IaaS cloud deployment models
- Evaluate Cloud Access Security Brokers (CASBs) to better protect and monitor SaaS deployments
- Build security for all layers of a hybrid cloud environment, starting with hypervisors and working to application layer controls
- Evaluate basic Virtualisation hypervisor security controls
- Design and implement network security access controls and monitoring capabilities in a public cloud environment
- Design a hybrid cloud network architecture that includes IPSec tunnels
- Integrate cloud identity and access management (IAM) into security architecture
- Evaluate and implement various cloud encryption types and formats
- Develop multi-tier cloud architectures in a Virtual Private Cloud (VPC), using subnets, availability zones, gateways, and NAT Integrate security into DevOps teams, effectively creating a DevSecOps team structure
- Build automated deployment workflows using AWS and native tools
- Incorporate vulnerability management, scanning, and penetration testing into cloud environments

**30 CPE/CMU CREDITS**
Many organisations have logging capabilities but lack the people and processes to analyse it. In addition, logging systems collect vast amounts of data from a variety of data sources that require an understanding of the sources for proper analysis. This class is designed to provide individuals training, methods, and processes for enhancing existing logging solutions. This class will also help you understand the when, what, and why behind the logs. This is a lab-heavy course that utilises SOF-ELK, a SANS-sponsored free Security Incident and Events Management (SIEM) solution, to provide hands-on experience and the mindset for large-scale data analysis.

Today, security operations do not suffer from a “big data” problem but rather a “data analysis” problem. Let’s face it, there are multiple ways to store and process large amounts of data without any real emphasis on gaining insight into the information collected. Added to that is the daunting idea of an infinite list of systems from which one could collect logs. It is easy to get lost in the perils of data saturation. This class moves away from the typical churn-and-burn log systems and moves instead towards achieving actionable intelligence and developing a tactical Security Operations Center (SOC).

This course is designed to demystify the SIEM architecture and process by navigating the student through the steps of tailoring and deploying a SIEM to full SOC integration. The material will cover many bases in the “appropriate” use of a SIEM platform to enrich readily available log data in enterprise environments and extract actionable intelligence. Once collected, the student will be shown how to present the gathered input into usable formats to aid in eventual correlation. Students will then iterate through the log data and events to analyse key components that will allow them to learn how rich this information is, how to correlate the data, start investigating based on the aggregate data, and finally, how to go hunting with this newly gained knowledge. They will also learn how to deploy internal post-exploitation tripcodes and breach canaries to nimbly detect sophisticated intrusions. Throughout the course, the text and labs will not only show how to manually perform these actions, but also how to automate many of the processes mentioned so students may employ these tasks the day they return to the office.

The underlying theme is to actively apply Continuous Monitoring and analysis techniques by utilising modern cyber threat attacks. Labs will involve replaying captured attack data to provide real-world results and visualizations.

**Course Author Statement**

“Today, security operations do not suffer from a ‘big data’ problem but rather a ‘data analysis’ problem. Let’s face it, there are multiple ways to store and process large amounts of data without any real emphasis on gaining insight into the information collected. Added to that is the daunting idea of an infinite list of systems from which one could collect logs and it is easy to get lost in the perils of data saturation. This class is the switch from the typical churn and burn log systems to achieving actionable intelligence and developing a tactical Security Operations Center (SOC).”

-Justin Henderson

**Who should attend?**

- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- SOC analysts
- SOC engineers SOC managers
- CND analysts
- Security monitoring specialists
- System administrators
- Cyber threat investigators
- Individuals working to implement Continuous Security Monitoring
- Individuals working in a hunt team capacity

---

**SIEM with Tactical Analytics NEW!**

HANDS-ON • SIX DAYS • LAPTOP REQUIRED

46 CPE/CMU CREDITS
One of today’s most rapidly evolving and widely deployed technologies is server virtualisation. SEC579: Virtualization and Software-Defined Security is intended to help security, IT operations, and audit and compliance professionals build, defend, and properly assess both virtual and converged infrastructures, as well as understand software-defined networking and infrastructure security risks.

Many organisations are already realizing cost savings from implementing virtualised servers, and systems administrators love the ease of deployment and management of virtualised systems. More and more organisations are deploying desktop, application, and network virtualisation as well. There are even security benefits of virtualisation: easier business continuity and disaster recovery, single points of control over multiple systems, role-based access, and additional auditing and logging capabilities for large infrastructure.

With these benefits comes a dark side, however. Virtualisation technology is the focus of many new potential threats and exploits, and it presents new vulnerabilities that must be managed. There are also 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.

Virtualisation technologies also connect to network infrastructure and storage networks, and require careful planning with regard to access controls, user permissions, and traditional security controls.

In addition, many organisations are evolving virtualised infrastructure into private clouds using converged infrastructure that employs software-defined tools and programmable stack layers to control large, complex data centers. Security architecture, policies, and processes will need to be adapted to work within a converged infrastructure, and there are many changes that security and operations teams will need to accommodate to ensure that assets are protected.

This course will cover core operational functions like secure network design and segmentation, building secure systems, and secure virtualisation implementation and controls. Cutting-edge topics like software-defined networking and container technology will also be covered in detail with an emphasis on security techniques and controls. Security-focused virtualisation, integration, and monitoring will be covered at length.

Attacks and threats to virtual environments will be discussed, and students will learn how to perform vulnerability assessments and penetration tests in their virtual environments. We’ll also look at how to implement network intrusion detection and access controls, implement log and event management, and perform forensics and incident handling in virtual and converged data centers. Finally, students will learn how to perform technical audits and assessments of their in-house and public cloud environments, creating reports and documenting technical controls. This instruction will heavily emphasise automation and scripting techniques.

Who should attend?

- Security personnel who are tasked with securing virtualisation and private cloud infrastructure
- Network and systems administrators who need to understand how to architect, secure, and maintain virtualisation and cloud technologies
- Technical auditors and consultants who need to gain a deeper understanding of VMware virtualisation from a security and compliance perspective

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 converged and software-defined 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

“Every single virtualisation admin (in our organisation) should take this course. I am going to promote this course!”

Cory Verboom, DMO

“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

30 CPE/CMU CREDITS

SANS TRAINING CATALOGUE, 2018
This course will arm you with the knowledge and expertise you need to detect and respond to today's threats. Recognising that a prevent-only strategy is not sufficient, we will introduce security controls designed to stop advanced adversaries.

With more than 20 labs plus a full-day “Defend-The-Flag” exercise during which students attempt to defend our virtual organization from different waves of attacks against its environment, SEC599 gives students real world examples of how to prevent attacks.

The six-day journey starts with an analysis of recent attacks through in-depth case studies. We explain what types of attacks are occurring and introduce the Advanced Persistent Threat (APT) Attack Cycle as a structured approach to describing attacks. In order to understand how attacks work, you will also compromise our virtual organisation “SyncTechLabs” in the Day 1 exercises.

Throughout days two to five we discuss how effective security controls can be implemented to prevent, detect, and respond to cyber attacks. Some of the topics addressed include:

- Building your own mail sandbox solution to detect spear phishing
- Developing effective group policies to stop malicious code execution
- Stopping 0-day exploits using exploit mitigation techniques and application whitelisting
- Detecting and avoiding malware persistence
- Detecting and preventing lateral movement through sysmon, Windows event monitoring, and group policies
- Blocking and detecting command and control through network traffic analysis
- Leveraging threat intelligence to improve your security posture

During the “Defend-the-Flag” challenge on the final course day you will be pitted against advanced adversaries in an attempt to keep your network secure. Can you protect the environment against the different waves of attacks? The adversaries aren’t slowing down, so what are you waiting for?
Experience NetWars

Play solo or on a team of up to five players

“NetWars takes the concepts in the class and gives you an opportunity to put them into action. Highly recommended!”

– Kyle McDaniel, Lenovo

Choose from:
Core NetWars | DFIR NetWars | Cyber Defense NetWars | ICS NetWars

Develop skills in:
• Cyber Defense
• Penetration Testing
• Digital Forensics & Incident Response
• ICS

Participation in NetWars is free for students taking 4-, 5-, or 6-day courses.

NetWars takes place in the evening, after class, and gives you an immediate opportunity to apply what you’ve learned in a fun, competitive, hands-on, and educational environment!

Seating is limited, register for NetWars when you register for your course.

www.sans.org/netwars
Computer exploitation is on the rise. As advanced adversaries become more numerous, more capable, and much more destructive, organizations must become more effective at mitigating their information security risks at the enterprise scale. SEC460 is the premier course focused on building technical vulnerability assessment skills and techniques, while highlighting time-tested practical approaches to ensure true value across the enterprise. The course covers threat management, introduces the core components of comprehensive vulnerability assessment, and provides the hands-on instruction necessary to produce a vigorous defensive strategy from day one. The course is focused on equipping information security personnel from organizations charged with effectively and efficiently securing 10,000 or more systems.

SEC460 begins with an introduction to information security vulnerability assessment fundamentals, followed by in-depth coverage of the Vulnerability Assessment Framework. It then moves into the structural components of a dynamic and iterative information security program. Through a detailed, practical analysis of threat intelligence, modeling, and automation, students will learn the skills necessary to not only use the tools of the trade, but also to implement a transformational security vulnerability assessment program. SEC460 will teach you how to use real industry-standard security tools for vulnerability assessment, management, and mitigation. It is the only course that teaches a holistic vulnerability assessment methodology while focusing on challenges faced in a large enterprise. You will learn on a full-scale enterprise range chock full of target machines representative of an enterprise environment, leveraging production-ready tools, and a proven testing methodology.

This course takes you beyond the checklist, giving you a tour of the attackers’ perspective that is crucial to discovering where they will strike. Operators are more than the scanner they employ. SEC460 emphasizes this personnel-centric approach by examining the shortfalls of many vulnerability assessment programs in order to provide you with the tactics and techniques required to secure networks against even the most advanced intrusions. We wrap up the first five days of instruction with a discussion of triage, remediation, and reporting before putting your skills to the test on the final day against an enterprise-grade cyber range with numerous target systems for you to analyze and explore. The cyber range is a large environment of servers, end-users, and networking gear that represents many of the systems and topologies used by enterprises. By adopting an end-to-end approach to vulnerability assessment, you can be confident that your skills will provide much-needed value in securing your medium- or large-scale organization.
Hacker Tools, Techniques, Exploits, and Incident Handling

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

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

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

Who should attend?

- Incident handlers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

You will be able to...

- Apply incident handling processes in-depth, including preparation, identification, containment, eradication, and recovery, to protect enterprise environments
- Analyse the structure of common attack techniques in order 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 defenses and response tactics for each
- Use built-in command-line tools such as Windows tasklist, wmic, and reg as well as Linux netstat, ps, and lsof to detect an attacker’s presence on a machine
- Analyse router and system ARP tables along with switch CAM tables to track an attacker’s activity through a network and identify a suspect
- Use memory dumps and the Volatility tool to determine an attacker’s activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network
- Gain access to a target machine using Metasploit, and then detect the artifacts and impacts of exploitation through process, file, memory, and log analysis
- Analyse a system to see how attackers use the Netcat tool to move files, create backdoors, and build relays through a target environment

“Very structured and well prepared course. Interesting and engaging for people new to the field as well as experienced professionals”

Ewe konkolska
PRUDENTIAL

GIAC CERT: GCIH
37 CPE/CMU CREDITS
WWW.GIAC.ORG/GCIH
Web App Penetration Testing and Ethical Hacking

Web applications play a vital role in every modern organisation. However, if your organisation doesn’t properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organisations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

SEC542 helps students move beyond push-button scanning to professional, thorough, and high-value web application penetration testing. Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organisation. Unfortunately, there is no “patch Tuesday” for custom web applications, and major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defence requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

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

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn. In addition to having more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way that hammers home lessons learned.

Who should attend
- General security practitioners
- Penetration testers
- Ethical hackers
- Web application developers
- Website designers and architects

You will be able to...
- Apply a detailed, four-step methodology to your web application penetration tests: reconnaissance, mapping, discovery, and exploitation
- Analyse the results from automated web testing tools to validate findings, determine their business impact, and eliminate false positives
- Manually discover key web application flaws
- Use Python to create testing and exploitation scripts during a penetration test
- Discover and exploit SQL injection flaws to determine true risk to the victim organisation
- Create configurations and test payloads within other web attacks
- Fuzz potential inputs for injection attacks
- Explain the impact of exploitation of web application flaws
- Analyse traffic between the client and the server application using tools such as the Zed Attack Proxy and Burp Suite to find security issues within the client-side application code
- Manually discover and exploit Cross-Site Request Forgery (CSRF) attacks
- Use the Browser Exploitation Framework (BeEF) to hook victim browsers, attack client software and the network, and evaluate the potential impact that XSS flaws have within an application
- Perform a complete web penetration test during the Capture the Flag exercise to bring techniques and tools together into a comprehensive test

“CTF is a great way to practice the course content, really enjoyed it.”
Chris Campbell, RBS
Developing the next generation of cybersecurity leaders.

Master’s Degrees

**Designed for Working Professionals**
Earn your degree in 3 to 5 years while continuing to work full-time.

**Attend Online and In-Person**
Choose from online courses and week-long, intensive live training options available throughout the world.

**Earn GIAC Certifications**
Validate your skills with industry-recognized credentials, earned throughout the program.

**Enter with Advanced Standing**
Apply past SANS training classes and GIAC certifications towards your degree.

Graduate Certificates

**Sharpen Your Skills**
Keep your knowledge and skills current with short, technically-focused programs.

**Complete in 18 to 24 Months**
Choose the pace that comfortably meets your personal and career demands.

**Multiple Focus Areas**
Cybersecurity Engineering (Core), Cyber Defense Operations, Penetration Testing and Ethical Hacking, Incident Response

**Cyber Range Capstone**
Test your hands-on skills in the NetWars Continuous exercise.

“I joined the master’s degree program with the expectation that the technical content from SANS would be great. And it more than met my expectations. To be honest though, I was shocked at how important I found the management courses. They complement the technical content perfectly. In the end, that combination is what really pushed me forward and turbocharged my career.”

– Philip Bosco, MSISE
Principal Security Consultant, Cylance

LEARN MORE AT SANS.EDU
As a cybersecurity professional, you have a unique responsibility to find and understand your organisation's vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this task head-on.

SEC560 is the must-have course for every well-rounded security professional. With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step-by-step and end-to-end. Every organisation needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with more than 30 detailed hands-on labs throughout. The course is chock-full of practical, real-world tips from some of the world’s best penetration testers to help you do your job safely, efficiently…and masterfully.

Learn the best ways to test your own systems before the bad guys attack.
SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test – and on the last day of the course you’ll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You’ll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organisation, demonstrating the knowledge you’ve mastered in this course.

You will bring comprehensive penetration testing and ethical hacking know-how back to your organisation.
You will learn how to perform detailed reconnaissance, studying a target’s infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won’t just cover run-of-the-mill options and configurations, we’ll also go over the lesser known but super-useful capabilities of the best pen test toolsets available today. After scanning, you’ll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You’ll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasise the importance of defence in depth.

“IT introduces the whole process of pen testing from start of engagement to end.”
Barry Tsang, Deloitte

Who should attend?
- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red and blue team members
- Forensics specialists who want to better understand offensive tactics

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 a scanning tool such as Nmap to conduct comprehensive network sweeps, port scans, OS fingerprinting, and version scanning to develop a map of target environments
- Choose and properly execute Nmap Scripting Engine scripts to extract detailed information from target systems Configure and launch a vulnerability scanner such as Nessus so that it safely discovers vulnerabilities through both authenticated and unauthenticated scans, and customise the output from such tools to represent the business risk to the organisation
- Analyse the output of scanning tools to eliminate false positive reduction with tools including Netcat and Scapy Utilise the Windows PowerShell and Linux bash command lines during post-exploitation to plunder target systems for vital information that can further overall penetration test progress, establish pivots for deeper compromise, and help determine business risks
To be a top penetration testing professional, you need fantastic hands-on skills for finding, exploiting and resolving vulnerabilities. Top instructors at SANS engineered SEC561: Immersive Hands-On Hacking Techniques from the ground up to help you get good fast. The course teaches in-depth security capabilities through 80%+ hands-on exercises, maximising keyboard time during in-class labs and making this SANS’s most hands-on course ever. With over 30 hours of intense labs, students experience a leap in their capabilities, as they come out equipped with the practical skills needed to handle today’s pen test and vulnerability assessment projects in enterprise environments. Throughout the course, an expert instructor coaches students as they work their way through solving increasingly demanding real-world information security scenarios using skills that they will be able to apply the day they get back to their jobs.

People often talk about these concepts, but this course teaches you how to actually do them hands-on and in-depth. SEC561 shows penetration testers, vulnerability assessment personnel, auditors, and operations personnel how to leverage in-depth techniques to get powerful results in every one of their projects. The course is overflowing with practical lessons and innovative tips, all with direct hands-on application. Throughout the course, students interact with brand new and custom-developed scenarios built just for this course on the innovative NetWars challenge infrastructure, which guides them through the numerous hands-on labs providing questions, hints, and lessons learned as they build their skills.

Topics addressed in the course include:
- Applying network scanning and vulnerability assessment tools to effectively map out networks and prioritise discovered vulnerabilities for effective remediation
- Manipulating common network protocols to reconfigure internal network traffic patterns, as well as defences against such attacks
- Analyzing Windows and Linux systems for weaknesses using the latest enterprise management capabilities of the operating systems, including the super-powerful Windows Remote Management (WinRM) tools
- Applying cutting-edge password analysis tools to identify weak authentication controls leading to unauthorised server access
- Scouring through web applications and mobile systems to identify and exploit devastating developer flaws
- Evading anti-virus tools and bypassing Windows User Account Control to understand and defend against these advanced techniques
- Honing phishing skills to evaluate the effectiveness of employee awareness initiatives and your organisation’s exposure to one of the most damaging attack vectors widely used today

"This training changed my perspective of IT and taught me how to think outside of the box.”

Timothy Mckenzie,
DELL/SECUREWORKS

Who should attend?
- Security professionals who want to expand their hands-on technical skills in new analysis areas such as packet analysis, digital forensics, vulnerability assessment, system hardening, and penetration testing
- Systems and network administrators who want to gain hands-on experience in information security skills to become better administrators
- Incident response analysts who want to better understand system attack and defence techniques
- Forensic analysts who need to improve their analysis through experience with real-world attacks
- Penetration testers seeking to gain practical experience for use in their own assessments
- Red team members who want to build their hands-on skills

You will be able to...
- Use network scanning and vulnerability assessment tools to effectively map out networks and prioritise discovered vulnerabilities for effective remediation
- Use password analysis tools to identify weak authentication controls leading to unauthorised server access
- Evaluate web applications for common developer flaws leading to significant data loss conditions
- Manipulate common network protocols to maliciously reconfigure internal network traffic patterns
- Identify weaknesses in modern anti-virus signature and heuristic analysis systems
- Inspect the configuration deficiencies and information disclosure threats present on Windows and Linux servers
- Bypass authentication systems for common web application implementations
- Exploit deficiencies in common cryptographic systems
- Bypass monitoring systems by leveraging IPv6 scanning and exploitation tools
- Harvest sensitive mobile device data from iOS and Android targets

“SANS TRAINING CATALOGUE, 2018
PRIVATE TRAINING
36 CPE/CMU CREDITS
SANS TRAINING CATALOGUE, 2018
39
SEC 573

HANDS-ON • SIX DAYS • LAPTOP REQUIRED

Automating Information Security with Python

All security professionals, including Penetration Testers, Forensics Analysts, Network Defenders, Security Administrators, and Incident Responders, have one thing in common: CHANGE. Change is constant. Technology, threats, and tools are constantly evolving. If we don’t evolve with them, we’ll become ineffective and irrelevant, unable to provide the vital defences our organisations increasingly require.

Maybe your chosen Operating System has a new feature that creates interesting forensics artifacts that would be invaluable for your investigation, if only you had a tool to access it. Often for new features and forensics artifacts, no such tool has yet been released. You could try moving your case forward without that evidence or hope that someone creates a tool before the case goes cold… or you can write a tool yourself.

Or, perhaps an attacker bypassed your defences and owned your network months ago. If existing tools were able to find the attack, you wouldn’t be in this situation. You are bleeding sensitive data and the time-consuming manual process of finding and eradicating the attacker is costing you money and hurting your organisation big time. The answer is simple if you have the skills: Write a tool to automate your defences.

Or, as a Penetration tester, you need to evolve as quickly as the threats you are paid to emulate. What do you do when “off-the-shelf” tools and exploits fall short? If you’re good, you write your own tool.

Writing a tool is easier said than done, right? Not really. Python is a simple, user-friendly language that is designed to make automating tasks that security professionals perform quick and easy. Whether you are new to coding or have been coding for years, SEC573: Automating Information Security with Python will have you creating programs to make your job easier and make you more efficient. This self-paced class starts from the very beginning assuming you have no prior experience or knowledge of programming. We cover all of the essentials like variables, loops, if then else, logic, file operations, exception handling, object-oriented coding and more.

This course is designed to give you the skills you need for tweaking, customising, or outright developing your own tools. We put you on the path of creating your own tools, empowering you in automating the daily routine of today’s information security professional, and achieving more value in less time. Again and again, organisations serious about security emphasise their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it. Join us and learn Python in-depth and fully weaponised.

Who should attend?

• Security professionals who want to learn how to develop Python applications
• Penetration testers who want to move from being a consumer of security tools to being the creator of security tools
• Technologists who need custom tools to test their infrastructure and who want to create those tools themselves

You will be able to...

• Develop forensics tool to carve artifacts from forensics evidence for which no other tool exists or use third-party modules for well-known artifacts to hidden evidence relevant to your investigations
• Create defensive tools to automate the analysis of log file and network packets using hunt team techniques to track down attackers in your network. Implement custom whitelisting, blacklisting, signature detection, long tail and short tail analysis, and other data analysis techniques to find attacks overlooked by conventional methods
• Write penetration testing tools including several backdoors with features like process execution, upload and download payloads, port scanning and more. Build essential tools that evade antivirus software and allow you to establish that required foothold inside your target
• Understand Python coding fundamentals required to automate common information security tasks. Language essentials like variables, loops, if then else, logic, file operations, command line arguments, debugging are all covered assuming no prerequisite knowledge
• Tap into the wealth of existing Python modules to complete tasks using Regular Expressions, Database interactions with SQL, IP Networking, Exception handling, Interact with websites using Requests, Packet Analysis, Packet reassembly techniques and much more.

UNIVERSITY-CREDIT-ELIGIBLE

Giac Cert: GPYC
36 CPE/CMU CREDITS
WWW.GIAC.ORG/GPYC

SANS TRAINING CATALOGUE, 2018
Imagine an attack surface spread throughout your organisation and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports numerous different wireless technologies all ripe for attack. You don’t need to imagine any further because this already exists today: mobile devices. These devices are the biggest attack surface in most organisations, yet these same organisations often don’t have the skills needed to assess them. Mobile devices are no longer a convenience technology: they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores throughout the world. Users rely on mobile devices more today than ever before – we know it, and the bad guys do too.

This course is designed to give you the skills you need to understand the security strengths and weaknesses in Apple iOS, Android, and wearable devices including Apple Watch and Android Wear. With these skills, you will evaluate the security weaknesses of built-in and third-party applications. You’ll learn how to bypass platform encryption, and how to manipulate Android apps to circumvent obfuscation techniques. You’ll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You’ll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS devices, and you’ll exploit lost or stolen devices to harvest sensitive mobile application data. Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you’ll review the ways in which we can effectively communicate threats to key stakeholders. You’ll leverage tools including Mobile App Report Cards to characterise threats for management and decision-makers, while identifying sample code and libraries that developers can use to address risks for in-house applications as well.

You’ll then use your new skills to apply a mobile device deployment penetration test in a step-by-step fashion. Starting with gaining access to wireless networks to implement man-in-the-middle attacks and finishing with mobile device exploits and data harvesting, you’ll examine each step in conducting such a test with hands-on exercises, detailed instructions, and tips and tricks learned from hundreds of successful penetration tests. By building these skills, you’ll return to work prepared to conduct your own test, and you’ll be better informed about what to look for and how to review an outsourced penetration test. Mobile device deployments introduce new threats to organisations including advanced malware, data leakage, and the disclosure of enterprise secrets, intellectual property, and personally identifiable information assets to attackers. Further complicating matters, there simply are not enough people with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you’ll be able to differentiate yourself as being prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test – all critical skills to protect and defend mobile device deployments.

Who should attend?
- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing, deploying or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets

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
- Change the functionality of Android and iOS apps to defeat anti-jailbreaking or circumvent in-app purchase requirements
- 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 behavior of mobile applications to bypass security restrictions

“I am learning a lot regarding mobile platforms and key differences between all of them. I recommend this course for anyone that wants to learn about mobile OS.”

Hilal Lootah, TRA
Despite the security concerns many of us share regarding wireless technology, it is here to stay. In fact, not only is wireless here to stay, it is growing in deployment and utilisation with wireless LAN technology and WiFi as well as other applications, including cordless telephones, smart homes, embedded devices, and more. Technologies like ZigBee and Z-Wave offer new methods of connectivity to devices, while other wireless technology, including WiFi, Bluetooth, Bluetooth Low Energy, and DECT, continue their massive growth rate, each introducing its own set of security challenges and attacker opportunities.

To be a wireless security expert, you need to have a comprehensive understanding of the technology, threats, exploits, and defensive techniques along with hands-on experience in evaluating and attacking wireless technology. Not limiting your skill-set to WiFi, you’ll need to evaluate the threat from other standards-based and proprietary wireless technologies as well. This course takes an in-depth look at the security challenges of many different wireless technologies, exposing you to wireless security threats through the eyes of an attacker.

Using readily available and custom-developed tools, you’ll navigate your way through the techniques attackers use to exploit WiFi networks, including attacks against WEP, WPA/WPA2, PEAP, TTLS, and other systems. You’ll also develop attack techniques leveraging Windows 7 and Mac OS X. We’ll examine the commonly overlooked threats associated with Bluetooth, ZigBee, DECT, and proprietary wireless systems. As part of the course, you’ll receive the SWAT Toolkit, which will be used in hands-on labs to back up the course content and reinforce wireless ethical hacking techniques.

Using assessment and analysis techniques, this course will show you how to identify the threats that expose wireless technology and build on this knowledge to implement defensive techniques that can be used to protect wireless systems.

**Who should attend?**
- Ethical hackers and penetration testers
- Network security staff
- Network and system administrators
- Incident response teams
- Information security policy decision-makers
- Technical auditors
- Information security consultants
- Wireless system engineers
- Embedded wireless system developers

**You will be able to...**
- Identify and locate malicious rogue access points using free and low-cost tools
- Conduct a penetration test against low-power wireless including ZigBee to identify control system and related wireless vulnerabilities
- Identify vulnerabilities and bypass authentication mechanisms in Bluetooth networks using Ubertooth, Car Whisperer, and btaptap to collect sensitive information from headsets, wireless keyboards and Bluetooth LAN devices
- Utilise wireless capture tools to extract audio conversations and network traffic from DECT wireless phones to identify information disclosure threats exposing the organisation
- Implement an enterprise WPA2 penetration test to exploit vulnerable wireless client systems for credential harvesting
- Utilise wireless fuzzing tools including Metasploit file2air, and Scapy to identify new vulnerabilities in wireless devices
SEC 642

HANDS-ON • SIX DAYS • LAPTOP REQUIRED

Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

Can Your Web Apps Withstand the Onslaught of Modern Advanced Attack Techniques?
Modern web applications are growing more sophisticated and complex as they utilise exciting new technologies and support ever more critical operations. Long gone are the days of basic HTML requests and responses. Even in the age of Web 2.0 and AJAX, the complexity of HTTP and modern web applications is progressing at breathtaking speed. With the demands of highly available web clusters and cloud deployments, web applications are looking to deliver more functionality in smaller packets, with a decreased strain on backend infrastructure. Welcome to an era that includes tricked-out cryptography, WebSockets, HTTP/2, and a whole lot more. Are your web application assessment and penetration testing skills ready to evaluate these impressive new technologies and make them more secure?

Are You Ready to Put Your Web Apps to the Test with Cutting-Edge Skills?
This pen testing course is designed to teach you the advanced skills and techniques required to test modern web applications and next-generation technologies. The course uses a combination of lecture, real-world experiences, and hands-on exercises to teach you the techniques to test the security of tried-and-true internal enterprise web technologies, as well as cutting-edge Internet-facing applications. The final course day culminates in a Capture-the-Flag competition, where you will apply the knowledge you acquired during the previous five days in a fun environment based on real-world technologies.

Hands-on Learning of Advanced Web App Exploitation Skills
We begin by exploring advanced techniques and attacks to which all modern-day complex applications may be vulnerable. We'll learn about new web frameworks and web backends, then explore encryption as it relates to web applications, digging deep into practical cryptography used by the web, including techniques to identify the type of encryption in use within the application and methods for exploiting or abusing it. We'll look at alternative front ends to web applications and web services such as mobile applications, and examine new protocols such as HTTP/2 and WebSockets. The final portion of the class will focus on how to identify and bypass web application firewalls, filtering, and other protection techniques.

Who should attend?
- Web penetration testers
- Red team members
- Vulnerability assessment personnel
- Network penetration testers
- Security consultants
- Developers
- QA testers
- System administrators
- IT managers
- System architects

You will be able to...
- Perform advanced Local File Include (LFI)/ Remote File Include (RFI), Blind SQL injection (SQLi), and Cross-Site Scripting (XSS) combined with Cross-Site Request Forger (XSRF) discovery and exploitation
- Exploit advanced vulnerabilities common to most backend language like Mass Assignments, Type Juggling, and Object Serialisation
- Perform JavaScript-based injection against ExpressJS, Node.js, and NoSQL
- Understand the special testing methods for content management systems such as SharePoint and WordPress
- Identify and exploit encryption implementations within web applications and frameworks
- Discover XML Entity and XPath vulnerabilities in SOAP or REST web services and other datastores
- Use tools and techniques to work with and exploit HTTP/2 and Web Sockets
- Identify and bypass Web Application Firewalls and application filtering techniques to exploit the system

“Very good techniques and methods covered which will be useful to any new app tester.”
Vivek Veerappan,
GEMALTO

“Hands-on and to the point!”
Frans Kollé,
MADISON GUKIRKA B.V.

36 CPE/CMU CREDITS

SANS TRAINING CATALOGUE, 2018
This course is designed as a logical progression point for those who have completed SEC560: Network Penetration Testing and Ethical Hacking, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered includes weaponising Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, return-oriented programming (ROP), Windows exploit-writing, and much more!

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, you need a strong desire to learn, the support of others, and the opportunity to practice and build experience. SEC660 provides attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios. This course goes far beyond simple scanning for low-hanging fruit, and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

SEC660 starts off by introducing the advanced penetration concept, and provides an overview to help prepare students for what lies ahead. The focus of day one is on network attacks, an area often left untouched by testers. Topics include accessing, manipulating, and exploiting the network. Attacks are performed against NAC, VLANs, OSPF, 802.1X, CDP, IPv6, VOIP, SSL, ARP, SNMP, and others. Day two starts off with a technical module on performing penetration testing against various cryptographic implementations. The rest of the day is spent on network booting attacks, escaping Linux restricted environments such as chroot, and escaping Windows restricted desktop environments. Day three jumps into an introduction of Python for penetration testing, Scapy for packet crafting, product security testing, network and application fuzzing, and code coverage techniques. Days four and five are spent exploiting programs on the Linux and Windows operating systems. You will learn to identify privileged programs, redirect the execution of code, reverse-engineer programs to locate vulnerable code, obtain code execution for administrative shell access, and defeat modern operating system controls such as ASLR, canaries, and DEP using ROP and other techniques. Local and remote exploits, as well as client-side exploitation techniques, are covered. The final course day is dedicated to numerous penetration testing challenges requiring you to solve complex problems and capture flags.

Who should attend?

- Network and systems penetration testers
- Incident handlers
- Application developers
- IDS engineers

You will be able to...

- Perform fuzz testing to enhance your company’s SDL process
- Exploit network devices and assess network application protocols
- Escape from restricted environments on Linux and Windows
- Test cryptographic implementations Model the techniques used by attackers to perform 0-day vulnerability discovery and exploit development
- Develop more accurate quantitative and qualitative risk assessments through validation
- Demonstrate the needs and effects of leveraging modern exploit mitigation controls
- Reverse-engineer vulnerable code to write custom exploits

“From high-level concepts to hands-on training, this course provides enough detail and depth to allow me to show the skillsets learned immediately after the learning, allowing my employer to see their return on investment.”

Brian Anderson,
NORTHROP GRUMMAN CORP
Advanced Exploit Development for Penetration Testers

Vulnerabilities in modern operating systems such as Microsoft Windows 7/8, Server 2012, and the latest Linux distributions are often very complex and subtle. Yet these vulnerabilities could expose organisations to significant attacks, undermining their defences when attacked by very skilled adversaries. Few security professionals have the skillset to discover let alone even understand at a fundamental level why the vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity. SEC760: Advanced Exploit Development for Penetration Testers teaches the skills required to reverse-engineer 32- and 64-bit applications, perform remote user application and kernel debugging, analyse patches for one-day exploits, and write complex exploits, such as use-after-free attacks, against modern software and operating systems.

**Who should attend?**
- Senior network and system penetration testers
- Secure application developers (C & C++)
- Reverse-engineering professionals
- Senior incident handlers
- Senior threat analysts
- Vulnerability researchers
- Security researchers

**You will be able to...**
- Discover zero-day vulnerabilities in programs running on fully-patched modern operating systems
- Create exploits to take advantage of vulnerabilities through a detailed penetration testing process
- Use the advanced features of IDA Pro and write your own IDC and IDA Python scripts
- Perform remote debugging of Linux and Windows applications
- Understand and exploit Linux heap overflows Write return-oriented shellcode
- Perform patch diffing against programs, libraries, and drivers to find patched vulnerabilities
- Perform Windows heap overflows and use-after-free attacks
- Use precision heap sprays to improve exploitability
- Perform Windows Kernel debugging up through Windows 8 64-bit
- Jump into Windows kernel exploitation

**Some of the skills you will learn in SEC760 include:**
- How to write modern exploits against the Windows 7/8/10 operating systems
- How to perform complex attacks such as use-after-free, Kernel exploit techniques, one-day exploitation through patch analysis, and other advanced topics
- The importance of utilising a Security Development Lifecycle (SDL) or Secure SDLC, along with Threat Modeling
- How to effectively utilise various debuggers and plug-ins to improve vulnerability research and speed
- How to deal with modern exploit mitigation controls aimed at thwarting success and defeating determination

"SEC760 is a kind of training we could not get anywhere else"

Jenny Kitaichit, INTEL
All organisations must prepare for cyber crime occurring on their computer systems and within their networks. Demand has never been greater for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world’s best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

FOR500: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can’t protect what you don’t understand, and understanding forensic capabilities and artifacts is a core component of information security. You’ll learn to recover, analyse, and authenticate forensic data on Windows systems. You’ll understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. You’ll be able to use your new skills to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR500 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyse everything from legacy Windows XP systems to just-discovered Windows 10 artifacts. FOR500 is continually updated.

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

“Course is very up to date and challenges existing ideas to help become a better investigator. Course is well prepared.”
Frank Visser, PWC

Who should attend?
• Information security professionals
• Incident response team members
• Law enforcement officers, federal agents, and detectives
• Media exploitation analysts
• Anyone interested in a deep understanding of Windows forensics

You will be able to...
• Perform proper Windows forensic analysis by applying key techniques focusing on Windows 7/8/10
• Use full-scale forensic tools and analysis methods to detail nearly every action a suspect accomplished on a Windows system, including who placed an artifact on the system and how, program execution, file/folder opening, geo-location, browser history, profile USB device usage, and more
• Uncover the exact time that a specific user last executed a program through Registry and Windows artifact analysis, and understand how this information can be used to prove intent in cases such as intellectual property theft, hacker-breached systems, and traditional crimes
• Determine the number of times files have been opened by a suspect through browser forensics, shortcut file analysis (LNK), e-mail analysis, and Windows Registry parsing
• Identify keywords searched by a specific user on a Windows system in order to pinpoint the files and information the suspect was interested in finding and accomplish detailed damage assessments
• Use Windows shellbags analysis tools to articulate every folder and directory that a user opened up while browsing local, removable, and network drives
• Determine each time a unique and specific USB device was attached to the Windows system, the files and folders that were accessed on it, and who plugged it in by parsing key Windows artifacts such as the Registry and log files
FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting will help you to:

• Detect how and when a breach occurred
• Identify compromised and affected systems
• Contain and remediate incidents
• Develop key sources of threat intelligence
• Hunt down additional breaches using knowledge of the adversary

DAY 0: A government agency contacts you to say an advanced threat group is targeting organisations like yours, and that your organisation is likely a target. They won’t tell how they know, but they suspect that there are already several breached systems within your enterprise. An advanced persistent threat, aka an APT, is likely involved. This is the most sophisticated threat that you are likely to face in your efforts to defend your systems and data, and these adversaries may have been actively rummaging through your network undetected for months or even years.

This is a hypothetical situation, but the chances are very high that hidden threats already exist inside your organisation’s networks. Organisations can’t afford to believe that their security measures are perfect and impenetrable, no matter how thorough their security precautions might be. Prevention systems alone are insufficient to counter focused human adversaries who know how to get around most security and monitoring tools.

This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and hacktivism. Constantly updated, FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting addresses today’s incidents by providing hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to detect, counter, and respond to real-world breach cases.

“...and this course has given me everything I need to do just that.”

Simon Fowler,
VIRGIN MEDIA
Mac Forensic Analysis

Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are familiar with Windows-only machines.

Times and trends change and forensic investigators and analysts need to change with them. The new FOR518: Mac Forensic Analysis course provides the tools and techniques necessary to take on any Mac case without hesitation.

The intense hands-on forensic analysis skills taught in the course will enable Windows-based investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyse any Mac or iOS system.

FOR518: Mac Forensic Analysis will teach you:

- Mac Fundamentals: How to analyse and parse the Hierarchical File System (HFS+) by hand and recognise the specific domains of the logical file system and Mac-specific file types.
- User Activity: How to understand and profile users through their data files and preference configurations.
- Advanced Analysis and Correlation: How to determine how a system has been used or compromised by using the system and user data files in correlation with system log files.
- Mac Technologies: How to understand and analyse many Mac-specific technologies, including Time Machine, Spotlight, iCloud, Versions, FileVault, AirDrop, and FaceTime.

FOR518: Mac Forensic Analysis aims to form a well-rounded investigator by introducing Mac forensics into a Windows-based forensics world. This course focuses on topics such as the HFS+ file system, Mac-specific data files, tracking user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac exclusive technologies. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac forensics case.

Who should attend?

- Experienced digital forensic analysts who want to solidify and expand their understanding of file system forensics and advanced Mac analysis
- Law enforcement officers, federal agents, or detectives who want to master advanced computer forensics and expand their investigative skill set
- Media exploitation analysts who need to know where to find the critical data they need from a Mac system
- Incident response team members who are responding to complex security incidents/intrusions from sophisticated adversaries and need to know what to do when examining a compromised system
- Information security professionals who want to become knowledgeable with Mac OS X and iOS system internals
- SANS FOR500 (formerly FOR408), FOR508, FOR526, FOR585, and FOR610 alumni looking to round out their forensic skills

You will be able to...

- Parse the HFS+ file system by hand, using only a cheat sheet and a hex editor
- Determine the importance of each file system domain
- Conduct temporal analysis of a system by correlating data files and log analysis
- Profile individuals’ usage of the system, including how often they used it, what applications they frequented, and their personal system preferences
- Determine remote or local data backups, disk images, or other attached devices
- Find encrypted containers and FileVault volumes, understand keychain data, and crack Mac passwords
- Analyse and understand Mac metadata and their importance in the Spotlight database, Time Machine, and Extended Attributes
- Develop a thorough knowledge of the Safari Web Browser and Apple Mail applications

“Best Mac forensics course available.”

David Klopp, J.P.MORGAN

“The depth of time exercise was outstanding. One can tell the amount of work that went into it.”

Gary Titus, STROZ FRIEDBERG LLC

36 CPE/CMU CREDITS

SANS TRAINING CATALOGUE, 2018
FOR526: Memory Forensics In-Depth provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and analyse captured memory images. The course uses the most effective freeware and open-source tools in the industry today and provides an in-depth understanding of how these tools work. FOR526 is a critical course for any serious DFIR investigator who wants to tackle advanced forensics, trusted insider, and incident response cases. In today’s forensics cases, it is just as critical to understand memory structures as it is to understand disk and registry structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the case at hand. For those investigating platforms other than Windows, this course also introduces OSX and Linux memory forensics acquisition and analysis using hands-on lab exercises.

There is an arms race between analysts and attackers. Modern malware and post-exploitation modules increasingly employ self-defence techniques that include more sophisticated rootkit and anti-memory analysis mechanisms that destroy or subvert volatile data. Examiners must have a deeper understanding of memory internals in order to discern the intentions of attackers or rogue trusted insiders. FOR526 draws on best practices and recommendations from experts in the field to guide DFIR professionals through acquisition, validation, and memory analysis with real-world and malware-laden memory images.

FOR526: Memory Forensics In-Depth will teach you:
- Proper Memory Acquisition: Demonstrate targeted memory capture ensuring data integrity and overcome obstacles to acquisition/anti-acquisition behaviors
- How to Find Evil in Memory: Detect rogue, hidden, and injected processes, kernel-level rootkits, Dynamic Link Libraries (DLL) hijacking, process hollowing, and sophisticated persistence mechanisms
- Effective Step-by-Step Memory Analysis Techniques: Use process timelining, high-low level analysis, and walking the Virtual Address Descriptors (VAD) tree to spot anomalous behavior
- Best Practice Techniques: Learn when to implement triage, live system analysis, and alternative acquisition techniques and how to devise custom parsing scripts for targeted memory analysis

Who should attend?
- Incident Response Team members who regularly respond to complex security incidents/intrusions and would like to know how memory forensics will expand their reach.
- Experienced Digital Forensic Analysts who want to consolidate and expand their understanding of memory forensics.
- Red Team Members, Penetration Testers, and Exploit Developers who want to learn how their opponents can identify their actions.
- Law enforcement officers, federal agents, or detectives who want to become a deep subject-matter expert on memory forensics.
- SANS FOR508 and SEC504 Graduates looking to take their memory forensics skills to the next level.
- Forensics Investigators working in organizations where memory is regularly obtained by first responders, and who want to raise the bar by analyzing the images.

“This training opened my eyes to the need to collect memory images, as well as physical images for single computer analysis, such as theft of IP or other employee investigations.”

Greg Caouette, KROLL
FOR 572

HANDS-ON • SIX DAYS • LAPTOP REQUIRED

Advanced Network Forensics and Analysis

Take your system-based forensic knowledge onto the wire. Incorporate network evidence into your investigations, provide better findings, and get the job done faster. It is exceedingly rare to work any forensic investigation that doesn’t have a network component. Endpoint forensics will always be a critical and foundational skill for this career, but overlooking their network communications is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, uncover attackers that have been active for months or longer, or even prove useful in definitively proving a crime actually occurred.

FOR572: Advanced Network Forensics and Analysis was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of compromised computer system drops to almost zero. Put another way: Bad guys are talking over the network. Without command-and-control and data extraction channels, the value of compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of compromised computer system drops to almost zero. Put another way: Bad guys are talking over the network.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence as well as how to place new collection platforms while an incident is already under way.

Whether you are a consultant responding to a client’s site, a law enforcement professional assisting victims of cybercrime and seeking prosecution of those responsible, an on-staff forensic practitioner, or a member of the growing ranks of “threat hunters”, this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS SEC curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS Forensics alumni from FOR500 (formerly FOR408) and FOR508 can take their existing knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same caliber of real-world problems without the use of disk or memory images.

Who should attend?
- Incident response team members and forensicators
- Hunt team members
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- Anyone interested in computer network intrusions and investigations
- Security Operations Center personnel and information security practitioners

You will be able to...
- Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis or definitive data loss determination
- Use historical NetFlow data to identify relevant past network occurrences, allowing accurate incident scoping
- Reverse-engineer custom network protocols to identify an attacker’s command-and-control abilities and actions
- Decrypt captured SSL traffic to identify attackers’ actions and what data they extracted from the victim
- Use data from typical network protocols to increase the fidelity of the investigation’s findings
- Identify opportunities to collect additional evidence based on the existing systems and platforms within a network architecture
- Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation
- Incorporate log data into a comprehensive analytic process, filling knowledge gaps that may be far in the past
- Learn how attackers leverage man-in-the-middle tools to intercept seemingly secure communications
- Examine proprietary network protocols to determine what actions occurred on the endpoint systems
- Analyse wireless network traffic to find evidence of malicious activity
Make no mistake: current network defence, threat hunting, and incident response practices contain a strong element of intelligence and counterintelligence that cyber analysts must understand and leverage in order to defend their networks, proprietary data, and organisations.

FOR578: Cyber Threat Intelligence will help network defenders, threat hunting teams, and incident responders to:

- Understand and develop skills in tactical, operational, and strategic-level threat intelligence
- Generate threat intelligence to detect, respond to, and defeat advanced persistent threats (APTs)
- Validate information received from other organisations to minimize resource expenditures on bad intelligence
- Leverage open-source intelligence to complement a security team of any size
- Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX

The collection, classification, and exploitation of knowledge about adversaries — collectively known as cyber threat intelligence — gives network defenders information superiority that is used to reduce the adversary’s likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture.

Cyber threat intelligence thus represents a force multiplier for organisations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats. Malware is an adversary’s tool but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders.

During a targeted attack, an organisation needs a top-notch and cutting-edge threat hunting or incident response team armed with the threat intelligence necessary to understand how adversaries operate and to counter the threat. FOR578: Cyber Threat Intelligence will train you and your team in the tactical, operational, and strategic-level cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, and organisations more aware of the evolving threat landscape.

Who should attend?

- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Security Operations Center personnel and information security practitioners
- Federal agents and law enforcement officials
- SANS FOR500 (formerly FOR408), FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

“Fantastic class! I love the way the terminology was covered. I will be making index cards to ensure I have them memorised.”

Nate DeWitt,
EBAY

“I am new to CTI and this course was really well put together to cater for people with different levels of expertise”

Ben Hargreaves,
PWC
Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, and more. Understanding how to leverage the data from the device in a correct manner can make or break your case and your future as an expert. FOR585: Advanced Smartphone Forensics will teach you those skills.

Every time the smartphone “thinks” or makes a suggestion, the data are saved. It’s easy to get mixed up in what the forensic tools are reporting. Smartphone forensics is more than pressing the “find evidence” button and getting answers. Your team cannot afford to rely solely on the tools in your lab. You have to understand how to use them correctly to guide your investigation, instead of just letting the tool report what it believes happened on the device. It is impossible for commercial tools to parse everything from smartphones and understand how the data were put on the device. Examining and interpreting the data is your job, and this course will provide you and your organisation with the capability to find and extract the correct evidence from smartphones with confidence.

This in-depth smartphone forensics course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 17 hands-on labs that allow students to analyse different datasets from smart devices and leverage the best forensic tools and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools. Each lab is designed to teach you a lesson that can be applied to other smartphones. You will gain experience with the different data formats on multiple platforms and learn how the data are stored and encoded on each type of smart device. The labs will open your eyes to what you are missing by relying 100% on your forensic tools.

FOR585 is continuously updated to keep up with the latest malware, smartphone operating systems, third-party applications, and encryption. This intensive six-day course offers the most unique and current instruction available, and it will arm you with mobile device forensic knowledge you can apply immediately to cases you’re working on the day you finish the course.

Smartphone technologies are constantly changing, and most forensic professionals are unfamiliar with the data formats for each technology. Take your skills to the next level: it’s 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!

“The best part about Advanced Smartphone Forensics is it provides real world technologies for forensically investigating devices without the typical point and click approaches.”

Brad Wardman, PAYPAL
Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Learn to turn malware inside out! This popular 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 many other freely available tools.

The course begins by establishing the foundation for analyzing malware in a way that dramatically expands upon the findings of automated analysis tools. You will learn how to set up a flexible laboratory to examine the inner workings of malicious software, and how to use the lab to uncover characteristics of real-world malware samples. You will also learn how to redirect and intercept network traffic in the lab to explore the specimen’s capabilities by interacting with the malicious program.

Malware is often obfuscated to hinder analysis efforts, so the course will equip you with the skills to unpack executable files. You will learn how to dump such programs from memory with the help of a debugger and additional specialised tools, and how to rebuild the files’ structure to bypass the packer’s protection. You will also learn how to examine malware that exhibits rootkit functionality to conceal its presence on the system, employing code analysis and memory forensics approaches to examining these characteristics.

FOR610 malware analysis training also teaches how to handle malicious software that attempts to safeguard itself from analysis. You will learn how to recognise and bypass common self-defensive measures, including code injection, sandbox evasion, flow misdirection, and other measures.

Hands-on workshop exercises are a critical aspect of this course. They enable you to apply malware analysis techniques by examining malicious software in a controlled and systematic manner. When performing the exercises, you will study the supplied specimens’ behavioral patterns and examine key portions of their code. To support these activities, you will receive pre-built Windows and Linux virtual machines that include tools for examining and interacting with malware.

“IT really gives a nice realistic guidance on how to approach complex problems in Malware Analysis.”
Markus Jeckeln, LUFTHANSA

Who should attend?
• Individuals who have dealt with incidents involving malware and want to learn how to understand key aspects of malicious programs
• Technologists who have informally experimented with aspects of malware analysis prior to the course and are looking to formalize and expand their expertise in this area
• Forensic investigators and IT practitioners looking to expand their skillsets and learn how to play a pivotal role in the incident response process

You will be able to...
• Build an isolated, controlled laboratory environment for analyzing code and behavior of malicious programs
• Employ network and system-monitoring tools to examine how malware interacts with the file system, registry, network, and other processes in a Windows environment
• Uncover and analyse malicious JavaScript and VBScript components of web pages, which are often used by exploit kits for drive-by attacks
• Control relevant aspects of the malicious program’s behavior through network traffic interception and code patching to perform effective malware analysis
• Use a disassembler and a debugger to examine the inner-workings of malicious Windows executables
• Bypass a variety of packers and other 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 and anti-analysis measures
• Assess the threat associated with malicious documents, such as PDF and Microsoft Office files, in the context of targeted attacks
• Derive Indicators of Compromise (IOCs) from malicious executables to perform incident response triage

GIAC CERT: GREM
36 CPE/CMU CREDITS
WWW.GIAC.ORG/GREM

SANS TRAINING CATALOGUE, 2018
Implementing and Auditing the Critical Security Controls – In-Depth

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organisation have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

As threats evolve, an organisation’s security should too. To enable your organisation to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course that teaches students the Critical Security Controls, a prioritised, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defences. They are designed to complement existing standards, frameworks, and compliance schemes by prioritising the most critical threat and highest payoff defences, while providing a common baseline for action against risks that we all face. The Controls are effective security framework because they are based on actual threats that is measurable, scalable, and reliable in stopping known attacks and protecting organisations’ important information and systems.

The course shows security professionals how to implement the Controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats. SANS’s in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

Who should attend?
- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defence personnel or contractors
- Staff and clients of federal agencies
- Private sector organisations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MGT512

You will be able to...
- Apply a security framework based on actual threats that is measurable, scalable, and reliable in stopping known attacks and protecting organisations’ important information and systems
- Understand the importance of each Control, how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of networks and systems
- Identify and utilise tools that implement Controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each Control
- Employ specific metrics to establish a baseline and measure the effectiveness of the Controls
- Understand how the Critical Controls map to standards such as NIST 800-53, ISO 27002, the Australian Top 35, and more
- Audit each of the Critical Controls with specific, proven templates, checklists, and scripts provided to facilitate the audit process

“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
MGT 414

SIX DAYS • LAPTOP REQUIRED

SANS Training Program for CISSP® Certification

SANS MG414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam.

MG414 focuses solely on the eight domains of knowledge as determined by (ISC)² that form a critical part of the CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

Obtaining Your CISSP® Certification Consists of:
- Fulfilling minimum requirements for professional work experience
- Completing the Candidate Agreement
- Review of your résumé
- Passing the CISSP® 250 multiple-choice question exam with a scaled score of 700 points or greater
- Submitting a properly completed and executed Endorsement Form
- Periodic audit of CPEs to maintain the credential

You will be able to...
- Understand the eight domains of knowledge that are covered on the CISSP® exam
- Analyse questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the eight domains of knowledge
- Apply the skills learned across the eight domains to solve security problems when you return to work

“Best security training I have ever received and just the right amount of detail for each domain.”

Tony Barnes,
UNITED STATES SUGAR CORP

GIAC CERT: GISP
46 CPE/CMU CREDITS
WWW.GIAC.ORG/GISP

Who should attend?
- Security professionals who are interested in understanding the concepts covered on the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of information security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® eight domains
- Security professionals and managers looking for practical ways the eight domains of knowledge can be applied to their current job
Organisations invest a tremendous amount of money and resources in securing technology, but little - if anything - into securing their employees and staff.

As a result, people, not technology, have become the weakest link in cybersecurity. The most effective way to secure the human element is to establish a high-impact security awareness programme – a programme that changes behaviour as opposed to merely achieving compliance.

MGTA33 is an intense, two-day course. It teaches the key concepts and skills needed to build, maintain, and measure a security awareness programme. All course content is based on lessons learned from hundreds of security awareness programmes from around the world. Students learn from their SANS Instructor and also through extensive interaction with their peers. As such, attendees should, therefore, bring example material from their security awareness programme.

Finally, through a series of labs and exercises, students develop a custom security awareness plan that can be implemented as soon as they return to their organisation.

“Good course whether you are developing training and awareness or improving your current system.”
Tina Baker
AWE PLC

“Securing The Human: How to build, maintain, and measure a high-impact awareness programme”

Who should attend?
- Security Awareness Officers
- Chief Security Officers & Security Management Officials
- Security Auditors, Governance & Compliance Officers
- Human Resources and communications staff
- Representatives from organisations regulated by industries such as HIPAA, FISMA, FERPA, PCI-DSS, ISO/IEC 27001 SOX, NERC, or any other compliance-driven standard
- Anyone involved in planning, deploying, or maintaining a security awareness programme

You will be able to...
- Identify the maturity level of existing awareness programmes and decide where to take it next
- Explain the difference between awareness, education, and training
- Explain the three different variables of risk and how they apply to human risk and security awareness training
- Explain why people are vulnerable and how cyber attackers exploit these vulnerabilities
- Create a Project Charter and gain management support for a security awareness programme
- Identify the different targets of an awareness programme
- Characterise the culture of an organisation and determine the most effective communication methods for that culture

“The course provides an excellent Framework within which any type of organisation can develop a security Awareness programme that fits in With needs.”
Mark James
UNIVERSITY OF BRISTOL
SANS Security Awareness is security awareness training that turns employees into the first line of defence.

Security Awareness is web-based and prepares employees to recognise and react correctly to today's dominant security threats. The product line features packages created to educate end users, developers, ICS engineers, utility workers, and healthcare professionals.

Training content is video-based, interactive, and uses quizzes to ensure staff retain what they've learned. SANS Security Awareness offers over 30 language options.

Security Awareness Key Benefits:

- **Role-based training** – Build training programmes that target particular groups of employees with bespoke training content.
- **Dependable and secure hosting** – SANS infrastructure ensures training is always available and is delivered securely.
- **Convenient** – Condensed, modular video training allows employees to complete training in multiple, short sessions.
- **Security Awareness Training In A Box** – A turn-key, hosted solution for organisations looking for a pre-defined programme.
- **Corporate branding** – Training programmes can be personalised with a company’s own logo, and can incorporate supporting documents and links.
- **Clear and informative back-end** – Dashboards and reporting systems allow the manager to monitor and assess an awareness programme’s effectiveness.
- **Automated reporting and reminders** – Managers can ensure all staff are prompted to take the necessary training.
- **Anti-Phishing Programme** – Humans are the key in thwarting phishing attacks, which is why an anti-phishing program, along with other security awareness training is crucial to keeping your organisation protected.

Whether it’s an SME looking to achieve compliance or an Enterprise seeking to increase security awareness, SANS offers the right service level.

SANS Programme Managers can offer insight and support to organisations looking to build and deploy an awareness programme, and measure its impact.

**How can we help?**

To help businesses create impactful awareness programmes, SANS runs cyber security Training Events and offers expertly created resources and training tools, plus access to a global awareness community. Visit www.sans.org/security-awareness-training/resources

---

“SANS Security Awareness is a blessing. We are thankful for the system’s easy use and access. The fact that employees can take the training 24/7 is a plus.”

Nic Lee
Northrop Grumman IS

For more information about SANS Security Awareness, to request a demo, and for professional advice about how to plan an awareness programme, contact our expert team: Phone: +44 203 3384 3470, Email: awarenesstraining@sans.org
MGT 512

FIVE DAYS • LAPTOP RECOMMENDED

SANS Security Leadership Essentials For Managers (with Knowledge Compression™)

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won’t just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it’s like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

Essential security topics covered in this management track include network fundamentals and applications, power, cooling and safety, architectural approaches to defence in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, web application security, and offensive and defensive information warfare, culminating with our management practicum.

The material uses Knowledge Compression™ special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA’s CAQC program for Security+ 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

Knowledge Compression™

Maximise your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class that aims to maximise the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialised training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

Who should attend?

• All newly-appointed information security officers
• Technically-skilled administrators that have recently been given leadership responsibilities
• Seasoned managers who want to understand what your technical people are telling you

You will be able to...

• Enable managers and auditors to speak the same language as system, security, and network administrators
• Establish a minimum standard for IT management knowledge, skills, and abilities. I keep running into managers who don’t know TCP/IP, and that is OK; but then they don’t know how to calculate total cost of ownership (TCO), leaving me quietly wondering what they do know
• Save the up-and-coming generation of senior and rapidly advancing managers a world of pain by sharing the things we wish someone had shared with us. As the saying goes, it is OK to make mistakes, just make new ones

“This course is highly useful for giving me a sound baseline of Technical and general skills to help me manage an effective team”

Richard Ward
REA GROUP

GIAC CERT: GSLC
33 CPE/CMU CREDITS
WWW.GIAC.ORG/GSLC

SANS TRAINING CATALOGUE, 2018
As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organisation than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to do three things:

**Develop Strategic Plans**
Strategic planning is hard for people in IT and IT security because we spend so much time responding and reacting. We almost never get to practice until we get promoted to a senior position and then we are not equipped with the skills we need to run with the pack. Learn how to develop strategic plans that resonate with other IT and business leaders.

**Create Effective Information Security Policy**
Policy is a manager’s opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and your response was, “No way, I am not going to do that?” Policy must be aligned with an organisation’s culture. We will break down the steps to policy development so that you have the ability to develop and assess policy to successfully guide your organisation.

**Develop Management and Leadership Skills**
Leadership is a capability that must be learned, exercised and developed to better ensure organisational success. Strong leadership is brought about primarily through selfless devotion to the organisation and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organisation’s mission. Learn to utilise management tools and frameworks to better lead, inspire, and motivate your teams.

**How the Course Works**
Using case studies from Harvard Business School, team-based exercises, and discussions that put students in real-world scenarios, students will participate in activities that they can then carry out with their own team members when they return to work. The next generation of security leadership must bridge the gap between security staff and senior leadership by strategically planning how to build and run effective security programs. After taking this course you will have the fundamental skills to create strategic plans that protect your company, enable key innovations, and work effectively with your business partners.

"This course is the Rosetta Stone between an MBA and a career in cyber."
Livingston,
DELOITTE
Managing Security Operations: Detection, Response, and Intelligence

Managing Security Operations covers the design, operation, and ongoing growth of all facets of the security operations capabilities in an organisation. An effective Security Operations Center (SOC) has many moving parts and must be designed with the ability to adjust and work within the constraints of the organisation. To run a successful SOC, managers need to provide tactical and strategic direction and inform staff of the changing threat environment as well as provide guidance and training for employees. This course covers design, deployment, and operation of the security program to empower leadership through technical excellence.

The course covers the functional areas of Communications, Network Security Monitoring, Threat Intelligence, Incident Response, Forensics, and Self-Assessment.

We discuss establishing Security Operations governance for:
- Business alignment and ongoing adjustment of capabilities and objectives Designing the SOC and the associated objectives of functional areas Software and hardware technology required for performance of functions Knowledge, skills, and abilities of staff as well as staff hiring and training Execution of ongoing operations
- You will walk out of this course armed with a roadmap to design and operate an effective SOC tailored to the needs of your organisation.

Course Author Statement
The inclusion of all functional areas of security operations is intended to develop a standardized program for an organisation and express all necessary capabilities. Admittedly ambitious, the intention of the class is to provide a unified picture of coordination among teams with different skillsets to help the business prevent loss due to poor security practices. I have encountered detrimental compartmentalization in most organisations. There is a tendency for a specialist to look only at her piece of the problem, without understanding the larger scope of information security within an organisation. Organisations are likely to perceive a security operations center as a tool, and not the unification of people, processes, and technologies.

This course provides a comprehensive picture of what a Cyber Security Operations Center (CSOC or SOC) is. Discussion on the technology needed to run a SOC are handled in a vendor agnostic way. In addition, technology is addressed in a way that attempts to address both minimal budgets as well as budgets with global scope. Staff roles needed are enumerated. Informing and training staff through internal training and information sharing is addressed. The interaction between functional areas and data exchanged is detailed. After attending this class, the participant will have a roadmap for what needs to be done in the organisation seeking to implement security operations. - Christopher Crowley

Who should attend?
- Information security managers
- SOC managers, analysts, and engineers
- Information security architects
- IT managers
- Operations managers
- Risk management professionals
- IT/System administration/Network administration professionals
- IT auditors
- Business continuity and disaster recovery staff

You will be able to...
- Design security operations to address all needed functions for the organisation
- Select technologies needed to implement the functions for a SOC
- Maintain appropriate business alignment with the security capability and the organisation
- Develop and streamline security operations processes
- Strengthen and deepen capabilities Collect data for metrics, report meaningful metrics to the business, and maintain internal
- SOC performance metrics
- Hire appropriate SOC staff and keep existing SOC staff up to date
This course is offered by the SANS Institute as a PMI® Registered Education Provider (R.E.P.). R.E.P.s provide the training necessary to earn and maintain the Project Management Professional (PMP®) and other professional credentials. PMP® is a registered trademark of Project Management Institute, Inc.

This course has been recently updated to fully prepare you for the 2016 PMP® exam changes. During this class you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. We will utilise project case studies that highlight information technology services as deliverables. MGT525 follows the basic project management structure from the PMBOK® Guide – Fifth Edition and also provides specific techniques for success with information assurance initiatives. Throughout the week, we will cover all aspects of IT project management from initiating and planning projects through managing cost, time, and quality while your project is active, and to completing, closing, and documenting as your project finishes. A copy of the PMBOK® Guide – Fifth Edition is provided to all participants. You can reference the PMBOK® Guide and use your course material along with the knowledge you gain in class to prepare for the 2016 updated Project Management Professional (PMP®) Exam and the GIAC Certified Project Manager Exam.

The project management process is broken down into core process groups that can be applied across multiple areas of any project, in any industry. Although our primary focus is the application to the InfoSec industry, our approach is transferable to any projects that create and maintain services as well as general product development. We cover in-depth how cost, time, quality, and risks affect the services we provide to others. We will also address practical human resource management as well as effective communication and conflict resolution. You will learn specific tools to bridge the communications gap between managers and technical staff.

“Honestly, this is one of the best courses I have had to date. I feel like I have thousands of things to take back to my job.”

Ryan Spencer, REED ELSEVIER INC.

Who should attend?
- Individuals interested in preparing for the Project Management Professional (PMP®) Exam
- Security professionals who are interested in understanding the concepts of IT project management
- Managers who want to understand the critical areas of making projects successful
- Individuals working with time, cost, quality, and risk-sensitive projects and applications
- Anyone who would like to utilise effective communication techniques and proven methods to relate better to people
- Anyone in a key or lead engineering/design position who works regularly with project management staff

You will be able to...
- Recognise the top failure mechanisms related to IT and InfoSec projects, so that your projects can avoid common pitfalls
- Create a project charter that defines the project sponsor and stakeholder involvement
- Document project requirements and create a requirements traceability matrix to track changes throughout the project lifecycle
- Clearly define the scope of a project in terms of cost, schedule and technical deliverables
- Develop a detailed project schedule, including critical path tasks and milestones
- Develop a detailed project budget including cost baselines and tracking mechanisms
- Develop planned and earned value metrics for your project deliverables and automate reporting functions
- Effectively manage conflict situations and build communication skills with your project team
SIX DAYS • LAPTOP REQUIRED

Auditing & Monitoring Networks, Perimeters, and Systems

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise. What systems really matter? How should the firewall and routers be configured? What settings should be checked on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? How do we turn this into a continuous monitoring process? All of these questions and more will be answered by the material covered in this course. This course is specifically organized to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organisation. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation are taken from realworld examples.

One of the struggles that IT auditors face today is helping management understand the relationship between the technical controls and the risks to the business that these controls address. In this course these threats and vulnerabilities are explained based on validated information from real-world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organisation to build an understanding of why these controls specifically and auditing in general are important. From these threats and vulnerabilities, we will explain how to build the ongoing compliance monitoring systems and automatically validate defences through instrumentation and automation of audit checklists.

You’ll be able to use what you learn immediately. Five of the six days in the course will either produce or provide you directly with a general checklist that can be customised for your audit practice. Each of these days includes hands-on exercises with a variety of tools discussed during the lecture sections so that you will leave knowing how to verify each and every control described in the class. Each of the five hands-on days gives you the chance to perform a thorough technical audit of the technology being considered by applying the checklists provided in class to sample audit problems in a virtualised environment. Each student is invited to bring her own Windows 7 Professional 64 bit or higher laptop for use during class. The ideal laptop will have at least 4 gigabytes of RAM.

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are, and why. Sign up for this course and gain the mix of theoretical, hands-on, and practical knowledge to conduct a great audit.

“The entire course has been awesome and prepared me to perform a comprehensive audit. It also provided me excellent information to operations to improve network security posture.”

Srinath Kannan, ACCENTURE

Who should attend?

- Auditors seeking to identify key controls in IT systems
- Audit professionals looking for technical details on auditing
- Managers responsible for overseeing the work of an audit or security team
- Security professionals newly tasked with audit responsibilities
- System and network administrators looking to better understand what an auditor is trying to achieve, how auditors think, and how to better prepare for an audit
- System and network administrators seeking to create strong change control management and detection systems for the enterprise

You will be able to...

- Understand the different types of controls (e.g., technical vs. non-technical) essential to perform a successful audit
- Conduct a proper risk assessment of a network to identify vulnerabilities and prioritise what will be audited
- Establish a well-secured baseline for computers and networks, constituting a standard against which one can conduct audits
- Perform a network and perimeter audit using a seven step process
- Audit firewalls to validate that rules/settings are working as designed, blocking traffic as required
- Utilise vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources
- Audit web application configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- Utilise scripting to build a system to baseline and automatically audit Active Directory and all systems in a Windows domain
FIVE DAYS • LAPTOP NOT REQUIRED

Law of Data Security and Investigations

NEW!
• Form contract for inviting outside incident responders - including police, contractors, National Guard, or civil defence agency anywhere in the world - to help with a cyber crisis
• EU’s new General Data Protection Regulation and its impact around the world
• The impact of Trump presidency and Brexit on data security law and regulatory enforcement
• The EU’s adoption of “Privacy Shield” to replace “Privacy Safe Harbor” for transferring data to the United States
• Cyber insurer’s lawsuit against hospital to deny coverage after data breach and $41 million legal settlement with patients

New laws on privacy, e-discovery and data security are creating an urgent need for professionals who can bridge the gap between the legal department and the IT department. SANS LEG523 provides this unique professional training including skills in the analysis and use of contracts, policies and records management procedures. This course covers the laws of business, contracts, fraud, crime, IT security, liability and policy – all with a focus on electronically stored and transmitted records. It also teaches investigators how to prepare credible, defensible reports, whether for cyber crimes, forensics, incident response, human resource issues or other investigations.

Each successive day of this five-day course builds upon lessons from the earlier days in order to comprehensively strengthen your ability to help your enterprise (public or private sector) cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with IT security.

Recent updates to the course address hot topics such as legal tips on confiscating and interrogating mobile devices, the retention of business records connected with cloud computing and social networks like Facebook and Twitter, and analysis and response to the risks and opportunities surrounding open-source intelligence gathering.

Over the years this course has adopted an increasingly global perspective. Non-U.S. professionals attend LEG523 because there is no training like it anywhere else in the world. For example, a lawyer from the national tax authority in an African country took the course because electronic filings, evidence and investigations have become so important to her work. International students help the instructor, U.S. attorney Benjamin Wright, constantly revise the course and include more content that crosses borders.

Who should attend?
• Investigators
• Security and IT professionals
• Lawyers
• Paralegals
• Auditors
• Accountants
• Technology managers
• Vendors
• Compliance officers
• Law enforcement
• Privacy officers
• Penetration testers
• Cyber incident and emergency responders

You will be able to...
• Work better with other professionals at your organisation who make decisions about the law of data security and investigations
• Exercise better judgment on how to comply with technology regulations, both in the United States and in other countries
• Evaluate the role and meaning of contracts for technology, including services, software and outsourcing
• Help your organisation better explain its conduct to the public and to legal authorities
• Anticipate technology law risks before they get out of control
• Implement practical steps to cope with technology law risk
• Better explain to executives what your organisation should do to comply with information security and privacy law
• Better evaluate technologies, such as digital signatures, to comply with the law and serve as evidence
• Make better use of electronic contracting techniques to get the best terms and conditions
• Exercise critical thinking to understand the practical implications of technology laws and industry standards (such as the Payment Card Industry Data Security Standard)
This is the course to take if you have to defend web applications!
The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure them. Traditional network defences, such as firewalls, fail to secure web applications. DEV522 covers the OWASP Top 10 Risks and will help you better understand web application vulnerabilities, thus enabling you to properly defend your organisation’s web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world applications that have been proven to work. The testing aspect of vulnerabilities will also be covered so that you can ensure your application is tested for the vulnerabilities discussed in class.

To maximise the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than 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, 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.

The course will also cover additional issues the authors have found to be important in their day-to-day web application development practices. The topics that will be covered include:

- Infrastructure security
- Server configuration
- Authentication mechanisms
- Application language configuration
- Application coding errors like SQL injection and cross-site scripting
- Cross-site request forging
- Authentication bypass
- Web services and related flaws
- Web 2.0 and its use of web services
- XPATH and XQUERY languages and injection
- Business logic flaws
- Protective HTTP headers

The course will make heavy use of hands-on exercises and conclude with a large defensive exercise that reinforces the lessons learned throughout the week.
Secure Coding in Java/JEE: Developing Defensible Applications

This secure coding course will teach students how to build secure Java applications and gain the knowledge and skills to keep a website from getting hacked, counter a wide range of application attacks, prevent critical security vulnerabilities that can lead to data loss, and understand the mindset of attackers.

The course teaches you the art of modern web defence for Java applications by focusing on foundational defensive techniques, cutting-edge protection, and Java EE security features you can use in your applications as soon as you return to work. This includes learning how to:

- Identify security defects in your code
- Fix security bugs using secure coding techniques
- Utilise secure HTTP headers to prevent attacks
- Secure your sensitive representational state transfer (REST) services
- Incorporate security into your development process
- Use freely available security tools to test your applications

Great developers have traditionally distinguished themselves by the elegance, effectiveness and reliability of their code. That is still true, but the security of the code now needs to be added to those other qualities. This unique SANS course allows you to hone the skills and knowledge required to prevent your applications from getting hacked.

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications is a comprehensive course covering a wide set of skills and knowledge. It is not a high-level theory course – it is about real-world, hands-on programming. You will examine actual code, work with real tools, build applications and gain confidence in the resources you need to improve the security of Java applications.

Rather than teaching students to use a given set of tools, the course covers concepts of secure programming. This involves looking at a specific piece of code, identifying a security flaw and implementing a fix for flaws found on the OWASP Top 10 and CWE/SANS Top 25 Most Dangerous Software Errors.

The course culminates in a Secure Development Challenge in which students perform a security review of a real-world open-source application. You will conduct a code review, perform security testing to actually exploit real vulnerabilities, and implement fixes for these issues using the secure coding techniques that you have learned in course.

Who should attend?
- Developers who want to build more secure applications
- Java Enterprise Edition (JEE) programmers
- Software engineers
- Software architects
- Developers who need to be trained in secure coding techniques to meet PCI compliance
- Application security auditors
- Technical project managers
- Senior software QA specialists
- Penetration testers who want a deeper understanding of target applications or who want to provide more detailed vulnerability remediation options

You will be able to...
- Use a web application proxy to view and manipulate HTTP requests and responses
- Review and perform basic exploits of common web application vulnerabilities, such as those found among the SANS/CWE Top 25 Most Dangerous Software Errors and the OWASP Top 10
- Mitigate common web application vulnerabilities using secure coding practices and Java libraries
- Build applications using:
  - Java Enterprise Edition authentication
  - Basic and form-based authentication
  - Client certificates
  - Secure Sockets Layer/Transport Layer Security (SSL/TLS)
- Java Secure Sockets Extension
- Secure password storage techniques
- Java Cryptography Architecture
- Security Manager
- Implement a secure software development lifecycle, including code review, static analysis and dynamic analysis techniques
ASP.NET and the .NET framework have provided web developers with tools that allow them an unprecedented degree of flexibility and productivity. However, these sophisticated tools make it easier than ever to miss the little details that allow security vulnerabilities to creep into an application. Since ASP.NET 2.0, Microsoft has done a fantastic job of integrating security into the ASP.NET framework, but the responsibility is still on application developers to understand the limitations of the framework and ensure that their own code is secure.

Have you ever wondered if the built-in ASP.NET validation is effective? Have you been concerned that Windows Communication Foundation (WCF) services might be introducing unexamined security issues into your application? Should you feel uneasy relying solely on the security controls built into the ASP.NET framework?

This comprehensive course covers a huge set of skills and knowledge. It is not a high-level theory course. It is about real programming. Students examine actual code, work with real tools, build applications, and gain confidence in the resources they need to improve the security of .NET applications.

Rather than teaching students to use a set of tools, the course teaches students concepts of secure programming. This involves looking at a specific piece of code, identifying a security flaw, and implementing a fix for flaws found on the OWASP Top 10 and CWE/SANS Top 25 Most Dangerous Programming Errors.

The class culminates with a security review of a real-world open-source application. Students will conduct a code review, review a penetration test report, perform security testing to actually exploit real vulnerabilities, and finally, using the secure coding techniques that they have learned in class, implement fixes for these issues.

“It is shocking to see how much we are missing in our code. I am going back to change the code immediately.”

Ruojie Wang,
NEW JERSEY HOSPITAL ASSOCIATION
ICS/SCADA Security Essentials

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. ICS410: ICS/SCADA Security Essentials provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with:

- An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints
- Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- Control system approaches to system and network defence architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as industrial control system penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

With the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. For their part, IT support personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

Who should attend?

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

You will be able to...

- 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
- Better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- Work with network infrastructure design (network architecture concepts, including topology, protocols, and components)
- Better understand the systems’ lifecycles
- Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)
- Use your skills in computer network defence (detecting host and network-based intrusions via intrusion detection technologies)
- Implement incident response and handling methodologies

Who should take this course?

Every IT security professional and others within support and projects around ICS should take this course.

Simon Poole, SHELL

When these different groups of professionals complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their industrial control system environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

GIAC CERT: GICSP
30 CPE/CMU CREDITS
WWW.GIAC.ORG/GICSP

SANS TRAINING CATALOGUE, 2018
Essentials for NERC Critical Infrastructure Protection

The Essentials for NERC Critical Infrastructure Protection 5-day course empowers students with knowledge of the “what” and the “how” of the version 5/6 standards. The course addresses the role of FERC, NERC and the Regional Entities, provides multiple approaches for identifying and categorising BES Cyber Systems and helps asset owners determine the requirements applicable to specific implementations. Additionally, the course covers implementation strategies for the version 5/6 requirements with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance.

Our 25 hands-on labs range from securing workstations to digital forensics and lock picking.

Author Statement

The SANS ICS456: NERC Critical Infrastructure Protection Essentials course was developed by SANS ICS team members with extensive electric industry experience including former Registered Entity Primary Contacts, a former NERC officer, and a Co-Chair of the NERC CIP Interpretation Drafting Team. Together the authors bring real-world, practitioner experience gained from developing and maintaining NERC CIP and NERC 693 compliance programs and actively participating in the standards development process.

Who should attend?

- Security Architects
- Network Engineers
- Network Architects
- Security Analysts
- Senior Security Engineers
- System Administrators
- Technical Security Managers
- CND Analysts
- Security Monitoring Specialists
- Cyber Threat Investigators

You will be able to...

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Determine appropriate security monitoring needs for organisations of all sizes
- Maximize existing investment in security architecture by reconfiguring existing assets
- Determine capabilities required to support continuous monitoring of key Critical Security Controls
- Configure appropriate logging and monitoring to support a Security Operations Center and continuous monitoring program
ICS Active Defense and Incident Response

ICS515: ICS Active Defense and Incident Response will help you deconstruct ICS cyber attacks, leverage an active defence to identify and counter threats in your ICS, and use incident response procedures to maintain the safety and reliability of operations. This course will empower students to understand their networked industrial control system environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This process of monitoring, responding to, and learning from threats internal to the network is known as active defence.

An active defence is the approach needed to counter advanced adversaries targeting ICS, as has been seen with malware such as Stuxnet, Havex, and BlackEnergy2. Students can expect to come out of this course with the ability to deconstruct targeted ICS attacks and fight these adversaries and others. The course uses a hands-on approach and real-world malware to break down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of leveraging active defence concepts such as using threat intelligence, performing network security monitoring, and utilising malware analysis and incident response to ensure the safety and reliability of operations. The strategy and technical skills presented in this course serve as a basis for ICS organisations looking to show that defence is do-able.

This course will prepare you to:

- Examine ICS networks and identify the assets and their data flows in order to understand the network baseline information needed to identify advanced threats
- Use active defence concepts such as threat intelligence consumption, network security monitoring, malware analysis, and incident response to safeguard the ICS
- Build your own Programmable Logic Controller using a CYBATIworks Kit and keep it after the class ends
- Gain hands-on experience with samples of Havex, BlackEnergy2, and Stuxnet through engaging labs while de-construcuting these threats and others
- Leverage technical tools such as Shodan, Security Onion, TCPDump, NetworkMiner, Foremost, Wireshark, Snort, Bro, SGUILL, ELSA, Volatility, Redline, FTK Imager, PDF analysers, malware sandboxes, and more
- Create indicators of compromise (IOCs) in OpenIOC and YARA while understanding sharing standards such as STIX and TAXII
- Take advantage of models such as the Sliding Scale of Cybersecurity, the Active Cyber Defense Cycle, and the ICS Cyber Kill Chain to extract information from threats and use it to encourage the long-term success of ICS network security

“This course is the missing piece to get companies to take threats seriously, pursue the truth, and share their findings.”

Rob Cantu, DOE

Who should attend?

- ICS incident response team leads and members
- ICS and operations technology security personnel
- IT security professionals
- Security Operations Center (SOC) team leads and analysts
- ICS red team and penetration testers
- Active defenders

You will learn...

- How to perform ICS incident response focusing on security operations and prioritising the safety and reliability of operations.
- How ICS threat intelligence is generated and how to use what is available in the community to support ICS environments. The analysis skills you learn will enable you to critically analyse and apply information from ICS threat intelligence reports on a regular basis.
- How to identify ICS assets and their network topologies and how to monitor ICS hotspots for abnormalities and threats. Methodologies such as ICS network security monitoring and approaches to reducing the control system threat landscape will be introduced and reinforced.
- How to analyse ICS malware and extract the most important information needed to quickly scope the environment and understand the nature of the threat.
- How to operate through an attack and gain the information necessary to instruct teams and decision-makers on when operations must shut down, or if it is safe to respond to the threat and continue operations.
- How to use multiple security disciplines in conjunction with each other to leverage an active defence and safeguard the ICS, all reinforced with hands-on labs and technical concepts.
The SANS Voucher Program is a cybersecurity workforce training management system that allows you to easily procure and manage your organization’s training needs.

As a SANS Voucher Program participant, you will be able to:

- Provide your cybersecurity team with the highest standard of skill training and certification available
- Give employees a simple way to select and procure the training they need, when they need it
- Easily approve and manage student enrollment
- Monitor employee training progress and exam scores to ensure satisfactory completion
- Track investments, debits, and account balance for optimal budgeting

Voucher Funds purchased can be applied to any live and online SANS training courses, SANS Summit events, GIAC Certifications, or certification renewals.* Voucher Funds must be used within 12 months, but the term can be extended with additional investments.

Get Started
Visit www.sans.org/vouchers and submit the contact request form to have a SANS representative in your region call or email you within 24 business hours. Within as little time as one week, your eligible team members can begin their training.

www.sans.org/vouchers

*Current exceptions from the SANS Voucher program are the Partnership program, Security Awareness training, and SANS workshops hosted at events run by other organizations.
Create a **SANS Account** today to enjoy these Free resources at **www.sans.org/account**

**Newsletters**

**NewsBites**
Twice-weekly, high-level executive summary of the most important news relevant to cybersecurity professionals. **OUCH!**
The world’s leading monthly, free security awareness newsletter designed for the common computer user.

**Webcasts**

**Ask the Experts Webcasts**
SANS experts bring current and timely information on relevant topics in IT Security. **Analyst Webcasts**
A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

**Other Free Resources**

(No portal account is necessary)

- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQs
- Tip of the Day

**@RISK: The Consensus Security Alert**
A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data.

**WhatWorks Webcasts**
The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.

**Tool Talks**
Tool Talks are designed to give you a solid understanding of a problem and how a vendor’s commercial tool can be used to solve or mitigate that problem.

- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

Follow us on our social media channels to stay up-to-date on the latest cyber security developments and announcements around SANS EMEA events and courses.
Take SANS training in a classroom environment and learn directly from a SANS Instructor.

SANS hosts live training events across Europe and the Middle East throughout the year.

For the latest schedule and course details visit www.sans.org/emea or contact us directly at emea@sans.org