SANS

The Most Trusted Name in Information Security Training, Certification, and Research

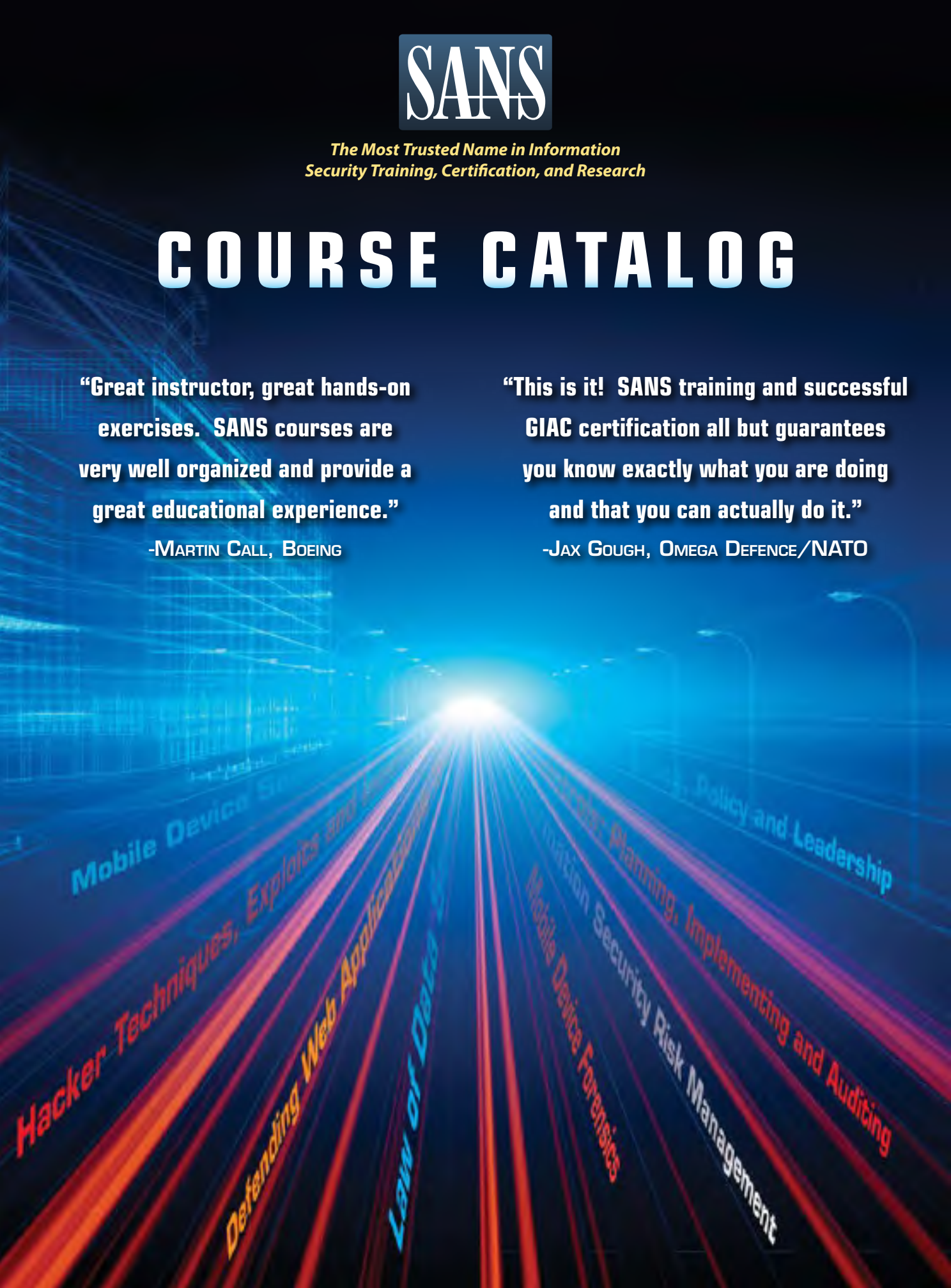
COURSE CATALOG

"Great instructor, great hands-on exercises. SANS courses are very well organized and provide a great educational experience."

-Martin Call, Boeing

"This is it! SANS training and successful GIAC certification all but guarantees you know exactly what you are doing and that you can actually do it."

-Jax Gough, Omega Defence/NATO



Your Source for IT Security Education

Whether you need continuing education courses, are looking for a career tract, want to strengthen your skills and knowledge with a GIAC certification, or would like to earn a Master's Degree in Information Security, SANS, Global Information Assurance Certification (GIAC), and the SANS Technology Institute (STI) can help you achieve your education goals. The SANS method of training has been effective for over 20 years. The courses are full of important and immediately useful techniques that you can put to work as soon as you return to your offices. They were developed through a consensus process involving hundreds of administrators, security managers, and information security professionals, and address both security fundamentals and awareness – and the in-depth technical aspects of the most crucial areas of IT security.

Why SANS is the best training and educational investment

- Intensive, hands-on immersion training with the highest quality courseware in the industry.
- Incomparable instructors and authors who are industry experts and practitioners. They are out there fighting the same battles and discovering new ways to thwart attacks.
- Increases a student's ability to achieve a GIAC certification. GIAC is unique in the field of information security certifications because it not only tests a candidate's knowledge but also the candidate's ability to put that knowledge into practice in the real world. See pages 12-13 for more about GIAC.

Continuing Education

Over 50 courses in the following disciplines:

- Security
- Management
- Forensics
- Audit
- Software Security

Career Paths

Ten career tract curriculums:

- Computer Forensics Analyst
- Computer Crime Investigator
- Cyber Guardian
- Incident Responder
- Intrusion Analyst
- Malware Analyst
- Pen Tester
- Security Auditor
- Security Analyst
- Developer
- Security Director

Higher Education

The SANS Technology Institute (STI) offers two master's degree programs:

- Master of Science in Information Security Engineering (MSISE)
- Master of Science in Information Security Management (MSISM)

Learn more about STI at www.sans.edu

Global Information Assurance Certification (GIAC)

Over 20 certifications in:

- Security
- Management
- Forensics
- Audit
- Software Security
- Legal

Table of Contents

Choose the Learning Format that Works for You!

SANS offers a variety of live training and online learning formats. See pages 2-3 for descriptions of each format.

Free Course Excerpts!

Got ten minutes? Come learn something new! Our free course excerpts let you see if a course is a good fit for your needs. Go to www.sans.org/security-training/courses.php and click on the free excerpt of available courses.

SANS Training Formats

Training Events

SANS Training Events are recognized as the best place in the world to get IT security education, from intimate gatherings to our action-packed national events! Network with other information security professionals, hear world-class speakers, actively engage with providers of proven security solutions, and participate in challenges and contests.
www.sans.org/security-training/bylocation/index_all.php

Community

Community Training Events

The SANS Community format offers our most popular security courses in a small classroom setting – most courses have fewer than 25 students. The course material is delivered over a six-day period, just like at larger SANS events, by instructors trained by SANS very best authors and instructors. We bring SANS to your community at a discounted tuition level while also saving you time and money on travel.
www.sans.org/community

OnSite

Information Security Training at Your Location

With the SANS OnSite program you can bring a combination of high-quality content and world-recognized instructors to your location and realize significant savings in employee travel costs and course fees for larger classes.
www.sans.org/onsite

Mentor & @Work

Intimate Live Instruction

The SANS Mentor program offers the flexibility of live instruction with self-paced learning. Classes are conducted over the course of several weeks, much like a graduate level course. Students study on their own then work with the Mentor during class to discuss material, answer questions and work on exercises and labs such as Capture the Flag.
www.sans.org/mentor

Summit Series

Your IT Security Connection

SANS WhatWorks Summits are unique events that focus on the most current topics in computer security. User panels, debates, vendor demos, and short talks by industry experts help you get the most up-to-date security solutions in the least amount of time.
www.sans.org/summit

OnDemand

Online Training & Assessments Anytime, Anywhere

If you're a self-motivated learner whose schedule changes often, then SANS OnDemand is the right learning platform for you. Choose from more than 40 courses and take them whenever and wherever you want. Each course gives you four months of access to our OnDemand computer-based training platform, which includes a mix of presentation slides, video demonstrations, and assessment tests supported with audio of SANS' top instructors teaching the material.

If you have questions about the material, our virtual mentors are available to help. You can also bundle OnDemand with any other SANS online or in-person training vehicle to diversify your learning experience or bolster your preparation for the GIAC certification exam. **www.sans.org/ondemand**

vLive!

Real-time access to Certified SANS Instructors

If you prefer a more structured and interactive learning environment, you should consider vLive! The vLive! platform uses cutting-edge webcast technology and collaboration software to create a virtual classroom. vLive! classes are typically scheduled from 7 to 10 p.m. EST and are taught in real time by SANS instructors, who communicate with students via audio and online chatting.

- Interact with your instructor during class and virtual office hours, which take place one hour before class.
- Classes are recorded and accessible online for six months.
- You can revisit individual class sessions to review challenging concepts or repeat exercises.

www.sans.org/vlive

Simulcast

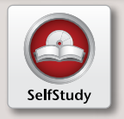
Live SANS Instruction in Multiple Locations

SANS Simulcast classes are:

- COST-EFFECTIVE – You can save thousands of dollars on travel costs, making Simulcast an ideal solution for students working with limited training budgets or travel bans.
- ENGAGING – Simulcast classes are live and interactive, allowing you to ask questions and share experiences with your instructor and classmates.
- CONDENSED – Complete your course quickly; Event Simulcast classes run all day in real time with select courses being held at our live training events. Custom Simulcast classes are just that, classes that can be customized to your training requirements.
- REPEATABLE – Simulcast classes are recorded and placed in an online archive in case you have to miss part of the class or just wish to view the material again at a later date.
- COMPLETE – You will receive the same books and course materials that conference students receive, and you will see and hear the same material presented to students at the events.

www.sans.org/simulcast

SelfStudy



Books & MP3s

With each SelfStudy course, you'll receive a complete set of SANS course books, MP3s of lectures by SANS' top instructors, and when applicable, hands-on CDs and virtual labs. **www.sans.org/selfstudy**

SANS IT Security Training and Your Career Roadmap

SECURITY CURRICULUM

Incident Handling

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

SEC501 Advanced Security Essentials – Enterprise Defender *GCED*

FOR508 Advanced Computer Forensic Analysis & Incident Response *GCFA*

COURSE RELAUNCH

Additional Incident Handling Courses
www.sans.org/security-training/curriculums/security

Beginners

SEC301 NOTE:
If you have experience in the field, please consider our more advanced course - SEC401.

SEC301 Intro to Information Security *GISF*

SEC401 SANS Security Essentials Bootcamp Style *GSEC*

Intrusion Analysis

SEC501 Advanced Security Essentials – Enterprise Defender *GCED*

SEC502 Perimeter Protection In-Depth *GCFW*

SEC503 Intrusion Detection In-Depth *GCIA*

Additional Intrusion Analysis Courses
www.sans.org/security-training/curriculums/security

Penetration Testing

Additional Penetration Testing Courses
http://pen-testing.sans.org

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

SEC560 Network Pen Testing and Ethical Hacking *GPEN*

SEC542 Web App Pen Testing and Ethical Hacking *GWAPT*

New!

SEC575 Mobile Device Security and Ethical Hacking

SEC660 Advanced Pen Testing, Exploits, and Ethical Hacking *GXPN*

New!

SEC642 Advanced Web App Pen Testing and Ethical Hacking

SEC617 Wireless Ethical Hacking, Pen Testing, and Defenses *GAWN*

Network Security

SEC501 Advanced Security Essentials – Enterprise Defender *GCED*

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

SEC540 VoIP Security

Additional Network Security Courses
www.sans.org/security-training/curriculums/security

System Administration

SEC501 Advanced Security Essentials – Enterprise Defender *GCED*

SEC505 Securing Windows *GCWN*

New!

SEC579 Virtualization and Private Cloud Security

SEC506 Securing Linux/Unix *GCUX*

Additional System Administration Courses
www.sans.org/security-training/curriculums/security

MANAGEMENT CURRICULUM

SEC301 Intro to Information Security *GISF*

SEC401 SANS Security Essentials Bootcamp Style *GSEC*

MGT512 SANS Security Leadership Essentials For Managers with Knowledge Compression™ *GSLC*

MGT525 IT Project Management, Effective Communication, and PMP® Exam Prep *GCPM*

MGT414 SANS® +S™ Training Program for the CISSP® Certification Exam *GISP*

Additional Management Courses
www.sans.org/security-training/curriculums/management

FORENSICS CURRICULUM

FOR408 Computer Forensic Investigations - Windows In-Depth *GCFE*

FOR508 Advanced Computer Forensic Analysis & Incident Response *GCFA*

COURSE RELAUNCH

FOR558 Network Forensics

FOR563 Mobile Device Forensics

FOR610 REM: Malware Analysis Tools & Techniques *GREM*

Additional Forensic Courses
http://computer-forensics.sans.org

AUDIT CURRICULUM

SEC301 Intro to Information Security *GISF*

SEC401 SANS Security Essentials Bootcamp Style *GSEC*

AUD407 Foundations of Auditing Information Systems

AUD507 Auditing Networks, Perimeters, and Systems *GSNA*

AUD566 Implementing & Auditing the Twenty Critical Security Controls – In-Depth

Additional Audit Courses
http://it-audit.sans.org

LEGAL CURRICULUM

SEC301 Intro to Information Security *GISF*

SEC401 SANS Security Essentials Bootcamp Style *GSEC*

LEG523 Law of Data Security and Investigations *GLEG*

GIAC certification available for courses indicated with GIAC acronyms

SOFTWARE SECURITY CURRICULUM

Defense

DEV522 Defending Web Applications Security Essentials *GWEB*

Attack

SEC542 Web App Pen Testing and Ethical Hacking *GWAPT*

New!

SEC642 Advanced Web App Pen Testing and Ethical Hacking

Secure Coding

JAVA

DEV541 Secure Coding in Java/JEE (4-Day Course) *GSSP-JAVA*

DEV530 Essential Secure Coding in Java/JEE (2-Day Course)

.NET

DEV544 Secure Coding in .NET (4-Day Course) *GSSP-.NET*

DEV532 Essential Secure Coding in ASP.NET (2-Day Course)

C & C++

DEV543 Secure Coding in C & C++

PCI

DEV536 Secure Coding for PCI Compliance

Additional Software Security Courses
http://software-security.sans.org

Cyber Security Career Paths

We are losing the cyber race – and falling behind at an accelerating pace. Almost every week, organizations and individuals use their advanced cyber skills to burrow deeply into the information systems that control our daily lives. A major cause of our stumbling is that we face an extreme shortage of people who are cyber security professionals. Without tens of thousands of people with these skills, we are unable to see most attacks and to dominate in cyber security.

The good news is that many young people are considering careers in cyber security and, with the right training, they will help fill the gap. Those drawn to the field are motivated by a variety of reasons. Some are looking for a challenge, others want a job that makes a difference, and still others want to solve computer crime, or better yet, help avoid it. One thing is clear – as the cyber race goes on, the top technical jobs in information security are only increasing in importance.

Below is a list of information security jobs along with the SANS courses necessary to attain one of these positions.

Computer Forensics Analyst

This expert analyzes how intruders breached the infrastructure in order to identify additional systems/networks that have been compromised. Investigating traces left by complex attacks requires a forensic expert who is not only proficient in the latest forensic, response, and reverse engineering skills, but is astute in the latest exploit methodologies.

SEC301 Intro to Information Security
→ **SEC401** SANS Security Essentials Bootcamp Style
→ **FOR408** Computer Forensic Investigations – Windows In-Depth
→ **FOR508** Advanced Computer Forensic Analysis and Incident Response

SPECIALIZATIONS

Computer Crime Investigator

Computer crime investigators include both 'sworn' law enforcement officers and 'un-sworn' employees of departments who are dedicated information security investigators. Both are entrusted with the preservation, acquisition, storage, detailed analysis, and clear reporting of digital evidence from many sources: from audio to data bases, e-mail to financial data, pictures and beyond – almost every contemporary crime has some digital evidence.

FOR558 Network Forensics
FOR563 Mobile Device Forensics
FOR526 Advanced Filesystem Recovery and Memory Forensics
LEG523 Law of Data Security and Investigations

Malware Analyst

A malware analyst examines malicious software to understand the nature of the threat. This usually involves reverse-engineering the compiled executable to figure out how the program interacts with its environment. The analyst may be asked to document the specimen's attack capabilities, understand its propagation characteristics, and define signatures for detecting its presence.

SEC569 Combating Malware in the Enterprise
FOR610 Reverse-Engineering Malware – Malware Analysis Tools and Techniques
SEC710 Advanced Exploit Development

Incident Responder

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

SEC301 Intro to Information Security
→ **SEC401** SANS Security Essentials Bootcamp Style
→ **SEC504** Hacker Techniques, Exploits, and Incident Handling
→ **FOR508** Advanced Computer Forensic Analysis and Incident Response

Penetration Tester

This expert contributes an integral piece to the company's software development life cycle. He/she does everything from developing code to reverse-engineering binaries to examining network traffic.

SEC401 SANS Security Essentials Bootcamp Style
→ **SEC504** Hacker Techniques, Exploits and Incident Handling
→ **SEC542** Web App Penetration Testing and Ethical Hacking
SEC560 Network Penetration Testing and Ethical Hacking
→ **SEC617** Wireless Ethical Hacking, Penetration Testing, and Defenses
SEC660 Advanced Penetration Testing, Exploits, and Ethical Hacking

SPECIALIZATIONS

SEC580 Metasploit Kung Fu for Enterprise Pen Testing
SEC710 Advanced Exploit Development

Intrusion Analyst

This analyst is responsible for monitoring traffic, blocking unwanted traffic from and to the Internet, and dealing with attackers. Firewalls and IPS technology are the starting point for hardening the network against possible intrusion attempts. Knowledge in firewall policies and functionality is crucial in network security.

SEC301 Intro to Information Security
→ **SEC401** SANS Security Essentials Bootcamp Style
→ **SEC503** Intrusion Detection In-Depth
→ **SEC502** Perimeter Protection In-Depth
→ **SEC567** Power Packet Crafting with Scapy

Security Auditor

Management depends on this expert to measure and report on risk to the organization by measuring compliance with policies, procedures, and standards. These experts are among the few in the organization, who are actually asked for their honest opinion on what could be improved or done better to make the organization more efficient and profitable through continuous monitoring risk management.

AUD407 Foundations of Auditing Information Systems
AUD507 Auditing Networks, Perimeters, and Systems
SEC566 Implementing and Auditing the Twenty Critical Security Controls In-Depth
AUD521 Meeting the Minimum: PCI/DSS 2.0: Becoming and Staying Compliant

To learn more about these careers and the 20 Coolest Jobs in Information Security, go to:

www.sans.org/20coolestcareers

Cyber Security Career Paths

Security Analyst

Responsible for research and analysis of security threats that may affect a company's assets, products or technical specifications. This analyst will dig into technical protocols and specifications for a greater understanding of security threats than most of his/her peers, identifying strategies to defend against attacks through intimate knowledge of the threats.

SEC301 Intro to Information Security
→ **SEC401** SANS Security Essentials Bootcamp Style
↓
SEC501 Advanced Security Essentials – Enterprise Defender
→ **SEC503** Intrusion Detection In-Depth
↓
SEC504 Hacker Techniques, Exploits and Incident Handling

SPECIALIZATIONS

WINDOWS

SEC505 Securing Windows

LINUX/UNIX

SEC506 Securing Linux/Unix

Security Developer

The security-savvy software developer leads all developers in the creation of secure software, implementing secure programming techniques that are free from logical design and technical implementation flaws. This expert is ultimately responsible for ensuring customer software is free from vulnerabilities that can be exploited by an attacker.

DEV304 Software Security Awareness
↓
DEV522 Developing Web Applications

SPECIALIZATIONS

JAVA

DEV541 Secure Coding in Java/JEE: Developing Defensible Applications

.NET

DEV544 Secure Coding in .Net: Developing Defensible Applications

MOBILE DEVICES

DEV551 Secure Mobile Applications Development: IOS Security

DEV568 Secure Mobile Applications Development: Android App Security

SEC542 Web App Penetration Testing and Ethical Hacking

Security Director

Management depends on this expert to measure and report on risk to the organization by measuring compliance with policies, procedures, and standards. These experts are among the few in the organization, who are actually asked for their honest opinion on what could be improved or done better to make the organization more efficient and profitable through risk management.

SEC301 Intro to Information Security
→ **MGT414** SANS® +S™ Training Program for the CISSP® Certification Exam
↓
MGT512 SANS Security Leadership Essentials For Managers with Knowledge Compression™
→ **MGT525** IT Project Management, Effective Communication, and PMP Exam Prep
↓
LEG523 Law of Data Security and Investigations

Cyber Guardian

A Cyber Guardian is a member of elite teams of technical security professionals who are part of the armed forces, Department of Defense, or other government agencies whose role includes securing systems, reconnaissance, counter terrorism, and counter hacks. These teams will be the cyber security special forces where each individual's role makes the team successful.

SEC401 SANS Security Essentials Bootcamp Style
→ **SEC503** Intrusion Detection In-Depth
↓
SEC504 Hacker Techniques, Exploits and Incident Handling
→ **FOR508** Advanced Computer Forensic Analysis and Incident Response

Cyber Guardian – Blue (Defense)

One of the following:

SEC502 Perimeter Protection In-Depth

SEC505 Securing Windows

SEC506 Securing Linux/Unix

Cyber Guardian – Red (Offense)

One of the following:

SEC542 Web App Penetration Testing and Ethical Hacking

SEC617 Wireless Ethical Hacking, Penetration Testing, and Defenses

SEC660 Advanced Penetration Testing, Exploits, and Ethical Hacking

To learn more about these careers and the 20 Coolest Jobs in Information Security, go to:

www.sans.org/20coolestcareers

"SANS is the fastest way to go from an information security beginner to an information security guru."

-David Howard, Emerson

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/security-training.php

SANS Technology Institute

The Premier Skills-Based Cyber Security Graduate School

Master of Science Degree in Information Security Management (MSISM)

Master of Science Degree in Information Security Engineering (MSISE)

Join a cohort of STI students who are admitted in the same academic quarter and develop professional relationships that will enhance your career for years to come.

www.sans.edu

info@sans.edu

720-941-4932

Apply Now!

Rolling Admissions

www.sans.edu

There is an immediate need for highly-qualified information security professionals in both the government and private sector. The SANS Technology Institute offers intensive, hands-on programs with a focus on information security engineering or information security management. STI will arm you with leadership skills as well as the knowledge and expertise necessary to help you obtain a top information security position in government or private industry.

STI students will:

- **Earn a Master's Degree in two to five years (average is three years)**
- **Enter the program, complete courses, perform Community Project Requirements, and graduate with a dynamic group of students**
- **Benefit from a strong, hands-on learning environment**
- **Build professional relationships for the future**
- **Apply skills immediately to their job**

IN THE INFORMATION SECURITY INDUSTRY,

GIAC CERTIFICATION MATTERS

There are a multitude of information security certifications, but only GIAC (Global Information Assurance Certification) builds the true hands-on skills that go beyond theory and tests on the pragmatics of security administration, management, audit, and software security.

GIAC offers more than 20 specialized information security certifications that correspond to specific job duties. The family of GIAC certifications target job-based skill sets rather than taking a one-size fits all approach. The GIAC certification process validates the specific skills of security professionals and developers with standards established on the highest benchmarks in the industry.

Top Four Reasons to Get GIAC Certified

1. **Promotes** hands-on technical skills and improves knowledge retention
2. **Provides** proof that you possess hands-on technical skills
3. **Positions** you to be promoted and earn respect among your peers
4. **Proves** to hiring managers that you are technically qualified for the job

How GIAC Differs from Other Certifications:

- Offers over 20 specialized information security certifications, rather than a one-size fits all approach
- Tests on pragmatics not theory
- RealSkillTest™ exam questions validate real world skills
- Ensures knowledge necessary to complete the task at hand
- Keeps you up to date with the latest industry information

"GIAC is the only certification that proves you have the hands-on technical skills."

-Christina Ford,

Department of Commerce

**GSEC, GSLC, GCIA, GCIH, and GCFA are accredited by the American National Standards Institute (ANSI) under the ANSI/ISO/IEC 17024 program. More certifications will be added in the future. Please check www.giac.org for updates.*

GIAC CERTIFICATION PROGRAM

GIAC certifications may be accomplished in any order. Since specific certification objectives are derived from real-world job duties, we strongly recommend that candidates possess these specific skill sets before attempting certification.

GIAC is uniquely committed to validating the hands-on skills of today's security professional. By offering more disciplines than anyone else in the industry, we are able to focus on the skills required for mastery of specific job duties and technologies.

Candidates earning GIAC certifications and employers who hire them can be confident that a holder of a GIAC certification possesses the skills and know-how to get the job done. The higher-level certifications, Gold and Expert Level, offer a way for outstanding performers to distinguish themselves through even more hands-on focused activities.

Get GIAC Certified

GIAC certification requires passing an on-line, proctored exam based on objectives derived for that specific discipline. GIAC certification assures that an individual possesses the practical real-world skills required for a specific job duty. For example, if you want to hire someone who can properly secure your firewalls and network perimeter, a GIAC Certified Firewall Analyst (GCFW) would be a perfect candidate for the job.

GIAC Gold Program

The GIAC Gold program offers certified individuals the opportunity to demonstrate they possess a deeper knowledge of a specific subject area by researching and writing a detailed technical report. Candidates work closely with a technical advisor while developing their research topic and report. Once complete, the submission is reviewed for acceptance and posted to the GIAC Reading Room. Posted gold papers are a great community resource. GIAC Gold certification shows that not only has an individual mastered a specific subject area, but that they are also qualified to carry out technical research and communicate their specialized knowledge with others in the IT security community.

GIAC Security Expert (GSE)

GIAC Expert Level certification demonstrates an unparalleled level of subject mastery. The GSE is by far the most rigorous and prestigious hands-on credential in the IT security industry, and consists of two days of hands-on performance testing. It is targeted for security engineers, incident handlers, top security consultants, and analysts. The current exam was developed by some of the leading industry practitioners in the world. Those who earn this challenging and well-respected certification may count themselves among the elite in IT security.

The GSE is also part of the SANS Cyberguardian program (www.sans.org.cyber-guardian) and the STI MSISE (engineering) Master's program (www.sans.edu/programs/gse_prep.php).

GSE prerequisite baseline is: GSEC, GCIH, GCIA with two gold or two higher level substitute certifications.

"Those that have the prerequisite certifications and hands-on skill should really consider sitting for the GSE exam. The experience is well worth it. Planning for the exam is a process that makes you learn and sharpens your professional skills. More importantly, the contacts you make through the process really add value to it."

-Craig Wright - GIAC Security Expert

"My GIAC certifications bring credence to the advice and direction I give people. Executive leadership has more confidence in me, and my staff has confidence in my decision-making." -James Caulfield, Federal Reserve Bank

Calculating the Return on Your Training Investment

While most cyber security professionals know how important keeping current on training and certification is to your job, you may be asked to provide an assessment to justify the costs. The return on investment (ROI) calculates the value of an improvement vs. the cost to achieve it. The challenge with cyber security is that gains are typically measured in cost avoidance rather than achievement.

There are Five Types of Losses

Numbers are provided to guide assumptions.

1. **Revenue Loss**
   $7.2 Million Average Organizational Cost of Data Breach
2. **Productivity Loss**
   $966 K in Detection, Escalation, and Notification
3. **Remediation Costs Post Breach**
   $1.7 Million per Ex-Post Response
4. **Loss or Compromise of Data**
   $214 Per Record
5. **Reputational Damage**
   $4.5 million in Loss Business Cost

Source: Cost of a Data Breach Climbs Higher – March 8, 2011 (Ponemon Institute)
www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher

The number one preventive measure to avoid a data breach is training both for your security professionals and your end users.

Worldwide Breaches

- **Negligence – 27%**
- **System Failure – 41%**
- **Malicious or Criminal Attack – 31%**

Tips When Talking with Managers

- Be an expert in the regulatory environment in which you work. Use that to your advantage (PCI HIPAA, DOD8570)
- Speak the same language as your management. Use the same methods to justify this investment as they would see for others (Payback, NPV, IRR)
- Be a pragmatic business partner to the executives
- Just because it is difficult, do not shy away from doing the analysis/justification
- Provide transparency on your assumptions
- Help your executives learn from history – share case studies

Three Common Metrics for ROI

1) Payback – Most common method

- Are the savings greater than the costs?
- Based on the reduction in annualized loss expectancy vs. the cost to achieve that reduction
- Annualized loss expectancy = (Probability of negative event) * (cost of negative event)

Example: *Company is considering training its team of 10 intrusion analysts*

- ☐ Training will reduce the risk of data loss from 20% to 10%.
- ☐ Cost of data loss and damage to reputation to be $2 million
- ☐ The cost of training is $50K
- ☐ Payback:
- Return on Investment: $150,000 = (20%-10%) *$2,000,000 - $50,000
- **Time of Return = Payback within 1/3 a Year** ($50,000/$150,000)

✔ Training is always a good investment, but it's important to remember that company executives may be evaluating other investments that are better for the company at the present time.

	Year 1	Year 2	Year 3	Year 4
Expected Savings	$200,000	$200,000	$200,000	$200,000
Expected Costs	$250,000	$100,000	$100,000	$100,000
Net Savings	$(50,000)	$100,000	$100,000	$100,000
Discounted Net Savings	$(45,455)	$82,645	$75,131	$68,301
Net Present Value	$180,623			
Internal Rate of Return	192%			

Assumption cost of capital (shareholder expected return) 10%

2) Net Present Value (NPV)

- Similar method to payback, but it takes into account the time value of money
- Remember that a dollar earned in the future is worth less than a dollar today. NPV is a better when comparing an expense today that will earn money for years in the future
- Takes into account the company's Cost of Capital

Example: *Company is considering training its team of 10 intrusion analysts and expects to reduce the risk of data loss*

- ☐ Training will reduce the risk of data loss from 20% to 10%.
- ☐ Cost of data loss and damage to reputation to be $2 million
- ☐ Cost of training:
  - Initial cost of training is $250K
  - Continuation training $100k per year for the next 3 years
  - Discounted net savings in year 1 = (-$50,000)/ (1.1)^1
  - Discounted net savings in year 2 = $100,000/(1.1)^2

Conclusion: This is an excellent investment. Remember that any investment with a positive NPV is a good investment.

3) Internal Rate of Return (IRR)

- Usually used in conjunction with NPV
- It is the discount rate which makes an investment NPV = 0
- Using the same example from before
- Thus, by both methods, NPV and IRR this is a good investment

Making the Case for Training

TO MANAGEMENT

Whether it's malware, hackers, or web application vulnerabilities, an attack is expensive. A few associated costs include:

• Loss of consumer trust • Legal fees • Cleaning up systems • Staff hours

In 2010, the average organizational cost of a data breach increased to $7.2 million, up 7% from $6.8 million in 2009. The average cost of a data breach was $214 per record, up $10 from 2009.

2010 Annual Study: U.S. Cost of a Data Breach Survey • Sponsored by PGP Corporation • Independently conducted by Ponemon Institute LLC.

One of the most effective ways to decrease breaches and the associated costs is to train and certify information security staff so they know how to prevent attacks, and what to do if a breach occurs. These critical actions cannot be handled by tools alone – it takes true knowledge and skills.

TO YOURSELF

A recent Kiplinger Letter states that IT firms will add 150,000 jobs this year and would add more if they could. The labor pool of skilled IT workers is tight. Dice.com, a leading IT job-listing site, currently has more than 80,000 postings from companies looking for workers.

The industry jobless rate was just 4.7% in July. For the U.S. as a whole, it was 9.1%.

"The Kiplinger Letter" (Tech section) - Vol 88, No. 32 - 8/12/11.

CASE STUDY

Two government departments were attacked almost simultaneously. Both departments had the proper tools in place, such as firewalls, antivirus, logging, and intrusion detection systems. Unfortunately, the outcomes were not the same.

One department did not discover the attack until the infection spread through the entire IT system. It took over a week to discover the problem and request the help of a third-party. All workstations were unsalvageable and had to be replaced.

The other department located the infection at the entry point in less than a day by using dynamic DNS blocking. They were able to isolate the problem with no user downtime by rebuilding servers, resetting passwords, testing and evaluating captured malicious code, setting up 'tripwires' to detect data theft, and coordinating with Microsoft® to develop a patch.

The difference between these departments was the staff's ability to analyze and react to the attack. Both had invested in the appropriate tools, but one realized that tools were only part of the solution – training of analysts in critical skills and experience in exercises of the topics below were essential:

1. Deep packet intrusion detection
2. In-depth analysis of vulnerabilities and hacker techniques
3. Red teaming/penetration testing
4. Perimeter protection
5. Reverse-engineering malware
6. Script development
7. System and disk forensics

Security 301

Intro to Information Security

Five-Day Program • 9:00am - 5:00pm
30 CPE/CMU Credits • Laptop NOT Required

This introductory certification course is the fastest way to get up to speed in information security. Written and taught by battle-scarred security veterans, this entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security and risk management. Organizations often tap someone who has no information security training and say, "Congratulations, you are now a security officer." If you need to get up to speed fast, SEC301 rocks!

We begin by covering basic terminology and concepts and then move to the basics of computers and networking, discussing Internet Protocol, routing Domain Name Service, and network devices. We cover the basics of cryptography and wireless networking; then we look at policy as a tool to effect change in your organization. In the final day of the course, we put it all together with an introduction to defense in depth.

If you're a newcomer to the field of information security, this is the course for you! You will develop the skills to bridge the gap that often exists between managers and system administrators and learn to communicate effectively with personnel in all departments and at all levels within your organization.

This is the course SANS offers for the professional just starting out in security. If you have experience in the field, please consider our more advanced offerings, such as SEC401: SANS Security Essentials Bootcamp Style.

Who Should Attend:

- Persons new to information technology (IT) who need to understand the basics of information assurance, computer networking, cryptography, and risk evaluation
- Managers and information security officers who need a basic understanding of risk management and the tradeoffs between confidentiality, integrity, and availability
- Managers, administrators, and auditors who need to draft, update, implement, or enforce policy

What Students Are Saying

"This class is great for IT professionals looking for their first step towards security awareness. I have been in IT for 17 years and I learned a lot on this first day of class."

-Paul Beninati, EMC

From the Author

A good friend of mine once said, "A little security is better than no security." If your organization is in either situation (little or no security) and you want to make a difference in a positive way, this course is a great place to start. If your organization has already made an investment in security, this is a great opportunity to compare notes with others and identify how to maximize the return on your investment. Twelve years ago I agreed to fill the position of "number one spear catcher" (the head security guy) for our organization. I asked about training and my predecessor told me that the agency would provide training, but suggested that I work for six months to get some "real-world experience to compare against the theory." It was a long and frustrating six months and the training was less than helpful. A few years later when SANS offered to let me help write and teach this course, I literally jumped at the opportunity. Every time I teach it, I'm excited and I enjoy it as much as the attendees. It's been very gratifying. -Fred Kerby

GIAC Certification
www.giac.org

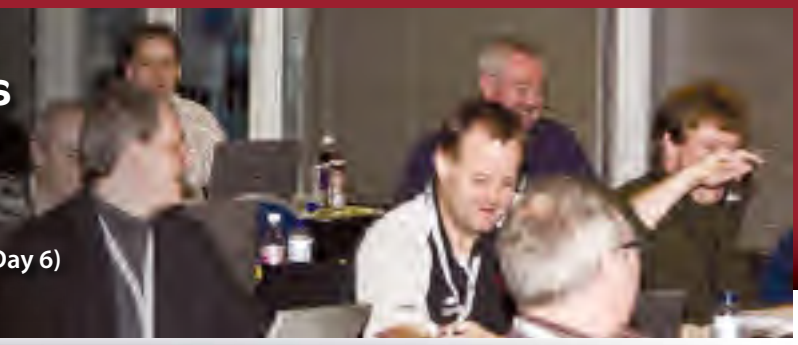
DoD 8570 Required
www.sans.org/8570

Delivery Methods

Live Events
OnDemand
OnSite
SelfStudy

Security 401

SANS Security Essentials Bootcamp Style



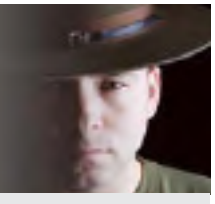
Six-Day Program
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required

Maximize your training time and turbo-charge your career in security by learning the full SANS Security Essentials curriculum needed to qualify for the GSEC certification. In this course you will learn the language and underlying theory of computer security. At the same time you will learn the essential, up-to-the-minute knowledge and skills required for effective performance if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will gain up-to-the-minute knowledge you can put into practice immediately upon returning to work; and, (2) You will be taught by the best security instructors in the industry. As always, great teaching sets SANS courses apart, and SANS ensures this by choosing instructors who have ranked highest in a nine-year competition among potential security faculty.

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
- Anyone new to information security with some background in information systems and networking

Bootcamp



This program has extended hours.
Security 401 PARTICIPANTS ONLY
Evening Bootcamp Sessions:
5:15pm - 7:00pm (Days 1-5)

Attendance is required for the evening bootcamp sessions as the information presented appears on the GIAC exams. These daily bootcamps give you the opportunity to apply the knowledge gained throughout the course in an instructor-led environment. It helps fill your toolbox with valuable tools you can use to solve problems when you go back to work. The material covered is based on Dr. Eric Cole's "Cookbook for Geeks," and most students find it to be one of the highlights of their Security Essentials experience! Students will have the opportunity to install, configure, and use the tools and techniques they have learned. CDs containing the software required will be provided for each student. Students should arrive with a laptop properly configured. A working knowledge of each operating system is recommended but not required. For students who do not wish to build a dual boot machine, SANS will provide a bootable Linux CD for the Linux exercises.

SPECIAL NOTE: This course is endorsed by the Committee on National Security Systems (CNSS) NSTISSI 4013 Standard for Systems Administrators in Information Systems Security (INFOSEC).

Test your security knowledge with our SANS Security Essentials Assessment Test. Get your free test at https://portal.sans.org/assessments

From the Author

One of the things I love to hear from students after teaching Security 401 is "I have worked in security for many years and after taking this course I realized how much I did not know." With the latest version of Security Essentials and the Bootcamp, we have really captured the critical aspects of security and enhanced those topics with examples to drive home the key points. After attending Security 401, I am confident you will walk away with solutions to problems you have had for a while plus solutions to problems you did not even know you had.
-Eric Cole

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

DoD 8570 Required
www.sans.org/8570

Cyber Guardian Program
www.sans.org/cyber-guardian

Delivery Methods
Live Events
Mentor
OnDemand
OnSite
vLive!
SelfStudy

Security 501

Advanced Security Essentials - Enterprise Defender

Six-Day Program • 9:00am - 5:00pm
36 CPE/CMU Credits • Laptop Required

Cyber security will continue to increase in importance as attacks become stealthier, have a greater financial impact on an organization, and cause reputational damage. While Security Essentials lays a solid foundation for the security practitioner, there is only so much that can be packed into a six-day course. SEC501 is a follow up to SEC401: SANS Security Essentials Bootcamp Style (with no overlap) and continues to focus on more technical areas needed to protect an organization. The course focus is on:

- **Prevention** - configuring a system or network correctly
- **Detection** - identifying that a breach has occurred at the system or network level
- **Reaction** - responding to an incident and moving to evidence collection/forensics

A key theme is that prevention is ideal, but detection is a must. We have to ensure that we constantly improve security to prevent as many attacks as possible. Attacks will continue to pose a threat to an organization as data becomes more portable and networks continue to be porous. Therefore a key focus needs to be on data protection both internally and externally - securing our critical information whether it resides on a server, in a robust network architecture, or on a portable device.

Despite our best effort at preventing attacks and protecting critical data, some attacks will still be successful. Therefore we need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic flowing on your networks and looking for indication of an attack. It also includes performing penetration testing and vulnerability analysis against an organization to identify problems and issues before a compromise occurs.

Finally, once an attack has been detected, we must react in a timely fashion and perform forensics. By understanding how the attacker broke in, this can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

Who Should Attend:

- **Students who have taken Security Essentials and want a more advanced 500-level course similar to SEC401**
- **People who have foundational knowledge covered in SEC401, do not want to take a specialized 500-level course, and still want a broad, advanced coverage of the core areas to protect their systems**
- **Anyone looking for detailed technical knowledge on how to protect against, detect, and react to the new threats that will continue to cause harm to an organization**

From the Author

It is always a thrill after I finish teaching SEC401 to see students leave with a fire in their eyes and an excitement about them. They walked into class feeling overwhelmed that security is a lost cause, but now they leave class understanding what they need to do and have a focus and drive to do the right thing to secure their organizations. However the next question we receive on a constant basis is, what course should I take next? How do I continue my journey? Well, it depends on what your focus area is. Do you want to get more into perimeter protection, IDS, operating system security, etc? The challenge is that many students have positions that do not allow them to focus on one area — they need to understand all of the key areas across security. What students are telling us is that they want a Security Essentials part 2 or a 500-level continuation of Security Essentials covering the next level of technical knowledge. In Security 501, SANS has decided to give students just what they have been asking for, and I am beyond thrilled with the results. We have identified core foundation areas that compliment SEC401 with no overlap and continue to build a solid security foundation for network practitioners.

This is illustrated by one student who after a recent class ran up to me, gave me a big hug (he was a retired football player, so I did not argue), and said, "SANS is awesome. I have been frustrated in my job for over a year and had lost hope that you really could secure an organization and that anything I did made a difference. Just as my light of hope was burning out, I decided to take the Security Essentials course, figuring it was a lost cause. After this class the fire is burning brighter than it ever was. I feel like a kid again and cannot wait to go back to my company and make a difference. However, I think my boss is scared because I called him eight times throughout the week, telling him all of the great information and practical knowledge I learned."

After teaching thousands of students, I am confident you will have similar results and be just as excited. However, just for reference, hugs are optional. -Eric Cole

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

DoD 8570 Required
www.sans.org/8570

Delivery Methods

Live Events
OnDemand
OnSite
vLive!
SelfStudy

Security 502

Perimeter Protection In-Depth

Six-Day Program • 9:00am - 5:00pm
36 CPE/CMU Credits • Laptop Required

There is no single fix for securing your network. That's why this course is a comprehensive analysis of a wide breadth of technologies. This is probably the most diverse course in the SANS catalog, as mastery of multiple security techniques is required to defend your network from remote attacks. You cannot just focus on a single OS or security appliance. A proper security posture comprises multiple layers. This course was developed to give you the knowledge and tools necessary at every layer to ensure your network is secure.

The course starts by looking at common problems: Is there traffic passing by my firewall I didn't expect? How did my system get compromised when no one can connect to it from the Internet? Is there a better solution than anti-virus for controlling malware? We'll answer these questions and more.

We all know how to assign an IP address, but to secure your network you really need to understand the idiosyncrasies of the protocol. We'll talk about how IP works and how to spot the abnormal patterns. If you can't hear yourself saying "Hummm, there are no TCP options in that packet. It's probably forged," then you'll gain some real insight from this portion of the material.

Once you have an understanding of the complexities of IP, we'll get into how to control it on the wire. We focus on the underlying technology used by all of the projects rather than telling you which ones are good and which ones are bad. A side-by-side product comparison is only useful for that specific moment in time. By gaining knowledge of what goes on under the cover, you will be empowered to make good product choices for years to come. Just because two firewalls are stateful inspection, do they really work the same on the wire? Is there really any difference between stateful inspection and network-based intrusion prevention, or is it just marketing? These are the types of questions we address in this portion of the course.

We move on to a proper, wire-level assessment of a potential product as well as what options and features are available. We'll even get into how to deploy traffic control while avoiding some of the most common mistakes. Feel like your firewall is generating too many daily entries for you to review the logs effectively? We'll address this problem not by reducing the amount of critical data, but by streamlining and automating the back-end process of evaluating it.

But you can't do it all on the wire. A properly layered defense needs to include each individual host – not just the hosts exposed to access from the Internet, but hosts that have any kind of direct or indirect Internet communication capability as well. We'll start with OS lockdown techniques and move on to third-party tools that can permit you to do anything from sandbox insecure applications to full-blown application policy enforcement.

Most significantly, I've developed this course material using the following guiding principles: learn the process, not just one specific product; you learn more by doing, so hands-on problem-solving is key; and always peel back the layers and identify the root cause. While technical knowledge is important, what really matters are the skills to properly leverage it. This is why the course is heavily focused on problem solving and root cause analysis. While these are usually considered soft skills, they are vital to being an effective security architect. So along with the technical training, you'll receive risk management capabilities and even a bit of Zen empowerment.

Who Should Attend:

- Information security officers
- Intrusion analysts
- IT managers
- Network architects
- Network security engineers
- Network and system administrators
- Security managers
- Security analysts
- Security architects
- Security auditors

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

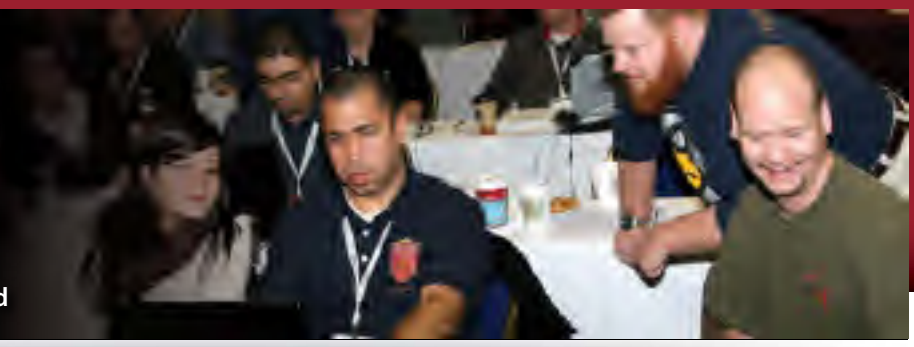
Cyber Guardian Program
www.sans.org/
cyber-guardian

Delivery Methods

Live Events
OnDemand
OnSite
vLive!
SelfStudy

Security 503

Intrusion Detection In-Depth



Six-Day Program • 9:00am - 5:00pm
36 CPE/CMU Credits • Laptop Required

Learn practical hands-on intrusion detection and traffic analysis from top practitioners/authors in the field. This is the most advanced program in network intrusion detection that has ever been taught. This course is jam-packed with network traces and analysis tips.

The emphasis of this course is on improving students' understanding of the workings of TCP/IP, methods of network traffic analysis, and one specific intrusion detection/prevention system (IDS/IPS) - Snort. This is not a comparison or demonstration of multiple IDS/IPS solutions. Instead, the knowledge provided here enables students to better understand the qualities that go into a sound IDS/IPS so they are better equipped to make a wise selection for a site's particular needs.

This is a fast-paced course, and students are expected to have a basic working knowledge of TCP/IP (see www.sans.org/conference/tcpip_quiz.php) in order to fully understand the topics that will be discussed. Although others may benefit from this course, it is most appropriate for students who are or who will become intrusion detection/prevention analysts. Students generally range from novices with some TCP/IP background all the way to seasoned analysts. The challenging hands-on exercises are specially designed to be valuable for all experience levels. We strongly recommend that you spend some time getting familiar with tcpdump or windump before coming to class.

Who Should Attend:

- Intrusion detection analysts (all levels)
- Network engineers
- System, security, and network administrators
- Hands-on security managers

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

DoD 8570 Required
www.sans.org/8570

Cyber Guardian Program
www.sans.org/cyber-guardian

Delivery Methods

Live Events
Mentor
OnDemand
OnSite
vLive!
SelfStudy

What Students Are Saying

"This class heightens your security awareness on protecting your network and provides excellent examples, in detail, on how to accomplish this."

-Laura Freeman, DND

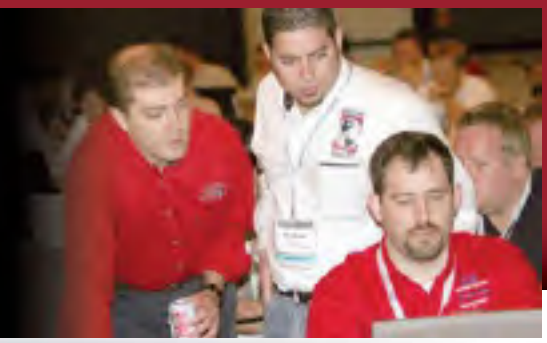
Mike Poor

From the Author

Guy Bruneau, Mike Poor, and I have worked as intrusion analysts for many years. Over the years, we have seen our fair share of attacks and suspicious traffic often leading to intrusions. Over time, we have developed various analysis techniques that work on new detects that we have learned to pass on to the students. Attendees will learn how TCP/IP really works from instructors that have spent thousands of hours analyzing, researching and categorizing suspicious traffic with a variety of security tools. You will learn from hundreds of old and current examples of detects that were captured in the real world and be able to apply these real world examples to analyze known and new intrusion patterns. We are confident that students will put the training they receive from this course into practice the day they get back to the office. - Judy Novak, Guy Bruneau, and Mike Poor

Security 504

Hacker Techniques, Exploits, and Incident Handling



Six-Day Program • 9:00am - 5:00pm
36 CPE/CMU Credits • Laptop Required

If your organization has an Internet connection or 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.

By helping you understand attackers' 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, the in-depth information in this course helps you turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them; and a hands-on workshop for discovering holes before the bad guys do. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

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

What Students Are Saying

"This class heightens your security awareness on protecting your network and provides excellent examples, in detail, on how to accomplish this."

-Laura Freeman, DND

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

It is imperative that you get written permission from the proper authority in your organization before using these tools and techniques on your company's system and also that you advise your network and computer operations teams of your testing.

From the Author

My favorite part of teaching Hacker Techniques, Exploits, and Incident Handling is watching students when they finally get it. It's usually a two-stage process. First, students begin to realize how truly malicious some of these attacks are. Some students have a very visceral reaction, occasionally shouting out "Oh, shoot!" when they see what the bad guys are really up to. But if I stopped the process at that point, I'd be doing a disservice. The second stage is even more fun. Later in the class, students gradually realize that, even though the attacks are really nasty, they can prevent, detect, and respond to them. Using the knowledge they gain in this track, they know they'll be ready when a bad guy launches an attack against their systems. And being ready to thwart the bad guys is what it's all about. -Ed Skoudis

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

DoD 8570 Required
www.sans.org/8570

Cyber Guardian Program
www.sans.org/
cyber-guardian

Delivery Methods

Live Events
Mentor
OnDemand
OnSite
vLive!
SelfStudy

Security 505

Securing Windows

Six-Day Program • 9:00am - 5:00pm
36 CPE/CMU Credits • Laptop Required

Will you be transitioning from Windows XP to Windows 7? The SEC505: Securing Windows course is fully updated for Windows Server 2008-R2 and Windows 7. Most of the content applies to Windows Server 2003 and XP too, but the focus is on 2008/Vista/7.

Concerned about the 20 Critical Security Controls of the Consensus Audit Guidelines? This course will help you implement , not just audit, the critical controls relevant to Windows systems and will also walk you through most of the tools step by step, too.

As a Windows security expert, how can you stand out from the crowd and offer management more than the usual apply-this-checklist advice? Be a security architect who understands the big picture. You can save your organization money, maintain compliance with regulations, secure your networks, and advance your career all at the same time. How? By leveraging the Windows infrastructure you've already paid for.

Who Should Attend:

- Windows network security engineers and architects
- Windows administrators with security duties
- Anyone with Windows machines who wants to implement the SANS 20 Critical Security Controls
- Active Directory designers and administrators
- Those who must enforce security policies on Windows hosts
- Those deploying or managing a PKI or smart cards
- IIS administrators and webmasters with web servers at risk
- Administrators who use the command line or scripting to automate their duties and must learn PowerShell (the replacement for CMD scripting and VBScript)

This program is a comprehensive set of courses for Windows security architects and administrators. It tackles tough problems like Active Directory forest design, how to use Group Policy to lock down desktops, deploying a Microsoft PKI and smart cards, pushing firewall and IPSec policies out to every computer in the domain, securing public IIS web servers, and PowerShell scripting.

PowerShell is the future of Windows scripting and automation. Easier to learn and more powerful than VBScript, PowerShell is an essential tool for automation and scalable management. If there is one skill that will most benefit the career of a Windows specialist, it's scripting. Most of your competition lacks scripting skills, so it's a great way to make your resume stand out. Scripting skills are also essential for being able to implement the 20 Critical Security Controls.

You are encouraged to bring a virtual machine running Windows Server 2008 Enterprise Edition configured as a domain controller, but this is not a requirement for attendance since the instructor will demo everything discussed on-screen. You can get a free evaluation version of Server 2008 from Microsoft's website (just do a Google search on "site:microsoft.com Server 2008 trial"). You can use VMware, Virtual PC, or any other virtual machine software.

This is a fun and fascinating course, a real eye-opener even for Windows administrators with years of experience. Come see why there's a lot more to Windows security than just applying patches and changing passwords; come see why a Windows network needs a security architect.

From the Author

I've happily been with SANS for over a decade, and the courses I write are always guided by two questions:
1) What do administrators need to know to secure their networks? and 2) What should administrators learn to advance their careers as IT professionals? I'm not a Microsoft employee or a Microsoft-basher, so you won't get either kind of propaganda here; my concern is with the health of your network and your career. As a security consultant I've seen it all (good, bad, and ugly), and my experience goes into the manuals I write for SANS and the stories I tell in seminars. The Securing Windows course is packed with interesting and useful advice that is hard or impossible to find on the Internet. We always have a good time, so I hope to meet you at the next training event! -Jason Fossen

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/
cyber-guardian

Delivery Methods

Live Events
OnDemand
OnSite
vLive!
SelfStudy

Security 542

Web App Penetration Testing and Ethical Hacking

Six-Day Program • 9:00am - 5:00pm
36 CPE/CMU Credits • Laptop Required

Assess Your Web Apps in Depth

Web applications are a major point of vulnerability in organizations today. Web app holes have resulted in the theft of millions of credit cards, major financial and reputational damage for hundreds of enterprises, and even the compromise of thousands of browsing machines that visited websites altered by attackers. In this intermediate- to advanced-level class, you'll learn the art of exploiting web applications so you can find flaws in your enterprise's web apps before the bad guys do. Through detailed, hands-on exercises and training from a seasoned professional, you will be taught the four-step process for web application penetration testing. You will inject SQL into back-end databases, learning how attackers exfiltrate sensitive data. You will utilize cross-site scripting attacks to dominate a target infrastructure in our unique hands-on laboratory environment. And you will explore various other web app vulnerabilities in depth with tried-and-true techniques for finding them using a structured testing regimen. You will learn the tools and methods of the attacker so that you can be a powerful defender.

Who Should Attend:

- General security practitioners
- Website designers and architects
- Developers

On day one, we will study the attacker's view of the web as well as learn an attack methodology and how the pen-tester uses JavaScript within the test. On day two we will study the art of reconnaissance, specifically targeted to web applications. We will also examine the mapping phase as we interact with a real application to determine its internal structure. During day three we will continue our test by starting the discovery phase using the information we gathered on day two. We will focus on application/server-side discovery. On day four we will continue discovery, focusing on client-side portions of the application, such as Flash objects and Java applets. On day five we will move into the final stage of exploitation. Students will use advanced exploitation methods to gain further access within the application. Day six will be a Capture the Flag event where the students will be able to use the methodology and techniques explored during class to find and exploit the vulnerabilities within an intranet site.

What Students Are Saying

"This is the first course I have taken where I was completely unaware of time – very engaging. Kevin is very knowledgeable and an excellent representative of the SANS Institute." -Scott Ashton, Police & Fire FCU

Throughout the class, you will learn the context behind the attacks so that you intuitively understand the real-life applications of our exploitation. In the end, you will be able to assess your own organization's web applications to find some of the most common and damaging Web application vulnerabilities today.

By knowing your enemy, you can defeat your enemy. General security practitioners, as well as website designers, architects, and developers, will benefit from learning the practical art of web application penetration testing in this class.

From the Author

Testing the security of web applications is not as simple as just knowing what SQL injection and cross-site scripting mean. Successful testers understand that methodical, thorough testing is the best means of finding the vulnerabilities within the applications. This requires a deep understanding of how web applications work and what attack vectors are available. This course provides that understanding by examining the various parts of a web application penetration. When teaching the class, I especially enjoy the use of real-world exercises and the in-depth exploration of web penetration testing. -Kevin Johnson

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/
cyber-guardian

Delivery Methods

Live Events
OnDemand
OnSite
vLive!
SelfStudy

Security 560

Network Penetration Testing and Ethical Hacking

Six-Day Program • 9:00am - 5:00pm
36 CPE/CMU Credits • Laptop Required

Equipping Security Organizations with Advanced Penetration Testing and Ethical Hacking Know-How

Security vulnerabilities, such as weak configurations, unpatched systems, and botched architectures, continue to plague organizations. Enterprises need people who can find these flaws in a professional manner to help eradicate them from our infrastructures. Lots of people claim to have penetration testing, ethical hacking, and security assessment skills, but precious few can apply these skills in a methodical regimen of professional testing to help make an organization more secure. This class covers the ingredients for successful network penetration testing to help attendees improve their enterprise's security stance.

We address detailed pre-test planning, including setting up an effective penetration testing infrastructure and establishing ground rules with the target organization to avoid surprises and misunderstanding. Then we discuss a time-tested methodology for penetration and ethical hacking across the network, evaluating the security of network services and the operating systems behind them.

Who Should Attend:

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing target networks and systems to find security vulnerabilities

Attendees will learn how to perform detailed reconnaissance, learning about a target's infrastructure by mining blogs, search engines, and social networking sites. We'll then turn our attention to scanning, experimenting with numerous tools in hands-on exercises. Our exploitation phase will include the use of exploitation frameworks, stand-alone exploits, and other valuable tactics, all with hands-on exercises in our lab environment. The class also discusses how to prepare a final report, tailored to maximize the value of the test from both a management and technical perspective. The final portion of the class includes a comprehensive hands-on exercise, following all of the steps to conduct a penetration test against a hypothetical target organization.

The course also describes the limitations of penetration testing techniques and other practices that can be used to augment penetration testing to find vulnerabilities in architecture, policies, and processes. We also address how penetration testing should be integrated as a piece of a comprehensive enterprise information security program.

What Students Are Saying

"This course taught me how to become a GIAC-certified professional! The instructor's professionalism and the layout/material of the course has opened up a whole new paradigm and career opportunity for me."

-Gene Wikle, SAIC, Inc.

From the Author

Successful penetration testers don't just throw a bunch of hacks against an organization and regurgitate the output of their tools. Instead, they need to understand how these tools work in depth and conduct their test in a careful, professional manner. This course explains the inner workings of numerous tools and their use in effective network penetration testing and ethical hacking projects. When teaching the class, I particularly enjoy the numerous hands-on exercises culminating with a final pen-testing extravaganza lab. -Ed Skoudis

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/
cyber-guardian

Delivery Methods

Live Events
OnDemand
OnSite
vLive!
SelfStudy

Security 566

Implementing and Auditing the Twenty Critical Security Controls – In Depth

Five-Day Program • 9:00am - 5:00pm
30 CPE/CMU Credits • Laptop Required

In the last couple of years it has become obvious that in the world of information security, the offense is outperforming the defense. Even though budgets increase and management pays more attention to the risks of data loss and system penetration, data is still being lost and systems are still being penetrated. Over and over people are asking, "What can we practically do to protect our information?" The answer has come in the form of 20 information assurance controls known as the Consensus Audit Guidelines (CAG), located at www.sans.org/critical-security-controls/guidelines.php.

This course has been written to help those setting/implementing/deploying a strategy for information assurance in their agency or organization by enabling them to better understand these guidelines. Specifically the course has been designed in the spirit of the offense teaching the defense to help security practitioners understand not only how to stop a threat, but why the threat exists and how later to audit to ensure that the organization is indeed in compliance with their standards. Walking away from this course, students should better understand how to create a strategy for successfully defending their data, implement controls to prevent their data from being compromised, and audit their systems to ensure compliance with the standard. And in SANS style, this course will not only provide a framework for better understanding, but also give you a hands-on approach to learning these objectives to ensure that what you learn today you'll be able to put into practice in your organization tomorrow.

Who Should Attend:

- Information assurance auditors
- System implementers/administrators
- Network security engineers
- IT administrators
- DoD personnel/contractors
- Federal agencies/clients
- Private sector organizations looking for information assurance priorities for securing their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD 440, SEC401, SEC501, SANS Audit classes, and MGT512

This course helps you master specific, proven techniques and tools needed to implement and audit the Top Twenty Most Critical Security Controls. These Top 20 Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. These controls were selected and defined by the US military and other government and private organizations (including NSA, DHS, GAO, and many others) who are the most respected experts on how attacks actually work and what can be done to stop them. They defined these controls as their consensus for the best way to block the known attacks and the best way to help find and mitigate damage from the attacks that get through. For security professionals, the course enables you to see how to put the controls in place in your existing network though effective and widespread use of cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Top 20 controls are effectively implemented. It closely reflects the Top 20 Critical Security Controls found at www.sans.org/critical-security-controls/guidelines.php.

James Tarala

From the Author

As we've had the opportunity to talk with information assurance engineers, auditors, and managers over the past ten years, we've seen frustration in the eyes of these hardworking individuals who are trying to make a difference in their organizations by better defending their data systems. It has even come to the point where some organizations have decided that it's simply too hard to protect their information, and many have started to wonder, is the fight really worth it? Will we ever succeed? We see companies and agencies making headway, but the offense keeps pushing. The goal of this course is to give direction and a realistic hope to organizations attempting to secure their systems.

The 20 Critical Security Controls: Planning, Implementing and Auditing offers direction and guidance from those in the industry that think through the eyes of the attacker as to what security controls will make the most impact. What better way to play defense than by understanding the mindset of the offense? By implementing our defense methodically and with the mindset of a hacker, we think organizations have a chance to succeed in this fight. We hope this course helps turn the tide.

-Dr. Eric Cole and James Tarala

What Students Are Saying

"The course material is put together in such a way that you will be able to follow it like a recipe in your real-life environment."

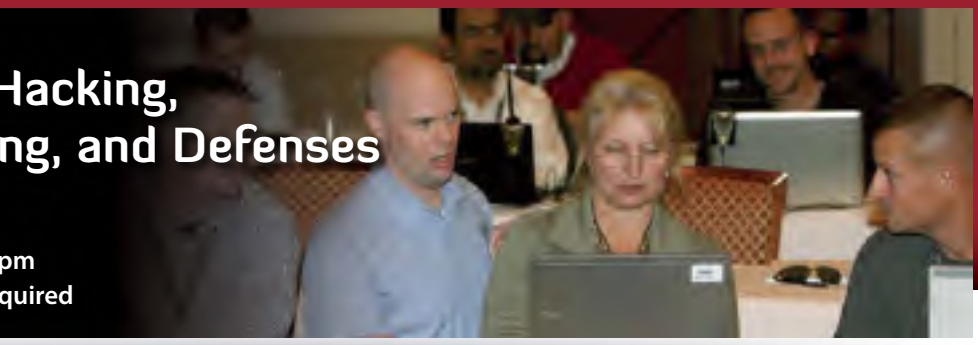
-Jane Citino, Verizon Wireless

Delivery Methods

Live Events
OnDemand
OnSite
vLive!
SelfStudy

Security 617

Wireless Ethical Hacking, Penetration Testing, and Defenses



Six-Day Program • 9:00am - 5:00pm
36 CPE/CMU Credits • Laptop Required

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, but it is growing in deployment and utilization with wireless LAN technology and WiFi as well as other applications, including cordless telephones, smart homes, embedded devices, and more. Technology such as ZigBee and WiMAX offer new methods of connectivity to devices, while other wireless technology, including WiFi, Bluetooth, and DECT, continue their massive growth rate, each introducing their own set of security challenges and attacker opportunities.

To be a wireless security expert, you need to have a comprehensive understanding of the technology, the threats, the exploits, and the defense 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, including developing attack techniques leveraging Windows 7 and Mac OS X. We'll also 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.

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

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.

In terms of technical content, SEC617 ranks up at the top for in-depth, comprehensive information about wireless security. However, you don't need to be an expert in wireless technology to succeed in this course. To help students consume the course content, I've written extensive notes for every topic, complete with review question and answer sections and recommendations for additional reading if you want to dig deeper. Many students comment that their favorite part about the course is the hands-on time, which makes up a significant part of the course. Classroom labs are written such that even if you have never used wireless technology or a Linux system before, you'll be able to complete all exercises and reproduce your results against your own networks when you return to the office. Everyone can take this class and gain useful and valuable skills for attacking and defending wireless networks.

From the Author

It's been amazing to watch the progression of wireless technology over the past several years. WiFi has grown in maturity and offers strong authentication and encryption options to protect networks, and many organizations have migrated to this technology. At the same time, attackers are becoming more sophisticated, and we've seen significant system breaches netting millions of payment cards that start with a wireless exploit. This pattern has me very concerned, as many organizations, even after deploying WPA2 and related technology, remain vulnerable to a number of attacks that expose their systems and internal networks. In putting this class together, I wanted to help organizations recognize the multi-faceted wireless threat landscape and evaluate their exposure through ethical hacking techniques. Moreover, I wanted my students to learn critical security analysis skills so that, while we focus on evaluating wireless systems, the vulnerabilities and attacks we leverage to exploit these systems can be applied to future technologies as well. In this manner, the skills you build in this class remain valuable for today's wireless technology, tomorrow's technology advancements, and for other complex systems you have to evaluate in the future as well. If you have questions or comments about this course, I would be very happy to hear from you. Please e-mail me at jwright@sans.org. -Joshua Wright

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

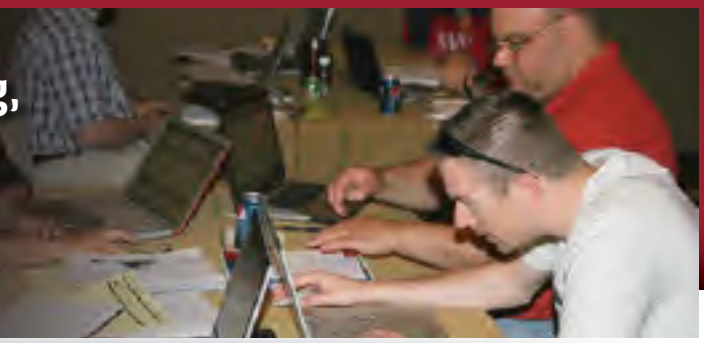
Cyber Guardian Program
www.sans.org/cyber-guardian

Delivery Methods

Live Events
OnDemand
OnSite
vLive!
SelfStudy

Security 660

Advanced Penetration Testing, Exploits, and Ethical Hacking



Six-Day Program
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required

Preparing Students for the Next Generation of Attacks

It is well-known that attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, one must have a strong desire to learn, the support of others, and the opportunity to practice and build experience. SEC660 engages 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 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.

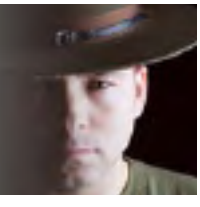
Who Should Attend:

- Network and Systems Penetration Testers
- Incident Handlers
- Application Developers
- IDS Engineers

The course starts off by introducing advanced penetration concepts, which will become the focus throughout the course. The course quickly dives deep into modern operating system controls, which stump many attackers and penetration testers. There are often ways around controls, such as address space layout randomization (ASLR), data execution prevention (DEP), canaries, and many others. These controls are introduced on day one and defeated at various points throughout the course. The remainder of the day is spent using the Python programming language for penetration testing. Scripting skills are essential to automate and speed up scanning, perform fuzzing, as well as launch exploits. Evening labs each day are used to allow for additional time practicing the techniques learned.

Day two jumps into accessing, manipulating, and exploiting the network. Attacks are performed against NAC, VLANs, DHCP, 802.1X, CDP, VOIP, ARP, SNMP, and others. Day three takes a look at very successful attacks against Windows domain environments. Topics include breaking out of RDP sessions, performing MitM attacks against Kerberos and RDP, downgrading authentication protocols, harvesting passwords in unusual locations, and many others. Days four and five are spent exploiting programs on the Linux and Windows operating systems. You will learn to identify privileged programs, redirect code execution in debuggers, reverse-engineer programs to locate vulnerable code, obtain code execution for administrative shell access, and defeat modern operating system controls, such as ASLR and DEP. Client-side attacks are also covered, and you will understand how to perform vulnerability discovery and exploit development. The final course day is dedicated to numerous penetration testing challenges requiring you to solve complex problems and capture flags.

Bootcamp



This program has extended hours.

Evening Bootcamp Sessions:
5:15pm - 7:00pm (Days 1-5)

What Students Are Saying

"SANS provides 'the' best curriculum, steeped in tons of real-world scenarios." -KTH Parts Industries

From the Author

As a perpetual student of information security, I am excited to offer this course on advanced penetration testing. Often, when conducting an in-depth penetration test, we are faced with situations that require unique or complex solutions to successfully pull off an attack, mimicking the activities of increasingly sophisticated real-world attackers. Without the skills to do so, you may miss a major vulnerability or not properly assess its business impact. Target system personnel are relying on you to tell them whether or not an environment is secured. Attackers are almost always one step ahead and are relying on our nature to become complacent with controls we work so hard to deploy. This course was written to keep you from making mistakes others have made, teach you cutting-edge tricks to thoroughly evaluate a target, and provide you with the skills to jump into exploit development. Contact me at stephen@deadlisting.com if you have any questions about the course! -Stephen Sims

GIAC Certification
www.giac.org

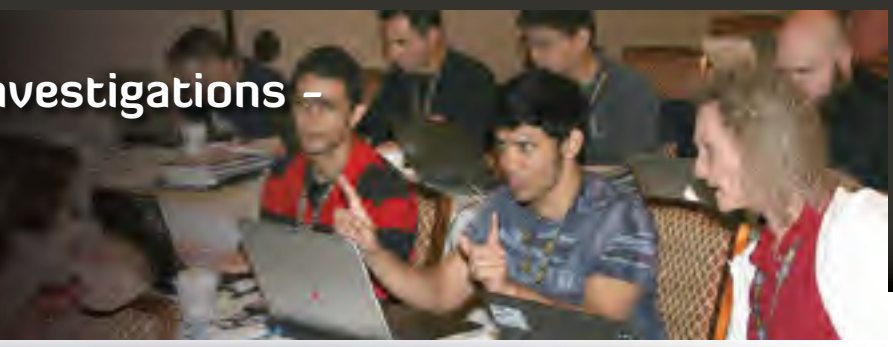
STI Graduate School
www.sans.edu

Delivery Methods

Live Events
OnSite
vLive!
SelfStudy

Forensics 408

Computer Forensic Investigations - Windows In-Depth



Six-Day Program • 9:00am - 5:00pm
36 CPE/CMU Credits • Laptop Required

Master computer forensics. Learn critical investigation techniques. With today's ever-changing technologies and environments, it is inevitable that every organization will deal with cybercrime including fraud, insider threat, industrial espionage, and phishing. In addition, government agencies are now performing media exploitation to recover key intelligence kept on adversary systems. In order to help solve these cases, organizations are hiring digital forensic professionals and calling cybercrime law enforcement agents to piece together what happened in these cases.

This course covers the fundamental steps of the in-depth computer forensic and media exploitation methodology so that each student will have the complete qualifications to work as a computer forensic investigator in the field helping solve and fight crime. In addition to in-depth technical digital forensic knowledge on Windows Digital Forensics (Windows XP through Windows 7 and Server 2008), you will be exposed to well-known computer forensic tools so such as Access Data's Forensic Toolkit (FTK), Guidance Software's EnCase, Registry Analyzer, FTK Imager, Prefetch Analyzer, and much more.

Who Should Attend:

- Information technology professionals
- Incident Response Team Members
- Law enforcement officers, federal agents, or detectives
- Media Exploitation Analysts
- Information security managers
- Information technology lawyers and paralegals
- Anyone interested in computer forensic investigations

FOR408: COMPUTER FORENSIC INVESTIGATIONS - WINDOWS IN-DEPTH is the first course in the SANS Computer Forensic Curriculum. If this is your first computer forensics course with SANS we recommend that you start here.

You will receive with this course:
Free SANS Investigative Forensic Toolkit (SIFT) Essentials

As a part of this course you will receive a SANS Investigative Forensic Toolkit (SIFT) Essentials with a Tableau Write Block Acquisition Kit.

- **Tableau T35es Write Blocker Kit**
- **SANS VMware-Based Forensic Analysis VMware Workstation**
- **Course DVD: Loaded with case examples, tools, and documentation**

From the Author

After 25 years in law enforcement, when I think of what makes a great digital forensic analyst, three things immediately rise to the top of my list. Superior Technical Skill, Sound Investigative Methodology, and the Ability to Overcome Obstacles. SANS FOR408, Windows In-Depth was designed around imparting these critical skills to the students. Unlike many other training courses that focus on teaching a single tool, SANS 408 provides training on over 25 tools. While there are some really exceptional tools available, we feel every forensicator needs a variety of tools in their arsenal so they can pick and choose the best tool for each task. But we also understand that a great forensics analyst is not great because of the tool(s) they use, but because they artfully apply the right investigative methodology to each analysis. A carpenter can be a master with all his tools and still not know how to build a house. SANS 408 is designed to teach and allow each student to apply digital forensic methodologies for a variety of case types and situations, allowing them to apply in the real world the right methodology to achieve the best outcome. Finally, this course is designed to teach and demonstrate problem-solving skills necessary to be a truly successful forensicator. Almost immediately after starting your forensic career, you learn each forensic analysis presents its own unique challenges. A technique that worked flawlessly in previous exams may not work in the next. A good forensicator must be able to overcome obstacles through advanced trouble shooting and problem solving. SANS 408 gives students the foundation that will allow them to solve future problems, overcome obstacles and become great forensicators. No matter if you are new to the forensic community or have been doing forensics for years, SANS 408 is a must have course. – Ovie Carroll

Forensics
http://computer-forensics.sans.org

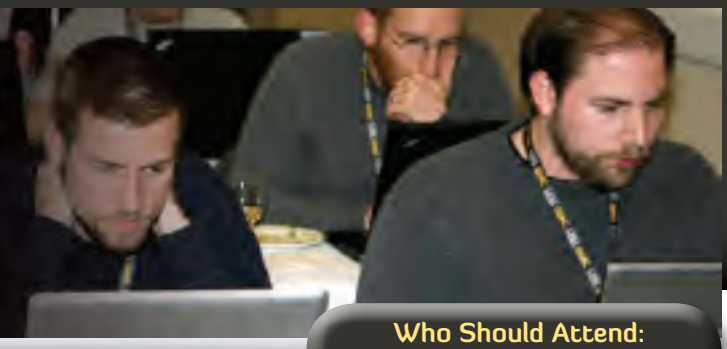
GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Delivery Methods
Live Events
OnDemand
OnSite
vLive!
SelfStudy

Forensics 508

Advanced Computer Forensic Analysis & Incident Response



Six-Day Program • 9:00am - 5:00pm
36 CPE/CMU Credits • Laptop Required

Who Should Attend:

- Incident response team members
- Experienced digital forensic analysts
- Law Enforcement Officers, Federal agents, or detectives
- Media exploitation analysts
- Red team members, penetration testers, and exploit developers
- Information security professionals

Data breaches and advanced intrusions are occurring daily. Sensitive personal data, credit cards, and intellectual property are stolen easily from enterprise networks that are protected by sophisticated network and host based security systems. A motivated criminal group or nation state can and will always find a way inside enterprise networks. In the commercial and government sectors, hundreds of victims responded to serious intrusions costing millions of dollars and loss of untold terabytes of data. Cyber attacks originating from China named the Advanced Persistent Threat (APT) have proved difficult to suppress. Financial attacks from Eastern Europe and Russia obtain credit card, and financial data that have resulted in millions of dollars being stolen.

FOR508: ADVANCED COMPUTER FORENSIC ANALYSIS AND INCIDENT RESPONSE will help you start to become a master of advanced incident response and computer forensics tools and techniques to investigate data breach intrusions, tech-savvy rogue employees, the advanced persistent threat, and complex digital forensic cases.

FIGHT CRIME. UNRAVEL INCIDENTS... ONE BYTE AT A TIME.

You will receive with this course:
Free SANS Investigative Forensic Toolkit (SIFT) Advanced

The SIFT Advanced Toolkit consists of:

- **F-Response Tactical**
  - **Tactical enables investigators to access remote system via the network**
  - **Perfect for incident response investigating compromised systems**
- **SANS VMware based Forensic Analysis Workstation (SIFT Workstation)**
- **Best-selling book "File System Forensic Analysis" by Brian Carrier**
- **Bootable Forensic Distribution**
- **Course DVD loaded with case examples, tools, and documentation**

What Students Are Saying

"Intense, fast paced. Modern-day Sherlock Holmes!"

-Cody Drake, Allstate Ins. Co.

From the Author

"There are people smarter than you, they have more resources than you, and they are coming for you. Good luck with that." Matt Olney said when describing the Advanced Persistent Threat. He was not joking. The results over the past several years clearly indicate that hackers employed by nation states and organized crime are racking up success after success. The Advanced Persistent Threat has compromised hundreds of organizations. Organized crime utilizing botnets are exploiting ACH fraud daily. Similar groups are penetrating banks and merchants stealing credit card data daily. Fortune 500 companies are beginning to detail data breaches and hacks in their annual stockholders reports.

The enemy is getting better, bolder, and their success rate is impressive.

We can stop them. We need to field more sophisticated incident responders and digital forensic investigators. We need lethal digital forensic experts that can detect and eradicate advanced threats immediately. A properly trained incident responder could be the only defense your organization has left in place during a compromise. Forensics 508: Advanced Computer Forensic Analysis and Incident Response is crucial training for you to become a lethal forensicator to step up to these advanced threats. The enemy is good. We are better. This course will help you become one of the best. -Rob Lee

Digital Forensics and Incident Response
http://computer-forensics.sans.org

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/cyber-guardian

Delivery Methods

Live Events
OnDemand
OnSite
vLive!
SelfStudy

Forensics 558

Network Forensics

Five-Day Program
9:00am - 6:30pm (Day 1), 9:00am - 5:00pm (Days 2-5)
31.5 CPE/CMU Credits • Laptop Required

Enterprises all over the globe are compromised remotely by malicious hackers each day. Credit card numbers, proprietary information, account usernames and passwords, and a wealth of other valuable data are surreptitiously transferred across the network. Insider attacks leverage cutting-edge covert tunneling techniques to export data from highly secured environments. Attackers' fingerprints remain throughout the network, in firewall logs, IDS/IPS, web proxies, traffic captures, and more.

Who Should Attend:

- Incident response team members
- Network and computer forensic professionals
- Law enforcement officers, federal agents, or detectives
- Information security professionals
- Network security professionals
- Anyone asked to investigate a data breach incident or intrusion case

FOR558 will teach you to how to follow the attacker's footprints and analyze evidence from the network environment. Every student will receive a VMware SNIFT Virtualized Workstation, which is a fully-loaded, portable forensics virtual workstation, designed by network forensics experts and distributed exclusively to Forensics 558: Network Forensics students. You are required to bring your own laptop configured using the specifications found under the laptop requirements.

Network equipment such as web proxies, firewalls, IDS, routers and even switches contain evidence that can make or break a case. Forensic investigators must be savvy enough to find network-based evidence, preserve it and extract the evidence. Forensics 558: Network Forensics will give you hands-on experience analyzing covert channels, carving cached web pages out of proxies, carving images from IDS packet captures, and correlating the evidence to build a solid case.

We will begin by diving right into covert tunnel analysis, DHCP log examination, and sniffing traffic. By day two, you'll be extracting tunneled flow data from DNS NULL records and extracting evidence from firewall logs. On day three, we analyze Snort captures and the web proxy cache. You'll carve out cached web pages and images from the Squid web proxy.

For the last two days, you'll be part of a live hands-on investigation. Working in teams, you'll use network forensics to solve a crime and present your case.

During hands-on exercises, we will use tools such as tcpdump, Snort, ngrep, tcpxtract, and Wireshark to understand attacks and trace suspect activity. Each student will be given a virtual network to analyze, and will have the opportunity to conduct forensic analysis on a variety of devices.

Underlying all of our forensic procedures is a solid forensic methodology. This course complements Forensic and Investigative Essentials (508), using the same fundamental methodology to recover and analyze evidence from network-based devices.

From the Author

Traditionally, computer forensics has focused on file recovery and filesystem analysis performed against system internals or seized storage devices. However, the hard drive is only a small piece of the story. These days, evidence almost always traverses the network and sometimes is never stored on a hard drive at all.

With network forensics, the entire contents of e-mails, IM conversations, Web surfing activities, and file transfers can be recovered from network equipment and reconstructed to reveal the original transaction. The payload inside the packet at the highest layer may end up on disc, but the envelope that got it there is only captured in the network traffic. The network protocol data that surrounded each conversation is often extremely valuable to the investigator. Network forensics enables investigators to piece together a more complete picture using evidence from the entire network environment. -Jonathan Ham

Digital Forensics and Incident Response
http://computer-forensics.sans.org

No Hard Drive? No Problem!

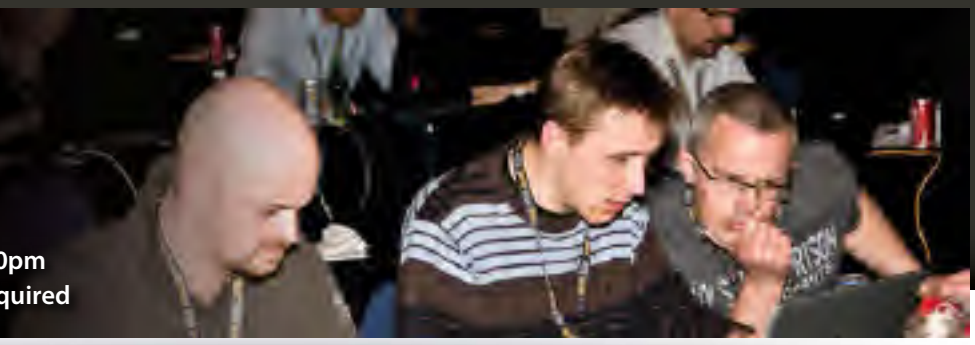
A hard drive is just a small part of the picture. Even if an attacker is smart enough to clean up tracks on the victim system, remnants remain in firewall logs, web proxy caches, and other sources. Forensics 558: Network Forensics, you'll learn to track attackers through the network and leverage network evidence to build a strong case.

Delivery Methods

Live Events
OnDemand
OnSite
vLive!
SelfStudy

Forensics 563

Mobile Device Forensics



Five-Day Program • 9:00am - 5:00pm
30 CPE/CMU Credits • Laptop Required

Mobile device forensics is a rapidly evolving field, creating exciting opportunities for practitioners in corporate, criminal, and military settings. Designed for students who are both new to and already familiar with mobile device forensics, this hands-on course provides the core knowledge and skills that a Digital Forensic Investigator needs to process cell phones, PDAs, and other mobile devices. Using state-of-the art tools, you will learn how to forensically preserve, acquire and examine data stored on mobile devices and utilize the results for internal investigations or in civil/criminal litigation. This course covers techniques and tools in the context of an overall forensic methodology, providing you with the ability to obtain and utilize digital evidence on mobile devices. In addition, by teaching lessons learned from years of experience, we will help you learn how to handle common challenges in the field.

With the increasing prevalence of mobile devices, Digital Forensic Investigators are encountering them in a wide variety of cases. Investigators within organizations can find stolen data and incriminating communications on devices used by rogue employees. In civil and criminal cases, investigators can extract useful evidence from mobile devices, can get a clearer sense of which individuals were in cahoots, and can even show the location of key suspects at times of interest. IT auditors, managers, and lawyers all need to understand the vast potential of mobile device forensics. Because mobile devices can contain details about who was doing what, where and when, their usefulness as a source of information in an investigation should never be underestimated.

Throughout this course we provide practical, hands-on exercises to give you ample opportunities to explore mobile devices and the data they contain.

Who Should Attend:

- Information security professionals
- Law enforcement officers, federal agents, or detectives
- Media exploitation analysts
- Information security managers
- Information technology lawyers and paralegals
- Anyone interested in mobile device forensics
- Information technology auditors

By guiding you through progressively more intensive exercises with mobile devices, we familiarize you with the inner workings of these devices and show you the benefits and limitations of various approaches and tools. We not only demonstrate state-of-the-art mobile forensic tools and techniques, we peel back the layers of digital evidence on mobile devices to show what is going on behind the scenes. In this way, you obtain a deeper knowledge of the information you rely on when investigating cases involving mobile devices. This combination of teaching skills and knowledge will enable you to resolve investigations. The capstone exercise at the end of this course is designed to hone your mobile device forensics skills, and help you to apply them to an actual investigation.

From the Author

Mobile devices are becoming ubiquitous, delivering powerful technology into our pockets, keeping us connected wherever we are. Individuals store personal data on their PDAs, parents use GPS enabled devices to track their children, hospitals use handhelds to access medical data and support patient care, and companies give each employee a Blackberry to support their business. Being so closely tied to an individual's daily movements and activities, these portable devices are creating new security risks while providing valuable sources of evidence.

Corporate spies and data thieves have been caught using their mobile devices. Organized criminal groups have been infiltrated and unraveled through their use of mobile devices. A killer's mobile device showed his whereabouts at the time of the crime, and inadvertently recorded the sounds of his brutal acts. Sex offenders have video taped their crimes using mobile devices. Terrorists have been tracked down using traces of data recovered from cell phones attached to improvised explosive devices. Mobile devices have helped rescue kidnap victims before they came to harm. Many vice officers and courts consider mobile devices as an integral part of drug trafficking and dealing.

Using the proper methodology and tools, you can extract useful evidence from mobile devices and obtain records from network service providers to help avert an attack, further an investigation, or solve a crime.
-Eoghan Casey

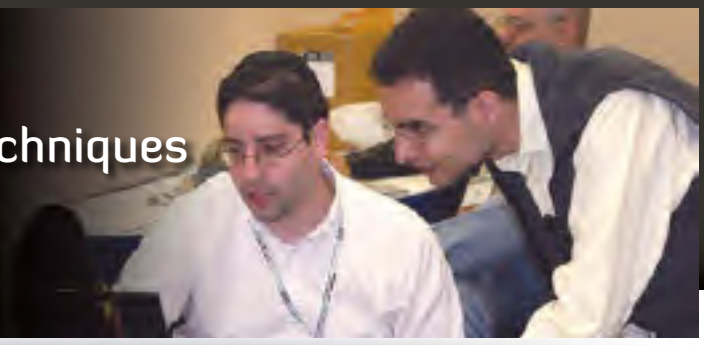
Digital Forensics and Incident Response
http://computer-forensics.sans.org

Delivery Methods

Live Events
OnSite

Forensics 610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques



Five-Day Program • 9:00am - 5:00pm
30 CPE/CMU Credits • Laptop Required

Expand your capacity to fight malicious code by learning how to analyze bots, worms, and trojans.

This popular malware analysis course has helped forensic investigators, malware specialists, incident responders, and IT administrators assess malware threats. The course teaches a practical approach to examining malicious programs-spyware, bots, trojans, etc.-that target or run on Microsoft Windows. This training also looks at reversing Web-based malware, such as JavaScript and Flash files, as well as malicious document files. By the end of the course, you'll learn how to reverse-engineer malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools for turning malware inside-out!

Who Should Attend:

- Incident response team members
- Experienced digital forensic analysts
- Law enforcement officers, federal agents, or detectives
- Media exploitation analysts
- Red team members, penetration testers, and exploit developers
- Application and software developers
- Information security professionals

Learn Malware Analysis to Improve Incident Response and Forensics Skills

This unique course provides a rounded approach to reverse-engineering by covering both behavioral and code phases of the analysis process. As a result, the course makes malware analysis accessible even to individuals with a limited exposure to programming concepts. The materials do not assume that the students are familiar with malware analysis; however, the complexity of concepts and techniques increases as the course progresses.

The malware analysis process taught in this class helps incident responders assess the severity and repercussions of a situation that involves malicious software. It also assists in determining how to contain the incident and plan recovery steps. Forensics investigators also learn how to understand key characteristics of malware present on compromised systems, including how to establish indicators of compromise (IOCs) for scoping and containing the intrusion.

A Methodical Approach to Reverse-Engineering

The course begins by covering fundamental aspects of malware analysis. You'll learn how to set up an inexpensive and flexible laboratory for understanding the inner-workings of malicious software and will understand how to use the lab for exploring characteristics of real-world malware. Then you'll learn to examine the program's behavioral patterns and code. Afterwards, you'll experiment with reverse-engineering compiled Windows executables and browser-based malware.

The course continues by discussing essential x86 assembly language concepts. You'll examine malicious code to understand the program's key components and execution flow. Additionally, you'll learn to identify common malware characteristics by looking at Windows API patterns and will examine excerpts from bots, rootkits, keyloggers, and downloaders. You'll understand how to work with PE headers and handle DLL interactions. Furthermore, you'll learn tools and techniques for bypassing anti-analysis capabilities of armored malware, experimenting with packed executables and obfuscated browser scripts.

Towards the end of the course, you'll learn to analyze malicious document files that take the form of Microsoft Office and Adobe PDF documents. Such documents act as a common infection vector and need to be understood by enterprises concerned about both large-scale and targeted attacks. The course also explores memory forensics approaches to examining rootkits. Memory-based analysis techniques also help understand the context of an incident involving malicious software.

Hands-On Training for Malware Analysis and Reversing

Hands-on workshop exercises are a critical aspect of this course and allow you to apply reverse-engineering techniques by examining malware in a controlled environment. When performing the exercises, you'll study the supplied specimen's behavioral patterns and examine key portions of its code. You'll examine malware on a Windows virtual machine that you'll infect during the course and will use the supplied Linux virtual machine (REMnux) that includes tools for examining and interacting with malware.

Digital Forensics and Incident Response
http://computer-forensics.sans.org

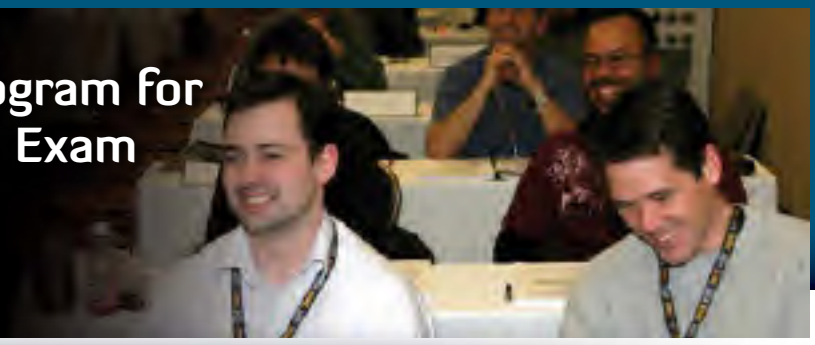
GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Delivery Methods
Live Events
OnDemand
OnSite
vLive!
SelfStudy

Management 414

SANS® +S™ Training Program for the CISSP® Certification Exam



Six-Day Program • 9:00am - 5:00pm
36 CPE/CMU Credits • Laptop NOT Required

The SANS® +S™ Training Program for the CISSP® Certification Exam will cover the security concepts needed to pass the CISSP® exam. This is an accelerated review course that assumes the student has a basic understanding of networks and operating systems and focuses solely on the 10 domains of knowledge of the CISSP:

Domain 1 **Access Control**
Domain 2 **Telecommunications and Network Security**
Domain 3 **Information Security Governance and Risk Management**
Domain 4 **Software Development Security**
Domain 5 **Cryptography**
Domain 6 **Security Architecture and Design**
Domain 7 **Security Operations**
Domain 8 **Business Continuity and Disaster Recover Planning**
Domain 9 **Legal, Regulations, Investigations, and Compliance**
Domain 10 **Physical (Environmental) Security**

Each domain of knowledge is dissected into its critical components. Every component is discussed in terms of its relationship to other components and other areas of network security. After completion of the course, the student will have a good working knowledge of the 10 domains of knowledge and, with proper preparation, be ready to take and pass the CISSP® exam.

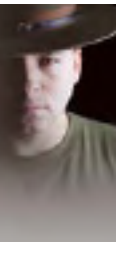
Who Should Attend:

- Security professionals who are interested in understanding the concepts covered in the CISSP® exam as determined by $(ISC)^2$
- Managers who want to understand the critical areas of network security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® 10 Domains
- Security professionals and managers looking for practical ways the 10 domains of knowledge can be applied to the current job
- In short, if you desire a CISSP® or your job requires it, MGT414 is the training for you to get GISP certified. Reinforce what you learned in training and prove your skills and knowledge with a GISP certification.

Obtaining your CISSP® certification consists of:

- Fulfilling minimum requirements for professional work experience
- Completing the Candidate Agreement
- Review of Resume
- 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
- Period Audit of CPEs to maintain the credential

Bootcamp



This program has extended hours.

Evening Bootcamp Sessions:
5:00pm - 7:00pm (Days 1-5)

Morning Bootcamp Sessions:
8:00am - 9:00am (Days 2-6)

You Will Receive With This Course:

Free "CISSP® Study Guide" by Eric Conrad, Seth Misenar, and Joshua Feldman.

"Ideal preparation tool for the CISSP® exam..." -Stephen Northcutt

What Students Are Saying

"This course was invaluable as a preparation tools for the CISSP exam."
-Matthew Slayton, Liberty Mutual Insurance

From the Author

The CISSP® certification has been around for almost ten years and covers security from a 30,000 foot view. CISSP® covers a lot of theoretical information that is critical for a security professional to understand. However, this material can be dry and since most students do not see the direct applicability to their jobs, they find it boring. The goal of this course is to bring the CISSP® 10 domains of knowledge to life. By explaining important topics with stories, examples, and case studies, the practical workings of this information can be discovered. I challenge you to attend the SANS CISSP® training course and find the exciting aspect of the ten domains of knowledge. -Dr. Eric Cole

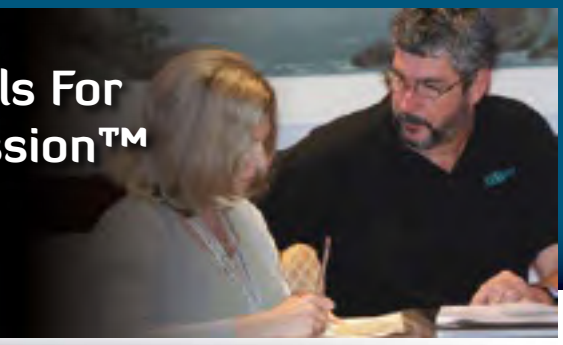
GIAC Certification
www.giac.org

DoD 8570 Required
www.sans.org/8570

Delivery Methods
Live Events
Mentor
OnDemand
OnSite
vLive!
SelfStudy

Management 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™



Five-Day Program
9:00am - 6:00pm (Days 1-4) • 9:00am - 4:00pm (Day 5)
33 CPE/CMU Credits • Laptop NOT Required

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 US 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 defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, Web application security, 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.

Who Should Attend:

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

Knowledge Compression™

uses specialized material, in-class reviews, examinations, and test-taking training to ensure that students have a solid understanding of the material that has been presented to them.

There are three goals for this course and certification:

- Establish a minimum standard for IT security knowledge, skills, and abilities. In a nutshell, this course covers all of the non-operating system topics that are in SANS Security Essentials, though not to the same depth. The goal is 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 that 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.

From the Author

When SANS designed the Security Leadership for Managers course, we chose to emulate the format utilized by many executive MBA programs. While core source material is derived from our highly regarded SANS Security Essentials program, we decided to focus this program on the big picture of securing the enterprise: network fundamentals, security technologies, using cryptography, defense-in-depth, policy development, and management practicum. This course includes executive briefings designed to present a distilled summary of vitally important information security topics like operating system security and security threat forecasts. Ultimately, the goal of this program is to ensure that managers charged with the responsibility for information security can make informed choices and decisions that will improve their organization's security. -Stephen Northcutt

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

DoD 8570 Required
www.sans.org/8570

Delivery Methods

Live Events
Mentor
OnDemand
OnSite
vLive!
SelfStudy

Management 514

IT Security Strategic Planning, Policy, and Leadership

Five-Day Program • 9:00am - 5:00pm
30 CPE/CMU Credits • Laptop Recommended

You know the expression, "What got you here, won't keep you here"? I have met many people who were successful in terms of being technical, but they have struggled in management, especially in senior management positions. This course is designed to help with the transition from technical person to manager to leader and give you the tools to be successful as a senior IT strategic planner, policy author, and leader.

Mastering the Strategic Planning Process

Strategic planning is hard for people in IT and IT Security because we spend so much time responding and reacting. Some of us have been exposed to a SWOT or something similar in an MBA course, but 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.

In this course you will learn the entire strategic planning process: what it is and how to do it; what lends itself to virtual teams, and what needs to be done face to face. We will practice building those skills in class. Topics covered in depth include how to plan the plan, horizon analysis, visioning, environmental scans (SWOT, PEST, Porter's etc.), historical analysis, mission, vision, and value statements. We will also discuss the planning process core, candidate initiatives, the prioritization process, resource and IT change management in planning, how to build the roadmap, setting up assessments, and revising the plan.

Who Should Attend:

This course is designed and taught for existing, recently appointed, and aspiring IT and IT Security managers and supervisors who desire to enhance their leadership and governance skills to develop their staff into a more productive and cohesive team.

Creating Effective Information Security Policy

Policy is a manager's opportunity to express expectations for the workforce, to 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 organization's culture. We will break down the steps to policy development so that you have the ability to develop and assess policy successfully.

Developing Management and Leadership Skills

The third focus of the course is on management and leadership competencies. Leadership is a capability that must be learned, exercised and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. However, leaders and followers influence each other toward the goal; it is a two-way street where all parties perform their functions to reach a common objective.

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 organization's mission. Grooming effective leaders is critical to all types of organizations, as the most effective teams are cohesive units that work together toward common goals with camaraderie and a can-do spirit!

Leadership tends to be a bit "squishy" and courses covering the topic are often based upon the opinions of people who were successful in the marketplace. However, success can be as much a factor of luck as skill, so we base this part of the course on five decades of the research of social scientists and their experiments going as far back as Maslow and on research as current as Sunstein and Thaler. We discuss leadership skills that apply to commercial business, non-profit, not-for-profit, or other organizations. This course is designed to develop existing and new supervisors and managers who aspire to go beyond being the boss. It will help you build leadership skills to enhance the organization's climate and team-building skills to support the organization's mission, its growth in productivity, workplace attitude/satisfaction, and staff and customer relationships.

Delivery Methods
Live Events
OnSite

Management 525

IT Project Management, Effective Communication, and PMP Exam Prep

Six-Day Program • 9:00am - 5:00pm
36 CPE/CMU Credits • Laptop NOT Required

Do you have the knowledge and tools you need to become a top-notch project manager and improve the success rate of your organization's IT projects? Do you need to improve your technical communication skills, risk analysis, and continuous monitoring processes?

The SANS MGT525 IT Project Management and Effective Communication course is a PMI Registered Education Provider (REP). REPs provide the training necessary to earn and maintain the Project Management Professional (PMP)® and other professional credentials. This course has been recently updated to fully align with the 2011 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 resources. We will utilize project case studies that highlight information technology services as deliverables. MGT525 follows the basic project management structure from the PMBOK® Guide 4th edition and also provides specific techniques for success with information assurance initiatives.

Throughout the week, we will cover all aspects of project management- from initiating and planning projects through managing cost, time, and quality while your project is active, to completing, closing, and documenting as your project finishes.

A copy of the *PMBOK® Guide* (Fourth 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 2011 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 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 risk 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.

Following the SANS promise, participants leave this course with specific tools that can be applied the day you get back to the office!

PMBOK® and PMP® are registered trademarks of the Project Management Institute.

Who Should Attend:

- Security professionals interested in understanding the concepts of 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 utilize 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.
- Individuals preparing for the Project Management Professional (PMP®) Exam

From the Author

Managing projects to completion, with an alert eye on quality, cost, and time, is something most of us need to do on an ongoing basis. In this course, we break down project management into its fundamental components and galvanize your understanding of the key concepts with an emphasis on practical application and execution of service based IT and InfoSec projects. Since project managers spend the vast majority of their time communicating with others, throughout the week we focus on traits and techniques that enable effective technical communication. As people are the most critical asset in the project management process, effective and thorough communication is essential. -Jeff Frisk

GIAC Certification
www.giac.org

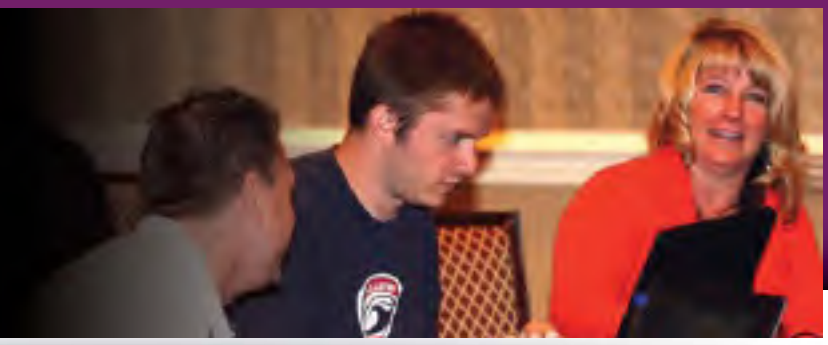
STI Graduate School
www.sans.edu

Delivery Methods

Live Events
OnDemand
OnSite

Legal 523

Law of Data Security and Investigations



Five-Day Program • 9:00am - 5:00pm
30 CPE/CMU Credits • Laptop NOT Required

New laws regarding 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. The professional training needed to accomplish this is uniquely available in SANS' LEG523 series of courses, which is designed to build skills in the analysis and use of contracts, policies, and records management procedures.

Earning the GLEG certification for LEG523 demonstrates to employers that a professional has not only attended classes, but studied and absorbed the sophisticated content of these courses. Certification distinguishes any professional, whether an IT expert, an auditor, a paralegal, or a lawyer, and the value of certification will grow in the years to come as law and security issues become even more interlocked.

Legal 523 covers the law of business, contracts, fraud, crime, IT security, IT liability and IT policy - all with a focus on electronically stored and transmitted records. The course also teaches investigators how to prepare credible, defensible reports, whether for cyber, forensics, incident response, human resources or other investigations. LEG523 is a five-day package delivering the content of the following one-day courses:

- **Fundamentals of IT Security Law and Policy**
- **E-records, E-discovery, and Business Law**
- **Contracting for Data Security and Other Technology**
- **The Law of IT Compliance: How to Conduct Investigations**
  - *Lessons will be invaluable to the proper execution of any kind of internal investigation.*
- **Applying Law to Emerging Dangers: Cyber Defense**
  - *In-depth review of legal response to the major security breach at TJX.*
  - *Learn how to incorporate effective public communications into your cyber security program.*

Recent updates to the courses address hot topics such as risk, investigations and business records retention connected with cloud computing, and social networks like Facebook and Twitter. Updates also teach students how to analyze and respond to the risks and opportunities surrounding OSINT (open source intelligence gathering).

Who Should Attend:

- Investigators
- Security and IT professionals
- Lawyers
- Paralegals
- Auditors
- Accountants
- Technology Managers
- Vendors
- Compliance officers
- Law enforcement
- Privacy Officers

What Students Are Saying

"Ben's insight into legal issues and teaching style makes this potentially dry material exciting. His stories and examples add to the printed material"

-Karl Kurrle, Golf Savings Bank

From the Author

These are five intense days covering the rapid development of law at the intersection of IT and security. Be prepared for insights and tips you've not heard before.

-Benjamin Wright

GIAC Certification
www.giac.org

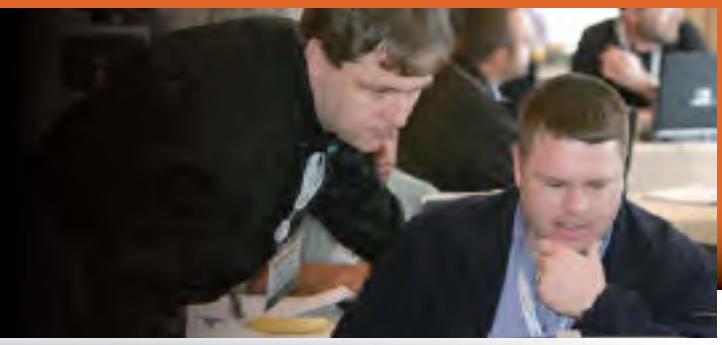
STI Graduate School
www.sans.edu

Delivery Methods

Live Events
OnDemand
OnSite
SelfStudy

Developer 522

Defending Web Applications Security Essentials



Six-Day Program • 9:00am - 5:00pm
36 CPE/CMU Credits • Laptop Required

This is the course to take if you have to defend web applications!

Traditional network defenses, such as firewalls, fail to secure web applications. The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure it. DEV522 covers the OWASP Top 10 and will help you to better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

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

This class goes beyond classic web applications and includes coverage of Web 2.0 technologies, like AJAX and web services. We also arm you with knowledge to defend yourself against cutting-edge attackers, such as various protective HTTP headers and new generation of browser-based web application protections.

To maximize 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.

The course will cover the topics outlined by OWASP's Top 10 risks document as well as additional issues the authors found of importance in their day-to-day web application development practice. 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. It will conclude with a large defensive exercise, reinforcing the lessons learned throughout the week.

Who Should Attend:

- Application developers
- Application security analysts or managers
- Application architects
- Penetration testers who are interested in learning about defensive strategies
- Security professionals who are interested in learning about web application security
- Auditors who need to understand defensive mechanisms in web applications
- Employees of PCI compliant organizations who need to be trained to comply with PCI requirements

From the Author

Too many websites are getting compromised these days. Our goal for this course is to arm the students with defensive strategies that can work for all web applications. We all know it is very difficult to defend a web application; there are so many different types of vulnerabilities and attack channels. Overlook one thing and your web app is owned. The defensive perimeter needs to extend far beyond just the coding aspects of web application. In this course, we cover the security vulnerabilities so students have a good understanding of the problems at hand. We then provide the defensive strategies and tricks as well as overall architecture that are proven to help secure sites. I have also included some case studies throughout the course so we can learn from the mistakes of others and make our own defense stronger. The exercises in class were designed to help you further the understanding and help retain the knowledge by hands-on practice. By the end of the course, you will have the practical skills and understanding of the defensive strategies to lock down existing applications,as well as building more secure applications in the future. -Dr. Johannes Ullrich

GIAC Certification
www.giac.org

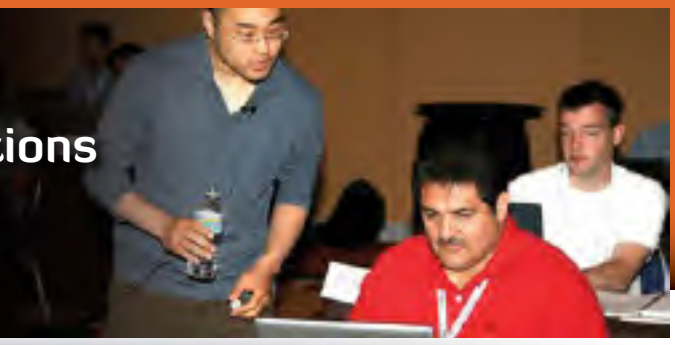
STI Graduate School
www.sans.edu

Delivery Methods

Live Events
OnDemand
OnSite
vLive!
SelfStudy

Developer 541

Secure Coding in Java/JEE: Developing Defensible Applications



Four-Day Program • 9:00am - 5:00pm
24 CPE/CMU Credits • Laptop Required

The Difference between Good and Great Programmers

Great programmers have traditionally distinguished themselves by the elegance, effectiveness, and reliability of their code. That's still true, but elegance, effectiveness, and reliability have now been joined by security. Major financial institutions and government agencies have informed their internal development teams and outsourcers that programmers must demonstrate mastery of secure coding skills and knowledge through reliable third-party testing or lose their right to work on assignments for those organizations. More software buyers are joining the movement every week.

Such buyer and management demands create an immediate response from programmers, "Where can I learn what is meant by secure coding?" This unique SANS course allows you to bone up on the skills and knowledge required to prevent your applications from getting hacked.

Who Should Attend:

- Developers who want to build more secure applications
- Java EE programmers
- Software engineers
- Software architects

This class is focused specifically on software development but is accessible enough for anyone who's comfortable working with code and has an interest in understanding the developer's perspective including:

- 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

What Does the Course Cover?

This is a comprehensive course covering a huge set of skills and knowledge. It's not a high-level theory course. It's about real programming. In this course you will examine actual code, work with real tools, build applications, and gain confidence in the resources you need for the journey to improving the security of Java applications.

Rather than teaching students to use a set of tools, we're teaching 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 Top 10 and CWE/SANS Top 25 Most Dangerous Programming Errors.

The class culminates in a Secure Development Challenge where you 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 finally, using the secure coding techniques that you have learned in class, implement fixes for these issues.

What Students Are Saying

"Intense training! An excellent combination of technical and theory instruction."

-Richard Brull

From the Author

After having taught application security to hundreds of developers, I've learned what works in teaching this important subject. Developers need to be intellectually challenged with exercises; they need a variety of solutions they can apply to a single problem in different scenarios. By giving our students concrete examples of applications they can take back with them, class attendees will be armed with strong techniques that can be applied to both current and future projects. By knowing how various Web application attacks work, how common programming errors are made, and how to prevent them, developers will have the tools necessary to prevent a large number of application attacks. Take part in this groundbreaking class and arm yourself with the knowledge to protect your Java applications. -Frank Kim

GIAC Certification
www.giac.org

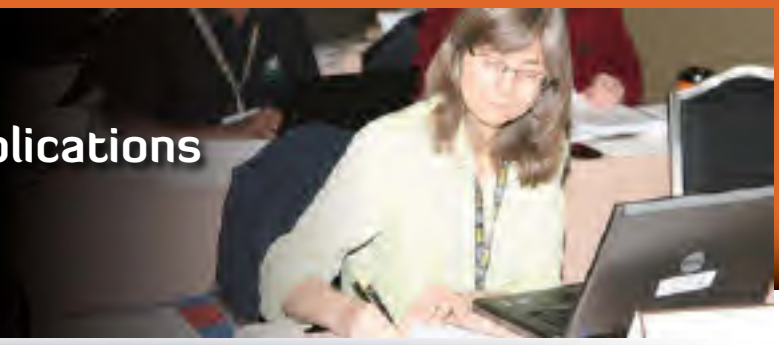
STI Graduate School
www.sans.edu

Delivery Methods

Live Events
OnDemand
OnSite
vLive!
SelfStudy

Developer 544

Secure Coding in .NET: Developing Defensible Applications



Four-Day Program • 9:00am - 5:00pm
24 CPE/CMU Credits • Laptop Required

ASP.NET and the .NET framework have provided web developers with tools that allow them an unprecedented degree of flexibility and productivity. On the other hand, 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 onus is still on application developers to understand the limitations of the framework and ensure that their own code is secure.

During this four-day course we will analyze the defensive strategies and technical underpinnings of the ASP.NET framework and learn where, as a developer, you can leverage defensive technologies in the framework, where you need to build security in by hand. We'll also examine strategies for building applications that will be secure both today and in the future.

Rather than focusing on traditional web attacks from the attacker's perspective, this class will show developers first how to think like an attacker, and will then focus on the latest defensive techniques specific to the ASP.NET environment. The emphasis of the class is a hands-on examination of the practical aspects of securing .NET applications during development.

Who Should Attend:

This class is focused specifically on software development but is accessible enough for anyone who's comfortable working with code and has an interest in understanding the developer's perspective:

- **Software developers and architects**
- **Senior software QA specialists**
- **System and security administrators**
- **Penetration testers**

Have you ever wondered if ASP.NET Request Validation is effective? Have you been concerned that XML web services might be introducing unexamined security issues into your application? Should you feel un-easy relying solely only on the security controls built into the ASP.NET framework? Secure Coding in ASP.NET will answer these questions and far more.

What Students Are Saying

"It was an eye-opener to many little (and big) things we were missing."

-Abby Jakoplic, Children's Mercy Hospital

From the Author

Microsoft has provided a great development platform with .NET. There is a rich set of features, not only for building solid applications, but also for securing those applications. Even with a robust platform and decent security features, unfortunately, there is still a disconnect between building solid applications and building secure applications.

Developers are always up against rigid deadlines, sparse and changing requirements and constant production support issues, which leaves little time for keeping up with the current threats and defenses and inevitably makes security an afterthought. Bolting security on at the end of the development phase leaves applications vulnerable and requires significantly more effort than if the applications were architected with security in mind at the beginning. CWE defines approximately 658 software weaknesses that can be introduced at different points in the software development lifecycle, and an attacker only needs to expose one of these while developers feel pressure to defend against them all. The goal of this course is not to teach developers how to write 100% secure code, but instead to help developers nurture a mindset for creating defensible code from the early stages of the SDL that will allow applications to withstand an attack and provide feedback when under attack, so organizations can adjust and adapt to the changing threat landscape.

This course covers common attacks, including applicable topics from the CWE/SANS Top 25 Most Dangerous Programming Errors, the OWASP Top 10 and deficiencies in the .NET framework, while also providing solid defensive techniques. This course will change the way developers approach the design and implementation of software. -Jason Montgomery

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Delivery Methods

Live Events
OnDemand
OnSite

Audit 407

Foundations of Auditing Information Systems

Six-Day Program • 9:00am - 5:00pm
36 CPE/CMU Credits • Laptop Required

This course is designed for security and assurance professionals, system administrators, and business and operational auditors who want to develop the technical and operational knowledge of information system auditing. This course is a careful balance of the audit process, governance, and compliance regulations, as well a hands-on introduction to the latest technology tools. The auditing skills taught in AUD 407: Foundations of Auditing Information Systems are in great demand, as companies and agencies are required to comply with a growing number of regulations.

Students will learn the role of an auditor, the types of audits performed, and various information security and audit frameworks, as well as the tools and techniques of auditing technical controls, foundations of auditing operating systems, and foundations of auditing applications. Even seasoned professionals will learn the value of performing information system audits as well as the business value of information system auditing.

This information systems audit course focuses on the following areas and more:

- **Audit frameworks**
- **The information systems audit process**
- **Project management for auditors**
- **Data collection methodologies**
- **Regulations and compliance**
- **Auditing, vulnerability testing & penetration testing**
- **Auditing technical controls**
- **Auditing networks & operating systems**
- **Auditing business application systems**

Who Should Attend:

This class is designed for individuals who are tasked with auditing IT systems for implementation of organizational policies and procedures, risk, and policy conformance.

- **System implementers/ administrators**
- **Network security engineers**
- **Internal auditors**
- **Assurance personnel**
- **Business and operational auditors**
- **DoD personnel/contractors**

From the Author

We believe auditors are the unsung heroes of organizations. Well planned information technology audits save companies time and money. Audits identify security risks and ways to reduce those risks. Being a good auditor is more than following a checklist. Great auditors have proficient technology skills. They are project managers, technical writers, persuaders, presenters, and subject matter experts. In this class, we provide students a solid foundation for understand the audit process. Let us teach you how to identify and evaluate security safeguards, and create a toolbox of automated technical auditing tools. Organizations are holding out for more audit heroes. Take the challenge! - James Tarala

Looking for a great IT audit resource?

SANS IT Audit website is a community-focused site offering IT audit professionals a one-stop resource to learn, discuss, and share current developments in the field. It also provides information regarding SANS audit training, GIAC certification, and upcoming events. New content is added regularly, so please visit often. And don't forget to share this information with your fellow IT audit professionals.
http://it-audit.sans.org

Delivery Methods

Live Events
OnDemand
OnSite
vLive!
SelfStudy

Audit 507

Auditing Networks, Perimeters, and Systems

Six-Day Program • 9:00am - 5:00pm
36 CPE/CMU Credits • Laptop Required

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. This course provides 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, you 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 any organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation will be given from real-world examples.

While the primary audience for this course is auditors, system and security administrators will find very powerful techniques and processes for building continuous monitoring of systems and networks. Throughout the course, time is spent exploring how to determine what the correct "settings" are for an organization, how to abstract those settings into an automated process and how to ensure that the processes in the organization select and manage those settings correctly.

Every day of this course includes hands-on exercises. A variety of tools will be discussed and demonstrated during the lecture sections. These examples are then put into practice during labs so that you will leave knowing how to verify each and every control described in the class and know what to expect as audit evidence. Five of the hands-on days will give 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 virtualized environment. Each student is invited to bring a Windows XP Professional or higher laptop for use during class. Macintosh computers running OS X may also be used with VMWare Fusion.

Sign up for this course and experience the mix of theory, hands-on, and practical knowledge.

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 they 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

What Students Are Saying

"This is the best group of instructors I've ever been exposed to."

-Mark Jeanmougin, 53.com

From the Author

This advanced systems audit course stands alone in the information assurance arena as the only comprehensive source for hands on audit how-to. Past students have included long-time auditors and those new to the field, both of whom have found significant benefit from the refresher material. One individual, a vice president with the Institute of Internal Auditors, said, I've been auditing systems for a very long time, and no one ever actually gave me a formal process that I can apply to conducting technical audits. Thank you! While we don't require a high level of technical experience as a prerequisite to this course, we have worked hard to make sure that anyone who comes to the course walks away with a wealth of material that they can go back to their office and apply tomorrow. We realistically address the problem, How do I get there from here? by offering short-term goal solutions, which, when combined, will allow you to achieve your goal: identify, report on, and reduce risk in your enterprise. - David Hoelzer

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

DoD 8570 Required
www.sans.org/8570

Delivery Methods

Live Events
OnDemand
OnSite
vLive!
SelfStudy

Additional SANS Training Courses

SECURITY: 5- and 6-Day Courses

SEC506 Securing Linux/Unix
Experience in-depth coverage of Linux and Unix security issues. 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. This course provides specific configuration guidance and practical, real-world examples, tips, and tricks.

SEC540 VoIP Security
VoIP has become a widely adopted technology, and it's here to stay. VoIP protocols and technologies, and especially VoIP security, are among the most complex fields in IT today. This course offers the in-depth knowledge required to understand how VoIP technologies work at the protocol level (mainly focusing on SIP and RTP).

SEC579 Virtualization and Private Cloud Security
The course starts out with architecture and security design for both virtualization and private cloud infrastructure. Then will help you adapt your existing security policies and practices to the new virtualized or cloud-based infrastructure.

SEC642 Advanced Web App Penetration Testing and Ethical Hacking *(Available May 2012)*
This course is designed to teach you the advanced skills and techniques required to test web applications today. This advanced pen testing course uses a combination of lecture, real-world experiences, and hands-on exercises to educate the you in the techniques used to test the security of enterprise applications.

SEC660 Advanced Penetration Testing, Exploits and Ethical Hacking
This course is designed as a logical progression point for those who have completed SEC560, 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.

SECURITY: 2- and 4-Day Courses

SEC464 Hacker Detection for Systems Administrators with Continuing Education Program
This educational program gives systems administrators tools and techniques to illuminate evidence of potentially malicious activity on their systems and to look deeper to determine whether the problems they see are real. It allows them to become the human sensors for malicious activity in their organization. It uses hands-on exercises to ensure they are comfortable using the tools.

SEC524 Cloud Security Fundamentals
The course covers a detailed introduction to the various delivery models of cloud computing ranging from Software as a Service (SaaS) to Infrastructure as a Service (IaaS) and everything in between.

SEC546 IPv6 Essentials
IPv6 is currently being implemented at a rapid pace in Asia in response to the exhaustion of IPv4 address space, which is most urgently felt in rapidly growing networks in China and India. This course will introduce network administrators and security professionals to the basic concepts of IPv6.

SEC569 Combating Malware in the Enterprise
This succinct course will teach you how to plan, resist, detect, and respond to malware infections throughout the enterprise. The course focuses on malware threats targeting Microsoft Windows systems in an enterprise environment.

SEC571 Mobile Device Security
This course is designed to teach students about the threats organizations are exposed to via the mobile devices on which they depend.

SEC577 Virtualization Security Fundamentals
Attendees will learn about virtualization security fundamentals with an in-depth treatment of today's most pressing virtualization security concerns: known attacks and threats, theoretical attack methods, and numerous real-world examples.

SEC580 Metasploit Kung Fu for Enterprise Pen Testing
This class will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen, according to a thorough methodology for performing effective tests.

SEC710 Advanced Exploit Development
Attendees can apply the skills developed in this class to create and customize exploits for penetration tests of homegrown software applications and newly discovered flaws in widespread commercial software.

SECURITY: 1-Day Courses

SEC351 Computer and Network Security Awareness
This course is offered for the individual just beginning to explore computer security. You will learn about many different threats, antivirus programs, firewalls, anti-spyware, identity theft, Phishing, how to create strong passwords, and more.

SEC352 Protecting Your Personal Privacy on the Internet
Whatever the scenario, there are many legitimate reasons to hide your identity on the Internet. And there are certainly many unjustified reasons to run silent and deep on the Internet. This course outlines the most common ways people try to maintain their anonymity when using the Internet.

SEC517 Cutting-Edge Hacking Techniques
This fast-paced, intermediate-to-advanced course is ideal for students who have taken a multi-day hacking course in the past and are looking to update their understanding and skills.

FORENSICS: 1-Day Course

FOR526 Advanced Filesystem Recovery and Memory Forensics
This advanced course is perfect for the diligent student familiar with core forensic methodology and techniques. If you understand forensic filesystem fundamentals, then this course is for you. It moves quickly from covering memory forensics to recovering and discovering deleted partitions from hard drives. This course focuses on innovative forensic techniques and methodologies so the seasoned practitioner can keep his skills sharp and up-to-date with the latest research areas in both live and static based disk forensics.

MANAGEMENT: 6-Day Course

MGT411 SANS 27000 Implementation & Management
This course is designed for information security officers or other management professionals who are looking for a how-to guide for implementing ISO-27000 effectively and quickly.

MANAGEMENT: 2-Day Courses

MGT405 Critical Infrastructure Protection
This class is designed to give the student a full examination of the scope of critical infrastructure vulnerabilities, the dependence of critical infrastructures on the Internet, and Internet security problems.

MGT433 Securing the Human: Building and Deploying an Effective Security Awareness Program
Organizations have invested in information security for years now. Unfortunately, almost all of this effort has been focused on technology with little, if any, effort on the human factor. As a result, the human is now the weakest link. In this challenging course you will learn the key concepts and skills to plan, implement, and maintain an effective security awareness program that makes your organization both more secure and compliant.

MGT442 Information Security Risk Management
This course will explore each phase of the risk management lifecycle, focusing on implementing assessment and analysis techniques that should be used to properly assess and mitigate information risk.

MGT519 Information Security Policy In-Depth
In two days, you will be exposed to over 100 different policies in a course that balances lecture, labs, and in-class discussion. We will emphasize techniques to create successful policy that users will read, follow, and that will be accepted by the business units because it is sensitive to the organizational culture and uses the psychology of information security to guide implementation.

MGT520 IT Security Strategic Planning
Business needs change, the environment changes, new risks are always on the horizon, and critical systems are continually exposed to new vulnerabilities. Strategic planning is a never-ending process. This is a hands-on, exercise-intensive course on writing, implementing and assessing strategic plans.

MANAGEMENT: 1-Day Courses

MGT305 Technical Communication and Presentation Skills for Security Professionals
In this course we cover the top techniques that will show any attendee how to research and write professional quality reports, how to create outstanding presentation materials, and as an added bonus, how to write expert witness reports. Attendees will also get a crash course on advanced public speaking skills.

MGT404 Fundamentals of Information Security Policy
This course focuses on how to write, analyze and assess a wide range of security policies including issue and system specific policy. The student will develop skills and practical experience by completing the 24 guided labs that cover both the policy header and policy body or statement and learn to create successful policy that is accepted by the organization by being sensitive to the corporate culture.

MGT421 SANS Leadership and Management Competencies
This course is designed to help you build leadership skills to enhance the organization's climate and team-building skills to support the organization's mission, its growth in productivity, workplace attitude/satisfaction, and staff and customer relationships.

MGT432 Information Security for Business Executives
Where do you go if you are a CEO or vice president looking to learn the fundamentals of information security? The SANS Institute, well known as a premier source for top quality technical instruction, information security thought leadership, and research, now offers this purpose-built course for senior leaders. The structure of the course is to present the information and provide the executive participant with additional reading.

MGT438 Establishing a Security Awareness Program
Being able to design, implement, and manage an effective security awareness program is difficult at best. MGT438 walks trainers and security managers through the architecture and design of a successful security awareness program. It helps the student to document and design a clear cut strategy, approach, and implementation plan.

MGT535 Incident Response Management
Students will learn by applying course content through hands-on skill-building exercises. These exercises range from: writing and evaluating incident response procedures, to the table-top validation of procedures, incident response management role playing in hypothetical scenarios, and hands-on experience in tracking incident status in hypothetical scenarios.

DEVELOPER: 2-Day Courses

DEV536 Secure Coding for PCI Compliance
Throughout the course we will look at examples of the types of flaws that secure coding protects against, examine how the flaw might be exploited and then focus on how to correct that code.

DEV543 Secure Coding in C & C++
This course will cover all of the most common programming flaws that affect C and C++ code.

DEVELOPER: 1-Day Courses

DEV551 Secure Mobile Applications Development: iOS App Security
This course is designed to educate developers on secure programming guidelines and tips for the iOS platform. Developers will learn how to leverage data protection APIs provided by the iOS platform to protect their and their user's data, and transfer them securely over wireless channels.

DEV568 Secure Mobile Applications Development: Android App Security
This is a one-day crash course to help you get your Android application to market securely by avoiding common security pitfalls seen in smartphone and tablet-based mobile applications.

AUDIT: 2-Day Course

AUD521 Meeting the Minimum: PCI/DSS 2.0: Becoming and Staying Compliant
This course was created to allow organizations to exercise due care by performing internal validations through a repeatable, objective process.

For complete course descriptions, please visit www.sans.org/security-training/courses.php.

Find out more about SANS Cyber Ranges at www.sans.org

SANS Cyber Ranges provide a safe, controlled environment for up-and-coming security professionals or seasoned experts to test their information security aptitude, skills and expertise. Individuals and organizations will benefit from the games in the **SANS Cyber Ranges** due to the hands-on components built into each series of security scenarios.

SANS Cyber Ranges have two classifications, each with their own set of challenges.

- **Cyber Quests**
- **NetWars**

SHALL WE PLAY A GAME?

- Designed for measuring skill
- Consists of on-line asset and a quiz
  - Each Cyber Quest has a different asset that defines the nature of that specific scenario
  - Assets include: vulnerable website, forensics disk image, neutered malware specimen
  - Analyze the asset and answer quiz questions
  - Quiz is designed to take 1 to 2 hours

CYBER QUESTS

"We were very impressed with SANS NetWars. The material is relevant and educational, and the tournament style play is remarkably engaging. I really like the scoring system and scoreboard."

-Adam Tice, Lockheed Center for Cyber Security

- Designed for measuring experience
- Consists of an interactive, Internet-based environment for computer attacks and analyzing defenses
- Offered in two forms:
  - Tournament play: 3 intense days, useful to evaluate performance
  - Continuous play: Played at will over months, useful as a learning tool
- And includes a report card showing areas for additional skill development

NETWARS

Department of Defense

Come to SANS and take the IT security training with the HIGHEST pass rate on 8570 required certifications including GSLC, GSEC, GCIA, GCFA, GCIH, GCED, GSNA, and CISSP!

www.sans.org/8570

DoD Baseline IA Certifications

TECH II

GSEC†
SEC401: SANS Security Essentials Bootcamp Style

Security+†

TECH III

GCED†
SEC501: Advanced Security Essentials - Enterprise Defender

GCIH†
SEC504: Hacker Techniques, Exploits and Incident Handling

CISSP*†
MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam

MGT I

GSLC†
MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™

GSIF†
SEC301: Intro to Information Security

MGT II

GSLC†
MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™

CISSP*†
MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam

MGT III

GSLC†
MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™

CISSP*†
MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam

Computer Environment (CE) Certifications

GCWN†
SEC505: Securing Windows

GCUX†
SEC506: Securing Linux/Unix

By the end of 2011, all personnel performing CND-SP and IASAE roles must be certified. These courses will prepare you for the required certifications:

Information Assurance System Architecture & Engineering (IASAE) Certifications

CND ANALYST

GCIA†
SEC503: Intrusion Detection In-Depth

CND INCIDENT RESPONDER

GCIH†
SEC504: Hacker Techniques, Exploits, and Incident Handling

CND AUDITOR

GSNA†
AUD507: Auditing Networks, Perimeters, and Systems

Computer Network Defense (CND) Certifications

IASAE I

CISSP*†
MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam

IASAE II

CISSP*†
MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam

*Or Associate †SANS training available

Voucher Program

www.sans.org/vouchers

The SANS Discount Program That Pays You Credits and Delivers Flexibility

Please contact us at
vouchers@sans.org
301-654-7267

Maximize Your Training Budget! Extend Your Fiscal Year

SANS Voucher Program - Overview

The SANS Voucher Program offers significant savings on our hands-on and job-based training as well as GIAC certification. Two Voucher options let you choose the method, time and place to train.

- **Universal Credit Option** - Designed for organizations that have a predetermined budget for training and want to maximize their training dollars. For more details, visit www.sans.org/vouchers.

- **FlexPass Option** - Designed specifically for an organization that has a predetermined number of people who need to be trained. For more details, visit www.sans.org/vouchers.

For orders or questions, please e-mail us at
Vouchers@sans.org
or call **301-654-7267**

Create an Account

Creating your Universal Credit or FlexPass account is easy. Follow the steps below and contact us at **vouchers@sans.org** if you have any questions.

1. Designate a Point of Contact (POC) that will have the responsibility of allocating funds from your Voucher Program account.
2. Decide how much money to deposit into your Voucher Program account.
3. Submit the attached SANS Voucher Program Agreement form.
4. Upon payment, SANS will provide the POC with instructions on how to use your Voucher Program account. See page five for available payment options.

What Students Are Saying:

"This is hands-down, the premiere training opportunity."

- Dan Mather, JICPAC

The SANS Promise

You will be able to use what you learn in class the day you return to the office.

Universal Credit Option

Designed for organizations that have a predetermined budget for training and want to maximize their training dollars.

When you have a set training budget, but need flexibility on training methods, certification, dates, and student names, SANS Universal Credit allows you invest today, earn instant credits, and decide later how to spend. Maximize your investment and extend your fiscal year. Universal Credit accounts are valid for 12 months and you can contribute additional funds during that time or renew the account before it expires. Pricing and savings are detailed on the chart below. If you have any questions, please contact us at **vouchers@sans.org**.

2012 Universal Credit Pricing

Minimum Investment	Maximum Investment	Bonus	Example
$25,000	$50,000	10%	$40,000 investment = $44,000
$50,001	$100,000	20%	$75,000 investment = $90,000
$100,001	$200,000	25%	$150,000 investment=$187,500
$200,001	Call	Ask for quote	Contact Your Account Manager Vouchers@sans.org

Universal Credit Benefits

- Valid for classroom, online learning, and GIAC certification
- Cost savings helps you expand your training budget
- Extends your fiscal year
- Free Learning Management Tool featuring online enrollment and usage reports
- Online access to credits, orders, GIAC certification results and OnDemand usage reports
- Fully transferable
- Only one procurement is needed for twelve months, but you can add funds to renew the account at any time
- Great way to motivate and retain your valued employees

Universal Credits are Valid for the Following SANS Products

- SANS Live Training Events
- SANS vLive!
- Community SANS
- SANS OnDemand
- SANS Mentor
- SelfStudy
- SANS OnSite
- SANS WhatWorks Summits
- SANS Simulcast
- Securing The Human
- SANS Technology Institute Master's Degree Program
- GIAC Exams, Practice Exams, Extensions, Retakes, and Certification Renewal

FlexPass Option

Designed specifically for an organization that has a predetermined number of people who need to be trained.

With a FlexPass account, you purchase a specific number of training courses to be used during a 12-month period. You choose the courses, delivery method and when you want to train. The more you purchase, the more you save! See the pricing chart below and contact us at vouchers@sans.org with any questions.

2012 FlexPass Pricing

Minimum Number of Long Courses	Maximum Number of Long Courses	Average Conference Retail Price	Discount for FlexPass	Discounted Price Per Seat
6	11	$ 4,000	9.1%	$ 3,477
12	24	$ 4,000	13.0%	$ 3,328
25	49	$ 4,000	20.0%	$ 3,060
Over 50		Call for Quote		

FlexPass Benefits

- Valid for classroom or online learning
- Cost savings helps you expand your training budget
- Extends your fiscal year
- Only one procurement is needed for twelve months, but you can add funds to renew the account at any time
- Online access to credits, orders, GIAC certification results and OnDemand usage reports
- Great way to motivate and retain your valued employees

FlexPass is Valid for the Following SANS Products

- SANS Live Training Events
- SANS OnDemand
- SANS vLive!
- Community SANS
- SANS Mentor
- SelfStudy
- GIAC Certification

Please contact your account manager at **vouchers@sans.org** for more details.

PLEASE NOTE: Due to the pre-negotiated discounts SANS Voucher Programs offer, they cannot be combined with any other promotions.

Future SANS Training Events Schedule

SANS Security East 2012
New Orleans, LA
January 17-26, 2012
www.sans.org/security-east-2012

North American SCADA 2012
Lake Buena Vista, FL
January 21-30, 2012
www.sans.org/north-american-scada-2012

SANS Monterey 2012
Monterey, CA
January 30 - February 4, 2012
www.sans.org/monterey-2012

SANS Phoenix 2012
Phoenix, AZ
February 13-18, 2012
www.sans.org/phoenix-2012

SANS 2012
Orlando, FL
March 23-30, 2012
www.sans.org/sans-2012

SANS Northern Virginia 2012
Reston, VA
April 7-13, 2012
www.sans.org/northern-virginia-2012

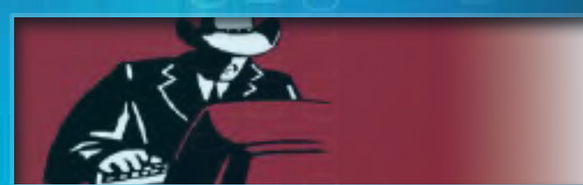
SANS AppSec 2012: Summit & Training
Las Vegas, NV • April 24 - May 2, 2012
www.sans.org/appsec-2012

SANS Cyber Guardian 2012
Baltimore, MD
April 30 - May 5, 2012
www.sans.org/cyber-guardian-2012

SANS Security West 2012
San Diego, CA
May 12-19, 2012
www.sans.org/security-west-2012

SANS Toronto 2012
Toronto, ON
May 14-19, 2012
www.sans.org/toronto-2012

SANS Rocky Mountain 2012
Denver, CO
June 4-9, 2012
www.sans.org/rocky-mountain-2012

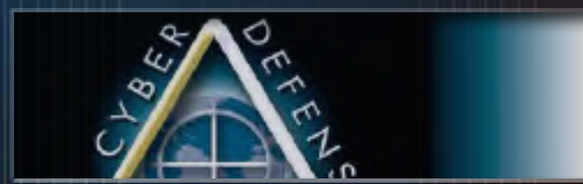


Forensics and Incident Response Summit 2012
Austin, TX • June 20-27, 2012
www.sans.org/forensics-incident-response-summit-2012

SANSFIRE 2012
Washington, DC
July 17-25, 2012
www.sans.org/sansfire-2012

SANS Boston 2012
Boston, MA
August 6-13, 2012
www.sans.org/boston-2012

SANS Network Security 2012
Las Vegas, NV
September 16-23, 2012
www.sans.org/network-security-2012



SANS Cyber Defense Initiative 2012
Washington, DC • December 2012
www.sans.org/cyber-defense-initiative-2012

SANS
5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

PRSRT STD
U.S. POSTAGE
PAID
SANS

PROMO CODE
CC12

Please enter your Promo Code when registering.

Setting the Standard for IT Security Training

SANS

SANS is the most trusted and by far the largest source for IT security training, certification, and research in the world.

Five Tips to Get Approval for SANS Training

1. EXPLORE

- Read this brochure and note the courses that will enhance your role at your organization.
- Use the Roadmap to arm yourself with all the necessary materials to make a good case for attending a SANS training event.
- Note that the core, job-based courses can be complemented by short, skill-based courses of one or two days. We also offer deep discounts for bundled course packages. Consider a GIAC Certification, which will show the world that you have achieved proven expertise in your chosen field.

2. RELATE

- Show how recent problems or issues will be solved with the knowledge you gain from the SANS course.
- Promise to share what you've learned with your colleagues.

3. SAVE

- The earlier you sign up, the more you save, so explain the benefit of signing up early.
- Save even more with group discounts!

Scan to see current course information and specials.

Scan to get up-to-date information for all events and training formats
www.sans.org/info/90921

4. ADD VALUE

- Share with your boss that you can add value to your experience by meeting with network security experts - people who face the same type of challenges that you face every single day.
- Explain how you will be able to get and share great ideas on improving your IT productivity and efficiency.
- Enhance your SANS training experience with SANS@Night talks and the Vendor Expo, which are free and only available at live training events.
- Take advantage of the special SANS host hotel rate so you will be right where the action is!

5. ACT

- With the fortitude and initiative you have demonstrated thus far, you can confidently seek approval to attend SANS training!

Return on Investment: SANS training events are recognized as the best place in the world to get information security education. With SANS, you will gain significant return on investment (ROI) for your InfoSec investment. Through our intensive immersion classes, our training is designed to help your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited.

Remember: SANS is your first and best choice for information and software security training. The SANS Promise is ***"You will be able to apply our information security training the day you get back to the office!"***