SANS

The Most Trusted Name for Information and Software Security Training

# COURSE CATALOG

SECURITY

MANAGEMENT

INCIDENT HANDLING

APPLICATION SECURITY

FORENSICS • IT AUDIT • LEGAL

PENETRATION TESTING & ETHICAL HACKING

# SANS TRAINING AND YOUR CAREER ROADMAP

## SECURITY CURRICULUM

### Beginners

**SEC301**
Intro to Information Security
*GISF*

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

**SEC401**
SANS Security Essentials Bootcamp Style
*GSEC*

### 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*

*Additional Incident Handling Courses*

**SEC517:** Cutting-Edge Hacking Techniques

### Penetration Testing

**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*

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

**SEC660**
Advanced Penetration Testing, Exploits, and Ethical Hacking

*Additional Penetration Testing Courses*

**DEV538:** Web App Pen Testing Immersion

**SEC580:** Metasploit Kung Fu for Enterprise Pen Testing

**SEC710:** Advanced Exploit Development

### 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*

**SEC440:** 20 Critical Security Controls: Planning, Implementing, and Auditing

**SEC556:** Comprehensive Packet Analysis

### 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*

**SEC577:** Virtualization Security Fundamentals

### System Administration

**SEC501**
Advanced Security Essentials – Enterprise Defender
*GCED*

**SEC505**
Securing Windows
*GCWN*

**SEC506**
Securing Linux/Unix
*GCUX*

**SEC509**
Securing Oracle

*Additional System Administration Courses*

**SEC434:** Log Management In-Depth

**SEC464:** Hacker Detection for Systems Administrators with Continuing Education Program

**SEC531:** Windows Command-Line Kung Fu

**SEC546:** IPv6 Essentials

**SEC569:** Combating Malware in the Enterprise: Practical Step-by-Step Guidance

## FORENSICS CURRICULUM

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

**FOR508**
Advanced Computer Forensic Analysis & Incident Response
*GCFA*

**FOR558**
Network Forensics

**FOR563**
Mobile Device Forensics

**FOR610**
REM: Malware Analysis Tools & Techniques
*GREM*

*Additional Forensics Courses*

**FOR526:** Advanced Filesystem Recovery and Memory Forensics

## APPSEC CURRICULUM

### Design & Test

**DEV522**
Defending Web Applications Security Essentials
*GWEB*

**SEC542**
Web App Pen Testing and Ethical Hacking
*GWAPT*

**DEV538**
Web App Pen Testing Hands-on Immersion

### 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 .NET (2-Day Course)

#### C & C++

**DEV543**
Secure Coding in C

#### PCI

**DEV536**
Secure Coding for PCI Compliance

#### PHP

**DEV545**
Secure Coding in PHP

### General / Management

**DEV304**
Software Security Awareness

## 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*

**AUD305:** Technical Communication & Presentation Skills

**AUD429:** IT Security Audit Essentials Bootcamp

**AUD440:** 20 Critical Security Controls: Planning, Implementing, and Auditing

**AUD521:** Meeting the Minimum: PCI/DSS 2.0: Becoming and Staying Compliant

## LEGAL CURRICULUM

**SEC301**
Intro to Information Security
*GISF*

**SEC401**
SANS Security Essentials Bootcamp Style
*GSEC*

**LEG523**
Law of Data Security and Investigations
*GLEG*

GIAC

*GIAC certification available for courses indicated with GIAC acronyms*

## MANAGEMENT CURRICULUM

**SEC301**
Intro to Information Security
*GISF*

**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**
Project Management and Effective Communications for Security Professionals and Managers
*GCPM*

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

*Additional Management Courses*

**MGT305:** Technical Communication and Presentation Skills for Security Professionals

**MGT405:** Critical Infrastructure Protection

**MGT411:** SANS 27000 Implementation & Management *G7799*

**MGT421:** SANS Leadership and Management Competencies

**MGT432:** Information Security for Business Executives

**MGT433:** Securing The Human: Building and Deploying an Effective Security Awareness Program

**MGT438:** How to Establish a Security Awareness Program

**MGT442:** Information Security Risk Management

**MGT514:** Information Security Policy – In Depth

**MGT520:** IT Security Strategic Planning

# Making the Case for Training

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

- Loss of consumer trust
- Legal costs
- Cleaning up systems
- Staff hours

*In 2009, the cost per compromised record involving a criminal act averaged $204.00.*

2009 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, but also know what to do if a breach occurs. These critical actions cannot be handled by tools alone; it takes true knowledge and skills.

*More than 222 million potentially compromised records were reported in 2009.*

The Identity Theft Resource's 2009 Breach Report

## 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

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

-David Howard, Emerson

# Why SANS?

SANS is the most trusted source for computer and information security training in the world. We are known for our hands-on, intensive, immersion training that is designed to help you and your staff master the practical steps necessary for defending systems, networks, and applications.

***Why is SANS the best training 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 Global Information Assurance Certification (GIAC). 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 6-7 for more about GIAC.

The SANS method of training has been effective for over 20 years. More than 15,000 information security professionals a year train with SANS. 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.

Many of the valuable SANS resources are free to all who ask. They include the very popular Internet Storm Center (the Internet's early warning system), the weekly news digest *NewsBites*, the weekly vulnerability digest *@RISK*, flash security alerts, and more than 1,200 award-winning original research papers.

## The SANS Promise

*You will be able to apply our information security training the day you get back to the office.*

# Table of Contents

# Calculating the Return on Your Training Investment

***While you know how important training is to your job, you may be asked to provide the ROI in order to justify the cost. ROI calculates the value of an improvement vs. the cost to achieve it. The challenge with security training is the gains are typically measured in cost avoidance rather than achievement.***

***Here are a few ways to help you calculate ROI and make your case for training.***

## There are five types of losses associated with ROI in cyber security.

1. Revenue loss
2. Productivity loss
3. Remediation costs post breach
4. Loss or compromise of data
5. Reputational damage

> *"SANS always tops other types of training I've had. I return to SANS and recommend it. The instructors, the content, and the labs are great."*
>
> -Kathleen Frederico, Indian Health Service

> *"Excellent class, well worth the time and money spent on attending SANS training."*
>
> -Jon Speak, Trans Union

## 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.

### 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

| Year | 1 | 2 | 3 | 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%***

### Tips When Talking with Supervisors

- Be an expert in the regulatory environment in which you work. Use that to your advantage (PCI, HIPAA, DoD8570).
- Know your organization and use the same methods used to justify other investments – (Payback, NPV, IRR).
- Be a pragmatic business partner to the executives – speak their language.
- 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.

There's no question that cyber security will only increase in importance in the future as attacks on our nation increase and become more sophisticated. Security is constantly evolving and preparing current and future employees to detect, remediate, and prevent intrusions is crucial.

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

**SANS Cyber Ranges** have three classifications, each with their own set of games.

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

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

# Shall we play a game?

## CYBER · FOUNDATIONS

- Designed for measuring aptitude
- 3 modules
  - TCP/IP Networking
  - Operating Systems (Windows and Linux)
  - System Administration (Windows and Linux)
- Each module includes a tutorial and a quiz

## CYBERQUESTS

- 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

## NETWARS

- 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

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.

### 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

## 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

> *"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 online, 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

# Earn Your Master's Degree in Information Security from the SANS Technology Institute!

SANS Technology Institute, an affiliate of the SANS Institute and Global Information Assurance Certification (GIAC), offers one of the few master's programs in the industry with a specific technical focus on information security. The SANS Technology Institute's mission is to develop the leaders who will strengthen the security of cyberspace.

## The STI Master's Program can be Completed in TWO Years

*STI operates on a semester or rolling system. See the recommended degree plans below if you want to complete it in two years. Students may take up to five years to complete their degree.*

> *"After starting the program, I was promoted to Information Security Officer. I believe my involvement in the program was a contributing factor in that happening. I also believe that I have challenged myself, learned a lot about security, and improved my people and presentation skills. Finally, I believe that as a graduate of the program I am in a better positioned to differentiate myself from others in the security field."*
>
> -John Brozycki, Information Security Officer, Hudson Valley FCU

| | First Semester | Second Semester | Third Semester | Fourth Semester | |
|---|---|---|---|---|---|
| **The Master of Science Degree in Information Security Engineering** | **MGT305**<br>Technical Communication and Presentation Skills for Security Professionals<br>**SEC504**<br>Hacker Techniques, Exploits & Incident Handling<br>&<br>*GIAC GCIH Gold*<br>**SEC401**<br>SANS Security Essentials Bootcamp Style<br>&<br>*GIAC GSEC Gold*<br>**CPR:** Work Study – must have taken a course at a large SANS training event before eligible to apply for Work Study | **MGT404***<br>Fundamentals of Information Security Policy<br>*OnDemand*<br>**MGT438***<br>How to Establish a Security Awareness Program<br>*OnDemand*<br>**MGT525****<br>Project Mgt and Effective Communications for Security Professionals and Managers<br>&<br>*GIAC GCPM Gold*<br>**CPR:** Group Discussion & Written Project at same training event where taking 3rd course<br>**CPR:** First Evening Presentation | **CPR:** Joint Written Project – done virtually, it is not done at training events<br>**MGT421***<br>SANS Leadership and Management Competencies<br>*OnDemand*<br>**SEC503**<br>Intrusion Detection In-Depth<br>&<br>*GIAC GCIA Gold*<br>**CPR:** Second Evening Presentation<br>**First Elective Course**<br>***Forensics Focus***<br>FOR408: Computer Forensic Investigations – Windows In-Depth – GCFE Cert<br>***Non-Forensics Focus***<br>Any major SEC/DEV 500/600/700 level course – GIAC Cert<br>or<br>AUD507: Auditing Networks, Perimeters & Systems – GSNA Cert | **CPR:** GSE Certification<br>**FOR508**<br>Advanced Computer Forensic Analysis and Incident Response & *GIAC GCFA Gold*<br>OR<br>**Software Security Training**<br>see **www.sans.edu/programs/msise**<br>& *GIAC Gold*<br>**Second Elective Course**<br>***Forensics Focus***<br>FOR610: REM: Malware Analysis Tools and Techniques – GREM Cert<br>***Non-Forensics Focus***<br>Any major SEC/DEV 500/600/700 level course – GIAC Cert<br>or<br>AUD507: Auditing Networks, Perimeters & Systems – GSNA Cert<br>**CPR:** Awareness Talk – does not require attendance at training event | **For a detailed description of this curriculum, please visit www.sans.edu/ programs/ msise.** |

*In addition to courses and exams, there are seven Community Project Requirements (CPRs) required with both degree programs. Learn more about CPRs at www.sans.edu/programs/community.php.*

| | First Semester | Second Semester | Third Semester | Fourth Semester | |
|---|---|---|---|---|---|
| **The Master of Science Degree in Information Security Management** | **MGT305**<br>Technical Communication and Presentation Skills for Security Professionals<br>**SEC504**<br>Hacker Techniques, Exploits & Incident Handling<br>&<br>*GIAC GCIH Gold*<br>**MGT512**<br>SANS Security Leadership Essentials For Managers with Knowledge Compression™<br>&<br>*GIAC GSLC Gold*<br>**CPR:** Work Study – must have taken a course at a large SANS training event before eligible to apply for Work Study | **MGT404***<br>Fundamentals of Information Security Policy<br>*OnDemand*<br>**MGT438***<br>How to Establish a Security Awareness Program<br>*OnDemand*<br>**MGT525****<br>Project Mgt and Effective Communications for Security Professionals and Managers<br>&<br>*GIAC GCPM Gold*<br>**CPR:** Group Discussion & Written Project at same training event where taking 3rd course<br>**CPR:** First Evening Presentation | **CPR:** Joint Written Project – done virtually, it is not done at training events<br>**MGT421***<br>SANS Leadership and Management Competencies<br>*OnDemand*<br>**MGT411**<br>SANS 27000 Implementation & Management<br>&<br>*GIAC G7799 Gold*<br>*OnDemand*<br>**AUD507**<br>Auditing Networks, Perimeters, and Systems<br>&<br>*GIAC GSNA Gold*<br>**CPR:** Second Evening Presentation | **CPR:** Teaching Assistant for a course you already certified<br>**LEG523**<br>Law of Data Security and Investigations<br>&<br>*GIAC GLEG Gold*<br>**Software Security Training**<br>Choice of courses: see **www.sans.edu/ programs/msism**<br>&<br>*GIAC Gold*<br>**CPR:** Awareness Talk – does not require attendance at training event | **For a detailed description of this curriculum, please visit www.sans.edu/ programs/ msism.** |

**Substitute for Exam, Written Assignment   **MGT525 is offered 2-3 times a year*

**Substitute for Exam, Written Assignment   **MGT525 is offered 2-3 times a year*

## Prerequisites

- A baccalaureate degree from a recognized college or university, or equivalent international education, with a minimum cumulative grade point average of 2.8. There are two exceptions to the 2.8 minimum described on the website. Your baccalaureate does not have to be in the field of information security/information technology.
- At least 12 months of experience in the field.
- Upon completion of the program, have three years of significant work experience in information technology, security or audit. If you are already working in the field, this should not be a problem.

See **www.sans.edu** or contact us at **info@sans.edu** for more details.

## How to Take Courses

Students have a multitude of course delivery options to meet their degree requirements. Courses may be taken at SANS training events or through the following delivery methods: SANS vLive!, SANS OnDemand, or a limited number of SANS SelfStudy.

Not all delivery methods are available for all courses.

## How to Apply

- Complete the downloadable application at **www.sans.edu/downloads/application.pdf**
- Submit the Employer Recommendation of Candidate Form and your resume
- Request undergraduate institution to forward an official sealed transcript to the SANS Technology Institute
- Submit a non-refundable Application Fee
- See **www.sans.edu/admissions** for detailed admission requirements

For admissions questions, please go to **www.sans.edu** or contact Debbie Svoboda, Dean of Admissions, at **info@sans.edu** or **720-941-4932**.

Tuition assistance is available through limited work-study opportunities.

## Authorization

The SANS Technology Institute (STI) is authorized to grant Master's degrees by the Maryland Higher Education Commission.

***Admission and curriculum requirements in effect when a person is admitted are the requirements that will apply to that person.***

DEPARTMENT OF DEFENSE

# *The Deadline for DoD 8570 IAT and IAM Certification has Passed!*

**If you missed the December 2010 deadline, come to SANS and take the training with the HIGHEST pass rate on 8570 required certifications including CISSP, GSLC, GSEC, GPEN, GCIA, GCFA, and more!**

| TECH I | TECH II | TECH III |
|---|---|---|
| A+<br>Network+<br>SSCP | **GSEC**<br>*SEC401: SANS Security Essentials Bootcamp Style*<br>**Security+**<br>SCNP<br>SSCP | **GCED**<br>*SEC501: Advanced Security Essentials - Enterprise Defender*<br>**GCIH**<br>*SEC504: Hacker Techniques, Exploits, and Incident Handling*<br>**CISSP**<br>*MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam*<br>**CISA**<br>SCNA |

> *"It's not about the cert, it's about the knowledge gained in pursuit of the cert."*
>
> -Dave Hull, Trusted Signal, LLC

| MGT I | MGT II | MGT III |
|---|---|---|
| **GSLC**<br>*MGT512: SANS Security Leadership Essentials for Managers with Knowledge Compression™*<br>**GSIF**<br>*SEC301: Intro to Information Security*<br>**Security+** | **GSLC**<br>*MGT512: SANS Security Leadership Essentials for Managers with Knowledge Compression™*<br>**CISSP**<br>*MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam*<br>CISM CAP | **GSLC**<br>*MGT512: SANS Security Leadership Essentials for Managers with Knowledge Compression™*<br>**CISSP**<br>*MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam*<br>CAP |

**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:***

| CND ANALYST | CND INFRASTRUCTURE SUPPORT | CND INCIDENT RESPONDER | CND AUDITOR | CN-SP MANAGER |
|---|---|---|---|---|
| **GCIA**<br>*SEC503: Intrusion Detection In-Depth*<br>CEH | SSCP<br>CEH | **GCIH**<br>*SEC504: Hacker Techniques, Exploits, and Incident Handling*<br>CSIH<br>CEH | **GSNA**<br>*AUD507: Auditing Networks, Perimeters, and Systems*<br>CISA<br>CEH | CISSP-ISSMP<br>CISM |

| IASAE I | IASAE II | IASAE III |
|---|---|---|
| **CISSP**<br>*MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam* | **CISSP**<br>*MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam* | ISSEP<br>ISSAP |

**Get more information at 8570@sans.org and www.sans.org/8570**

SEC301

# Intro to Information Security

*IAM Level I of the Department of Defense Baseline Certification for 8570*

Five-Day Course
30 CPE/CMU Credits

## *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, Security 301 rocks!

We begin by covering basic terminology and concepts, and then move to the basics of computers and networking as we discuss 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

GIAC Certification
www.giac.org

## AUTHOR STATEMENT

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

Fred Kerby

> *"This fundamental course sets the groundwork for a successful future in IT security."*
>
> -Brian Fricke, US Navy/MSC

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • OnDemand • OnSite • SelfStudy

## SEC401

# SANS Security Essentials Bootcamp Style

*IAT Level II of the Department of Defense Baseline Certification for 8570*

Six-Day Course
46 CPE/CMU Credits
Laptop Required

### 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

GIAC Certification
www.giac.org

STI Masters Program
www.sans.edu

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

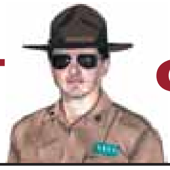
***Maximize your training time and turbo-charge your career in security by learning the full SANS Security Essentials curriculum needed to qualify for the GSEC certification.***

SANS Security Essentials is designed to give anyone interested in network security the skills required to be an effective player in this arena. This in-depth, comprehensive course provides the essential, up-to-the-minute knowledge and skills required for securing systems and organizations and equips you with the language and theory of computer security. Learn all of this and more from the best security instructors in the industry.

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

***Please note that some course material for SEC401 and MGT512 may overlap. We recommend SEC401 for those interested in a more technical course of study and MGT512 for those primarily interested in a leadership-oriented but less technical learning experience.***

**BOOT**



**CAMP**

When Security 401 is taught in a live classroom environment, mandatory bootcamp sessions are held on course days 1-5, usually from 5:15pm - 7:00pm. 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.

### AUTHOR STATEMENT

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 SANS Security Essentials Bootcamp Style, we have really captured the critical aspects of security and enhanced those topics with examples to drive home the key points. After attending this course, 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, PhD

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • Mentor • OnDemand • OnSite • vLive! • SelfStudy

# Advanced Security Essentials – Enterprise Defender

SEC501

### *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 (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

Prevention is ideal, but detection is a must. We have to ensure that we constantly improve security to prevent as many attacks as possible. This prevention/ protection occurs externally and internally. 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 – 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.

## AUTHOR STATEMENT

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 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 complement SEC401 with no overlap and continue to build a solid security foundation for network practitioners.
-Eric Cole, PhD

**Six-Day Course**
**36 CPE/CMU Credits**
**Laptop Required**

### 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

GCED

**GIAC Certification**
www.giac.org

### *PREREQUISITE*

***SEC401 is recommended but not required.***

> *"This was a great class. The instructor had great high energy and kept things moving!"*
>
> -Michelle Herd,
> University of Denver

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • OnDemand • OnSite • vLive!

SEC502

# Perimeter Protection In-Depth

Six-Day Course
36 CPE/CMU Credits
Laptop Required

## Who Should Attend

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

GIAC Certification
www.giac.org

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

> *"The expertise of the trainer is impressive, real life situations explained, very good manuals. Best training ever!"*
>
> -Jerry Robles de Medina Godo CU

### *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 are 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.

## AUTHOR STATEMENT

One of the most rewarding things I have ever done in my career is author this course material. It is really difficult to find solid, unbiased advice for securing your network. Vendors must watch their bottom line. This need can manifest itself in some interesting ways, like giving you poor advice that focuses more on reducing their support costs than increasing your security posture. Is it any surprise that vendor training has turned into a marketing opportunity rather than a chance to tell you how to work around the problems in their product? The Internet can also be hit or miss. There are testing centers, news sites, blogs, etc., but most are either owned by a security vendor, do work for them, or sell ad space to them. There are individuals who honestly want to be helpful, but they lack the expertise to do so effectively. For example, post this question to any given security forum or mailing list: "I need a new firewall. Can anyone recommend something?" and watch the product recommendations come pouring in. How helpful can this advice really be when they know nothing about your network or specific needs? -Chris Brenton

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • OnDemand • OnSite • vLive!

# Intrusion Detection In-Depth

## SEC503

*CND Analyst for the Department of Defense Baseline Certification for 8570*

***Learn practical, hands-on intrusion detection and traffic analysis from top practitioners/authors in the field.***

This is the most advanced network intrusion detection program that has ever been taught. All of the course material is either new or just updated to reflect the latest attack patterns. This series is jam-packed with network traces and analysis tips. The emphasis is on increasing students' understanding of the workings of TCP/IP and Hex, methods of network traffic analysis, and one specific network intrusion detection system—Snort. This course is not a comparison or demonstration of multiple NIDS. Instead, the knowledge/information provided here allows students to better understand the qualities that go into a sound NIDS and the "whys" behind them so that they will be better equipped to make a wise selection for their 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/training/tcpip_quiz.php**) in order to fully understand the topics that will be discussed. Although others may benefit, this course is most appropriate for students who are or will become intrusion detection 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 for all experience levels. We strongly recommend that you spend some time getting familiar with TCPdump, WINdump, or another network analyzer output before coming to class.

### AUTHOR STATEMENT

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, and we have learned how to pass those on to the students. Attendees will learn how TCP/IP really works from instructors who 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

*"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

**Six-Day Course**
**36 CPE/CMU Credits**
**Laptop Required**

### 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 Masters Program**
www.sans.edu

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

### PREREQUISITES

***You must possess at least a working knowledge of TCP/IP and Hex. See www.sans.org/training/tcpip_quiz.php to test your TCP/IP and Hex basics knowledge.***

SEC504

# Hacker Techniques, Exploits, and Incident Handling

*CND Incident Responder for the Dept. of Defense Baseline Certification for 8570*

Six-Day Course
36 CPE/CMU Credits
Laptop Required

## 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

GIAC Certification
www.giac.org

STI Masters Program
www.sans.edu

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

***If your organization has an Internet connection or a disgruntled employee (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 to the spyware your otherwise wholesome users inadvertently downloaded, 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, this course helps you turn the tables on computer attackers. It 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. This workshop also includes the unique SANS Capture-the-Flag event on the last day where you will apply your skills developed throughout the session to match wits with your fellow students and instructor in a fun and engaging learning environment. You'll get to attack the systems in our lab and capture the flags to help make the lessons from the whole week more concrete. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

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

***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.***

## AUTHOR STATEMENT

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 course, 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

# Securing Windows

SEC505

### *Will you be transitioning from Windows XP to Windows 7?*

The 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 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.

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 lack 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.

## AUTHOR STATEMENT

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 seminar. The Securing Windows course is packed with interesting and useful advice which isn't so easy to find on the Internet. We always have a good time, so I hope to meet you at the next training event! -Jason Fossen

**Six-Day Course**
**36 CPE/CMU Credits**
**Laptop Recommended**

## 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 web masters 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)

**GIAC Certification**
www.giac.org

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

SEC542

# Web App Penetration Testing and Ethical Hacking

Six-Day Course
36 CPE/CMU Credits
Laptop Required

### Who Should Attend

- General security practitioners
- Website designers and architects
- Developers

GIAC Certification
www.giac.org

STI Masters Program
www.sans.edu

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

*"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

## *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.

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.

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.

*Kevin Johnson*

### AUTHOR STATEMENT

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

# Network Penetration Testing and Ethical Hacking

SEC560

Six-Day Course
36 CPE/CMU Credits
Laptop Required

### *Find Security Flaws Before the Bad Guys Do.*

Security vulnerabilities, such as weak configurations, unpatched systems, and botched architectures, continue to plague organizations. Enterprises need people who can find and eradicate flaws from our infrastructures in a professional manner. 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.

*IMPORTANT NOTE: SEC560 is one of the most technically rigorous courses offered by SANS. Attendees are expected to have a working knowledge of TCP/IP; cryptographic routines, such as DES, AES, and MD5; and the Windows and Linux command lines before they step into class. Although SEC401 and SEC504 are not prerequisites for SEC560, these courses cover the groundwork that all SEC560 attendees are expected to know. This course is technically in-depth and programming knowledge is NOT required.*

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 in which students will conduct a penetration test against a hypothetical target organization following all of the steps we've covered over the last six days.

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 address how penetration testing should be integrated as a piece of a comprehensive enterprise information security program.

## AUTHOR STATEMENT

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 hands-on exercises that culminate in a final pen-testing extravaganza lab.
-Ed Skoudis

*Ed Skoudis*

### 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

GIAC Certification
www.giac.org

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

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • Mentor • OnDemand • OnSite • vLive! • SelfStudy

SEC566

# Implementing and Auditing the 20 Critical Security Controls – In Depth

Five-Day Course
30 CPE/CMU Credits
Laptop Required

## 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, listed below, 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 through 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 **http://www.sans.org/critical-security-controls**.

One of the best features of the course is that it uses offense to inform defense. In other words, you will learn about the actual attacks that you'll be stopping or mitigating. That makes the defenses very real, and it makes you a better security person.

## Top 20 Critical Security Controls

*Critical Controls Subject to Automated Collection, Measurement, and Validation:*

1 Inventory of Authorized and Unauthorized Devices
2 Inventory of Authorized and Unauthorized Software
3 Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4 Secure Configurations of Network Devices, such as Firewalls, Routers, and Switches
5 Boundary Defense
6 Maintenance and Analysis of Security Audit Logs
7 Application Software Security
8 Controlled Use of Administrative Privileges
9 Controlled Access Based On Need to Know
10 Continuous Vulnerability Assessment and Remediation
11 Account Monitoring and Control
12 Malware Defenses
13 Limitation and Control of Network Ports, Protocols, and Services
14 Wireless Device Control
15 Data Loss Prevention

*Additional Critical Controls (not directly supported by automated measurement and validation):*

16 Secure Network Engineering
17 Penetration Tests and Red Team Exercises
18 Incident Response Capability
19 Data Recovery Capability
20 Security Skills Assessment and Training to Fill Gaps

Eric Cole, PhD

### AUTHOR STATEMENT

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. -Eric Cole, PhD and James Tarala

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • OnSite

# Wireless Ethical Hacking, Penetration Testing, and Defenses

**SEC617**

***Despite the security concerns many of us share regarding wireless technology, it is here to stay.***

In fact, not only is wireless here to stay, it is growing in deployment and utilization with wireless LAN technology and WiFi as well as with other applications, including cordless telephones, smart homes, embedded devices, and more. Technologies, such as ZigBee and WiMAX, offer new methods of connectivity to devices, while other wireless technologies, 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 such as 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.

**The SWAT Toolkit consists of:**

- Powerful 500 mW ALFA 802.11a/b/g/n wireless card
- USB Global Positioning System (GPS) adapter
- High-power Bluetooth interface with external antenna connector
- All software and tools used in lab exercises based on Backtrack 4

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, this course 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, there are 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. Combine this with excellent SANS instructors, and everyone can take this class and gain useful and valuable skills for attacking and defending wireless networks.

GIAC Certification
www.giac.org

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

*Joshua Wright*

**Six-Day Course**
**36 CPE/CMU Credits**
**Laptop Required**

## Who Should Attend

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

## AUTHOR STATEMENT

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 email me at jwright@sans.org.
-Joshua Wright

**Delivery Methods** *(Visit pages 46-47 for more details)*

Live Events • Mentor • OnDemand • OnSite • vLive! • SelfStudy

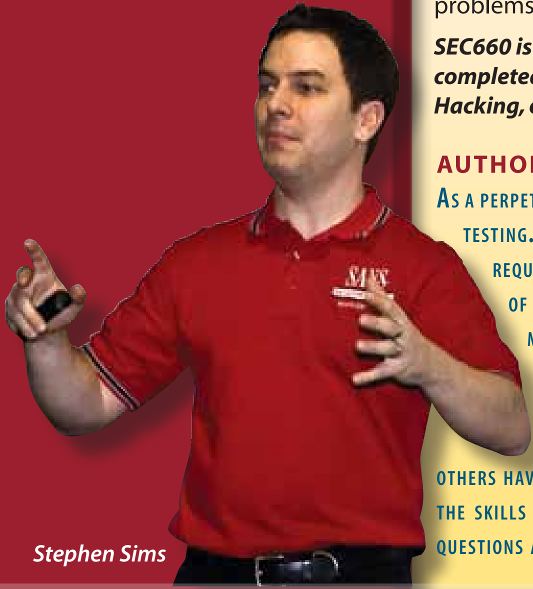
SEC660

# Advanced Penetration Testing, Exploits, and Ethical Hacking

Six-Day Course
46 CPE/CMU Credits
Laptop Required

## Who Should Attend

- Network and Systems Penetration Testers – SEC660 gives penetration testers the training needed to perform advanced penetration testing against known or unknown applications, services, and network systems. It gives them the expertise to perform complex attacks and develop their own exploits for existing and new frameworks.
- Incident Handlers – The ability to understand advanced attack techniques and analyze exploit code can help a handler identify, detect, respond to an incident.
- Application Developers – SEC660 provides developers with the knowledge to create proof-of-concept exploit code and document their findings.
- IDS Engineers – SEC660 teaches IDS professionals how to analyze exploit code and identify weaknesses. This knowledge can be used to write better IDS signatures and understand the impact of an alert.



*Stephen Sims*

## *Preparing Students for the Next Generation of Attacks*

It is well-known that attackers are becoming cleverer 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.

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.

***SEC660 is designed as a logical progression point for those who have completed SANS SEC560 Network Penetration Testing and Ethical Hacking, or for those with existing penetration testing experience.***

**GIAC Certification**
***Coming Soon!***
www.giac.org

### AUTHOR STATEMENT

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, Joshua Wright, and Bryce Galbraith

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • OnSite

# Computer Forensic Investigations – Windows In-Depth

FOR408

*This course has been recently renamed to better reflect the content and skill level. The course content has remained the same.*

## *Master computer forensics. Learn essential investigation techniques.*

With today's ever-changing technologies and environments, it is inevitable that organizations will deal with some form of cyber crime. These forms include, but are not exclusive to, fraud, insider threat, industrial espionage, and phishing. In order to help solve these cases, organizations are hiring digital forensic professionals and calling cybercrime law enforcement agents to fight and solve these cyber crimes.

FOR408 focuses on the critical knowledge that a computer forensic investigator must know to investigate computer crime incidents successfully. You will learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation.

This course covers the fundamental steps of the in-depth computer forensic 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 such as FTK, Registry Analyzer, FTK Imager, Prefetch Analyzer, and much more.

FOR408 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.

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

**With this course, you will receive a FREE SANS Investigative Forensic Toolkit (SIFT) Essentials with a Tableau Write Block Acquisition Kit.** The entire kit will enable each investigator to accomplish proper and secure examinations of SATA, IDE, or Solid State Drives (SSD). The toolkit consists of:

- One Tableau T35es Write Blocker (Read-Only)
- IDE Cable/Adapters
- SATA Cable/Adapters
- FireWire and USB Cable Adapters
- Forensic Notebook Adapters (IDE/SATA)
- HELIX Incident Response & Computer Forensics Live CD
- SANS VMware-Based Forensic Analysis Workstation
- Course DVD: Loaded with case examples, tools, and documentation

**GIAC Certification**
www.giac.org

**STI Masters Program**
www.sans.edu

### AUTHOR STATEMENT

SANS COMPUTER FORENSICS GRADUATE THWARTS BANK HEIST. Headlines similar to these are now a reality as former students have e-mailed me regularly about how they were able to use their digital forensic skills in very real situations. Graduates of Computer Forensics Essentials are the front line troops deployed when incidents occur. From stopping online bank heists to logic bombers trying to destroy data that could affect many lives, SANS digital forensic graduates are battling and winning the war on crime. Graduates have described solved cases involving computer break-ins, intellectual property theft, fraud, and, in some cases, internal infractions by belligerent employees. Knowing that this course places the correct methodology and knowledge in the hands of responders who thwart the plans of criminals or foreign cyber attacks brings me great comfort. Graduates are doing it. Daily. I am proud that the Computer Forensics Essentials course at SANS helped prepare them to fight and solve crime. - Rob Lee

**Six-Day Course**
**36 CPE/CMU Credits**
**Laptop Required**

### Who Should Attend

- Information technology professionals who wish to learn the core concepts in computer forensics investigations
- Incident Response Team Members who are responding to security incidents and need to utilize computer forensics to help solve their cases
- Law enforcement officers, federal agents, or detectives who desire to become a subject matter expert on computer forensics for Windows based operating systems
- Information security managers who need to understand digital forensics in order to understand information security implications and potential litigation related issues or manage investigative teams
- Information technology lawyers and paralegals who desire to have a formal education in digital forensic investigations
- Anyone interested in computer forensic investigations with a background in information systems, information security, and computers

*Rob Lee*

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • OnDemand • OnSite • vLive!

FOR508

# Computer Forensic Investigations – Windows In-Depth

Six-Day Course
36 CPE/CMU Credits
Laptop Required

## Who Should Attend

- Incident response team members that respond to complex security incidents/intrusions and need computer forensics to help solve their cases
- Computer forensic professionals who want to solidify and expand their understanding of file system forensics and incident response related topics
- Law enforcement officers, federal agents, or detectives who want to master computer forensics and expand their investigative skill set to include data breach investigations, intrusion cases , and tech-savvy cases
- Information security professionals with some background in hacker exploits, penetration testing, and incident response
- Information security managers who would like to master digital forensics to understand information security implications and potential litigation or manage investigative teams

**GIAC Certification**
www.giac.org

**STI Masters Program**
www.sans.edu

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

*This course has been recently renamed to better reflect the content and skill level.*
*The course content has remained the same.*

### *Data breaches and advanced intrusions are occurring daily.*

Sensitive data and intellectual property is stolen from systems that are protected by sophisticated network and host-based security. 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 dubbed the Advanced Persistent Threat have proved difficult to suppress. FOR508 will help you respond to and investigate these incidents.

This course will give you a firm understanding of advanced incident response and computer forensics tools and techniques to investigate data breach intrusions, tech-savvy rogue employees, advanced persistent threats, and complex digital forensic cases.

Utilizing advances in spear phishing, web application attacks, and persistent malware, these new sophisticated attackers advance rapidly through your network. Incident responders and digital forensic investigators must master a variety of operating systems, investigation techniques, incident response tactics, and even legal issues in order to solve challenging intrusion cases. FOR508 will teach you critical forensic analysis techniques and tools in a hands-on setting for both Windows- and Linux-based investigations.

Attackers will use anti-forensic techniques to hide their tracks. They use rootkits, file wiping, timestamp adjustments, privacy cleaners, and complex malware to hide in plain sight, avoiding detection by standard host-based security measures. Everything will leave a trace; you merely need to know where to look.

Learning more than just how to use a forensic tool, by taking this course you will be able to demonstrate how the tool functions at a low level. You will become skilled with new tools, such as the Sleuthkit, Foremost, and the HELIX3 Pro Forensics Live CD. SANS' hands-on technical course arms you with a deep understanding of the forensic methodology, tools, and techniques to solve advanced computer forensics cases.

### *FREE SANS Investigative Forensic Toolkit (SIFT) Advanced*

**The *SIFT Kit Advanced* consists of:**

- F-RESPONSE TACTICAL
  - TACTICAL enables investigators to access physical drives and physical memory of a remote computer via the network
  - Able to use any tool to parse the live remote system including the SIFT Workstation
  - Perfect for Intrusion Investigations and Data Breach Incident Response situations
- Hard Drive USB mini adapter kit for SATA/IDE hard drives 1.8"/2.5"/3.5"/5.25" (Read and Write)
- SANS VMware based Forensic Analysis Workstation (SIFT Workstation)
- Best-selling book "File System Forensic Analysis" by Brian Carrier
- Helix3 Pro that will be individually licensed to each student.
- Course DVD loaded with case examples, tools, and documentation

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

## AUTHOR STATEMENT

"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. FOR508 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

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • Mentor • OnDemand • OnSite • vLive! • SelfStudy

# Advanced Computer Forensic Analysis and Incident Response

FOR558

## "CATCHING HACKERS ON THE WIRE."

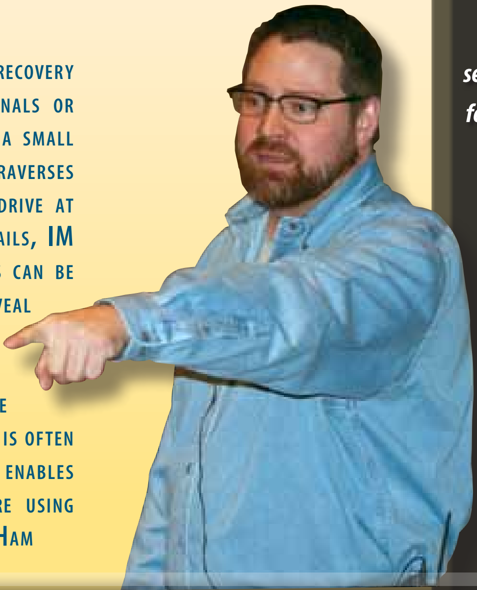
Enterprises all over the globe are compromised remotely by malicious hackers each day. Credit card numbers, proprietary information, account usernames, passwords, and a wealth of other valuable data are surreptitiously transferred across the network. Insider attacks leverage cutting-edge covert tunneling 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.

This course will teach you to how to follow the attacker's footprints and analyze evidence from the network environment. Every student will receive a SNIFT Kit, which is a fully-loaded, portable forensics workstation, designed by network forensics experts. Network equipment, such as web proxies, firewalls, IDS, routers and switches, contains 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. You will gain 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 dive 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. 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 FOR 508: Advanced Computer Forensic Analysis and Incident Response, using the same fundamental methodology to recover and analyze evidence from network-based devices.

### AUTHOR STATEMENT

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



Jonathan Ham

**Five-Day Course**
**31.5 CPE/CMU Credits**
**Laptop Required**

### Who Should Attend

- Incident Response team members
- Network and computer forensic professionals
- Law enforcement officers, federal agents, or detectives
- Information security professionals
- Networking professionals
- Anyone with a firm technical background who might be asked to investigate

### PREREQUISITES

*Students should be familiar with basic networking fundamentals, such as the OSI model and basics of TCP/IP. Please ensure that you can pass the SANS TCP/IP & Hex Knowledge quiz. Students should also have basic familiarity with Linux or willingness to learn in a Linux-based environment. This course is particularly recommended for students who have previously attended either FOR508 or SEC503.*

*If you are just beginning in information security, then this course is not appropriate for you as the basics of computer forensics, system administration, and hacker techniques will not be covered.*

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • OnSite

FOR563

# Network Forensics

**Five-Day Course**
**31.5 CPE/CMU Credits**
**Laptop Required**

## Who Should Attend

- Incident Response team members
- Network and computer forensic professionals
- Law enforcement officers, federal agents, or detectives
- Information security professionals
- Networking professionals
- Anyone with a firm technical background who might be asked to investigate

## PREREQUISITES

*Students should be familiar with basic networking fundamentals, such as the OSI model and basics of TCP/IP. Please ensure that you can pass the SANS TCP/IP & Hex Knowledge quiz. Students should also have basic familiarity with Linux or willingness to learn in a Linux-based environment. This course is particularly recommended for students who have previously attended either FOR508 or SEC503.*

*If you are just beginning in information security, then this course is not appropriate for you as the basics of computer forensics, system administration, and hacker techniques will not be covered.*

*"This is a great course because it's extremely comprehensive, up-to-date, and not software specific."*

-Kevin Moore,
Software Engineering
Inst/CMU

***Mobile device forensics is a rapidly evolving field, creating exciting opportunities for practitioners in corporate, criminal, and military settings.***

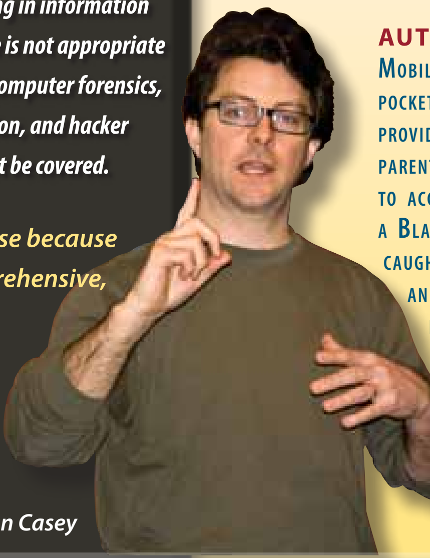
Written for students who are both new to and already familiar with mobile device forensics, this hands-on course provides the core knowledge and skills that a digital forensic investigator needs to process cell phones, PDAs, and other mobile devices. Using state-of-the art tools, you will learn how to forensically preserve, acquire, and examine data stored on mobile devices and utilize the results for internal investigations or in civil/criminal litigation.

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.

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. The 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 apply them to an actual investigation.

Laptops are required for this course. A variety of devices will be available for you to work with during the course. You are also encouraged to bring used mobile devices and SIM cards from home to experiment with using the tools and techniques in this course, but this is not required.

**PREREQUISITE: Students should have an understanding of fundamental principles and processes in digital forensics, including acquisition, examination, and presentation of results. In addition, students should be familiar with reading and interpreting data in hexadecimal format.**



*Eoghan Casey*

## AUTHOR STATEMENT

Mobile devices are becoming ubiquitous, delivering powerful technology into our pockets, keeping us connected wherever we are, and creating new security risks while providing valuable sources of evidence. 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. 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 videotaped their crimes using mobile devices. 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

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • OnSite

# Reverse-Engineering Malware: Malware Analysis Tools & Techniques

FOR610

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

This popular five-day course discusses practical approaches to examining Windows malware using a variety of monitoring utilities, a disassembler, a debugger, and other tools useful for reverse-engineering malicious software. You don't have to be a full-time malware searcher to benefit from this course—as organizations increasingly rely on their staff to act as first responders during a security incident, malware analysis skills become increasingly important.

LEARN REM

By covering both behavioral and code analysis approaches, this unique course provides a rounded approach to reverse-engineering. 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 reverse-engineering; however, the difficulty level of concepts and techniques increases quickly as the course progresses.

In the first half of the course, you will learn how to set up an inexpensive and flexible laboratory for understanding inner-workings of malware and demonstrate the process by exploring capabilities of real-world specimens. You will learn to examine the program's behavioral patterns and assembly code and study techniques for bypassing common code obfuscation mechanisms. The course also explores how to analyze browser-based malware.

In the second half of the course, you will review key assembly language concepts. You will learn to examine malicious code to understand its flow by identifying key logic structures, looking at examples of bots, rootkits, key loggers, and so on. You will understand how to work with PE headers and handle DLL interactions. You will also develop skills for analyzing self-defending malware through advanced unpacking techniques and bypassing code-protection mechanisms. Finally, you will discover how to bypass obfuscation techniques employed by browser-based malicious scripts.

Hands-on workshop exercises are an essential aspect of this course and allow you to apply reverse-engineering techniques by examining malicious code in a carefully controlled environment. When performing the analysis, you will study the supplied specimen's behavioral patterns and examine key portions of its assembly code.

## Prerequisites:

- **Students should have a computer system that matches the stated laptop requirements. Some software needs to be installed before you come to class.**
- **Students should be familiar with using Windows and Linux operating environments and be able to troubleshoot general connectivity and setup issues.**

**REM course on YouTube**
**http://www.youtube.com/watch?v=5AFdZ0v23YA**

*Lenny Zeltser*

**Five-Day Course**
**30 CPE/CMU Credits**
**Laptop Required**

## Who Should Attend

- Anyone whose job requires an understanding of key aspects of malicious programs
- Individuals with responsibilities in incident handling, forensic analysis, Windows security, and system administration
- Individuals responsible for supporting their organization's internal security needs
- Engineers from security product and service companies who are looking to deepen their malware analysis expertise

GIAC Reverse Engineering Malware GREM

**GIAC Certification**
www.giac.org

SANS Technology Institute Knowledge for Peace

**STI Masters Program**
www.sans.edu

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • Mentor • OnDemand • OnSite • vLive!

MGT414

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

*IAT Level III and IAM Levels II and III of the Dept. of Defense Baseline Certification for 8570*

Six-Day Course
46 CPE/CMU Credits
Laptop NOT Required

## 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 their current job
- In short, if you desire a CISSP or your job requires it, MGT414 is the training for you

GIAC Certification
www.giac.org

## 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*

> *"The level of detail and depth of knowledge provided by the instructor exceeded my expectations."*
>
> -Tom Hughes, Cornice Networks, LLC

***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:

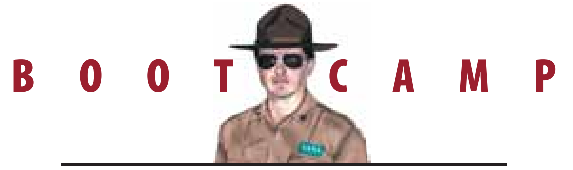
| | |
|---|---|
| Domain 1 | Information Security Governance & Risk Management |
| Domain 2 | Access Controls |
| Domain 3 | Cryptography |
| Domain 4 | Physical (Environmental) Security |
| Domain 5 | Security Architecture & Design |
| Domain 6 | Business Continuity & Disaster Recovery Planning |
| Domain 7 | Telecommunications & Network Security |
| Domain 8 | Application Security |
| Domain 9 | Operations Security |
| Domain 10 | Legal, Regulations, Compliance & Investigations |

***Obtaining your CISSP® certification consists of:***

- **Fulfilling minimum requirements for professional work experience**
- **Completing the Candidate Agreement**
- **Periodic audit based on submission 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**

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.

***Note:** The official (ISC)² courseware and the CISSP® exam are NOT provided as part of the training.*



*When MGT414 is taught in a live classroom environment, there are additional bootcamp sessions*
**Evening Bootcamp Sessions:** 5:00pm - 7:00pm days 1 - 5.
**Morning Bootcamp Sessions:** 8:00am - 9:00am days 2 - 6.

## AUTHOR STATEMENT

The CISSP® certification has been around for almost 10 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 aspects of the 10 domains of knowledge.
-Eric Cole, PhD

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • Mentor • OnDemand • OnSite • vLive! • SelfStudy

# SANS Security Leadership Essentials for Managers with Knowledge Compression™

MGT512

*IAM Levels I, II, and III of the Department of Defense Baseline Certification for 8570*

***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 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.

*Please note that some course material for SEC401 and MGT512 may overlap. We recommend SEC401 for those interested in a more technical course of study and MGT512 for those primarily interested in a leadership-oriented but less technical learning experience.*

Essential topics covered in this management course 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. Only SANS top instructors with management experience are invited to teach this course, and you will be able to put what you learn into practice the day you get back into the office.

**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.**

## AUTHOR STATEMENT

When SANS designed the Security Leadership Essentials for Managers with Knowledge Compression™ 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. 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

Stephen Northcutt

**Five-Day Course**
**33 CPE/CMU Credits**
**Laptop NOT Required**

### Who Should Attend

- This course is designed and taught for mid-level to C-level managers and leaders. It will give you the ability to better manage IT projects in a secure manner.
- Anyone with 8570 information assurance management responsibilities
- Senior executives
- Vice presidents
- Security or assurance officers and managers
- Upwardly mobile managers

**GIAC Certification**
www.giac.org

**STI Masters Program**
www.sans.edu

*"The course content is very good. It is current to today's world. Stephen's years of experience/stories move this course into the 'Excellent' category."*
-Jesse Smith, WCNOC

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • Mentor • OnDemand • OnSite • SelfStudy

MGT514

# Information Security Policy – In Depth

Two-Day Course
12 CPE/CMU Credits
Laptop Recommended

## Who Should Attend

- Managers with security program responsibilities
- Security professionals with policy development and assessment duties
- Anyone who serves on a policy steering committee

## Sampling of Course Topics

- Policy Establishes Bounds for Behavior
- Policy Empowers Users to do the Right Thing
- Should and Shall, Guidelines and Policy
- ISMS as Governing Policy
- Policy versus Procedure
- Policy Needs Assessment Process
- Organizational Assumptions, Beliefs and Values (ABVs)
- Relationship of Mission Statement to Policy
- Organizational Culture
- Using the Principles of Psychology to Implement Policy
- Applying the SMART to Policy
- How Policy Protects People, Organizations and Information
- Case Study, the Process to Handle a New Risk (Sexting)
- Policy Header Components and How to Use Them
- Issue Specific Policies
- Behavior Related Polices, Acceptable Use, Ethics
- Warning Banners
- Policy Development Process
- Policy Review and Assessment Process
- Wrap up, the Six Golden Nuggets of Policy

### *The most in-depth coverage of security policy ever developed.*

By the end of the course your head will be spinning. Students and other SANS instructors that have seen the draft of the material have the same comment, "I never realized there is so much to know about security policy." Any security manager, any one assigned to review, write, assess, or support security policy and procedure can benefit from policy in depth.

You will learn what policy is, positive and negative tone, consistency of policy bullets, how to balance the level of specificity to the problem at hand, the role of policy, awareness and training, the SMART approach to policy development, and assessment. We cover different levels of policy from ISMS governing policy to detailed issue specific policies like acceptable use, approved encryption, and end of life disposal of IT assets. 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 technique to create successful policy that users will read and follow; 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.

Business needs change, the environment changes, new risks are always on the horizon, and critical systems are continually exposed to new vulnerabilities. Policy development and assessment is a never-ending process. This is a hands-on, exercise intensive course on writing, implementing, and assessing security policies.

### AUTHOR STATEMENT

I have been told, "do this according to your security policy," or "you should have this in your security policy" so many times, but no one ever said how to create a policy. In 1997, an instructor in a class I was taking said that and I remember thinking, "Alrighty then, I am going to figure this out." As a result, I started a research project with SANS and a colleague, John Ritter, to determine the steps to consistently develop good, and the right, policy and then get it approved. We do not claim to have all the answers, but this is the most comprehensive security policy training available. A lot of material can be found on the web if you are skilled at targeted Google searches, but I have been researching, improving, and adding to the material for a long time, and frankly time is money. In two course days, the diligent student will become an expert on information security policy. -Stephen Northcutt

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • OnDemand • OnSite • SelfStudy

# Project Management and Effective Communications for Security Professionals and Managers

MGT525

***Designed to give you the knowledge and tools you need to become a top-notch project manager, this course focuses on effective communication, human resources, and quality management.***

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. This class has a strong focus on effective communication, risk analysis, and continuous monitoring and utilizes 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. A copy of the 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 solidify your preparation for the 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. Keeping in line with prevalent needs from the InfoSec industry, we look at projects that create and maintain services and cover in depth how cost, time, quality, and risk affect IT security and the services we provide to others both inside and outside of our organizational boundaries. We go into great detail covering human resource management as well as effective communication and conflict resolution.
People are the most valuable resource we have on a project, and the communication and conflict resolution techniques presented can be used in all areas of professional work. Above all, projects fail or succeed because of the people involved. You want to make sure the people involved with the development and execution of your project build a strong team and communicate effectively.

> *"This course will provide a wealth of information to advance my career in the IT field."*
>
> -Doreen Lawrence, Los Alamos National Lab

PMP exams are not hosted by SANS. You will need to make separate arrangements to take the PMP exam.

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

## AUTHOR STATEMENT

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 work to galvanize your understanding of the key concepts with an emphasis on practical application and execution. Since project managers spend the vast majority of their time communicating with others, we focus on traits and techniques that enable effective communication. As people are the most critical asset in the project management process, effective and thorough communication is essential. -Jeff Frisk

Jeff Frisk

**Six-Day Course**
**36 CPE/CMU Credits**
**Laptop NOT Required**

## Who Should Attend

- Security professionals who are 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
- Security professionals and managers who would like to utilize effective communication techniques and proven methods to relate better to people
- Individuals interested in preparing for the Project Management Institute's – Project Management Professional (PMP®) Exam

GIAC Certification
www.giac.org

STI Masters Program
www.sans.edu

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • OnSite

LEG523

# Law of Data Security and Investigations

Five-Day Course
30 CPE/CMU Credits
Laptop NOT Required

## Who Should Attend

- Security and IT professionals
- Lawyers
- Paralegals
- Auditors
- Accountants
- Compliance officers
- Vendors of security technologies and services
- Investigators
- Technology managers
- Law enforcement
- Privacy officers

GIAC Certification
www.giac.org

STI Masters Program
www.sans.edu

*"This course provided tools to help me protect my company's assets on the Internet in a noble and justifiable way I had never thought of before – great insights and great discussions."*
-Paul Jacobsen, Fluor Hanford

***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 needed professional training is uniquely available in SANS' LEG523 series of courses, including skills in the analysis and use of contracts, policies, and records management procedures.

GIAC certification under 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.

This course 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. 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

### ▸ 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.*

Ben Wright

**Special Features!** This legal offering will cover many recent developments, including TJX, amendments to the Federal Rules of Civil Procedure pertaining to the discovery of electronic records in litigation, and the torment Hewlett-Packard has endured for spying on journalists and members of its board of directors. Hewlett-Packard employed its internal security team and outside investigators in ways that raised legal questions (can you say, "computer crime law"?) and led to criminal indictments. All security professionals should know the lessons from these cases.

*"This course adopts an increasingly global perspective. Non-US professionals attend the LEG523 course because there is no training like it anywhere else in the world. A lawyer from a European police agency recently attended and expressed high praise for the course when it was over. Although as a US attorney Mr. Wright does not know every law in the world, students like this European lawyer help him improve the course and include more non-US content each time he teaches it."*

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • OnDemand • OnSite • SelfStudy

# Defending Web Applications Security Essentials

DEV522

## *Defending web applications is critical!*

Traditional network defenses such as firewalls fail to secure web applications, which have to be available to large user communities. The amount 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.

The class goes beyond classic web applications and includes coverage of Web 2.0 technologies like AJAX and web services.

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. An example of 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

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.

### AUTHOR STATEMENT

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. -Jason Lam and Johannes Ullrich, PhD

*Johannes Ullrich, PhD*

**Six-Day Course**
**36 CPE/CMU Credits**
**Laptop Required**

### 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

**GIAC Certification**
www.giac.org

**STI Masters Program**
www.sans.edu

DEV541

# Secure Coding in Java/JEE: Developing Defensible Applications

**Four-Day Course**
**24 CPE/CMU Credits**
**Laptop Required**

### 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

GIAC Certification
www.giac.org

STI Masters Program
www.sans.edu

## *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.

### The Only Course Covering the Key Elements of Secure Application Development in Java

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 being measured in the third-party assessments as defined in the Essential Skills for Secure Programmers Using Java/JavaEE. (You can find the Essential Skills document at **www.sans-ssi.org/blueprint_files/java_blueprint.pdf**.)

### What Does the Course Cover?

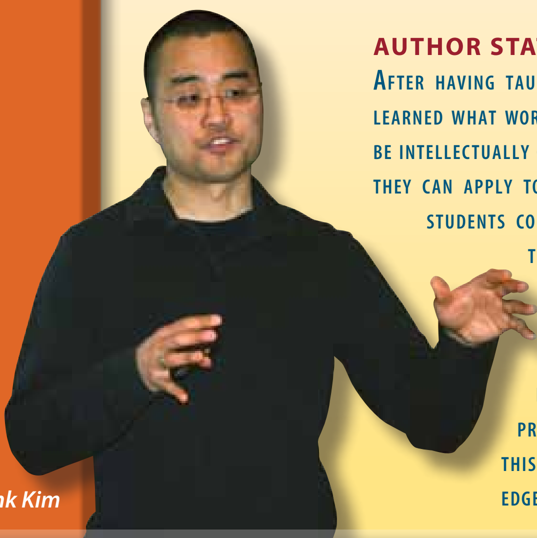
This is a comprehensive course covering a huge set of skills and knowledge. It's not a high-level theory course. It's about real programming. In this course you will examine actual code, work with real tools, build applications, and gain confidence in the resources you need for the journey to improving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

***A two-day Java essentials course is available. Visit www.sans.org/security-training/essential-secure-coding-in-java-jee-1332-mid for more details.***

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 that flaw.

### Prerequisites

**Students should have at least one years' experience working with the JEE framework and should have thorough knowledge of Java language and web technology.**



*Frank Kim*

### AUTHOR STATEMENT

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

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • OnDemand • OnSite

# Secure Coding in .NET: Developing Defensible Applications

DEV544

***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 and 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.

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 uneasy relying solely on the security controls built into the ASP.NET framework? Secure Coding in ASP.NET will answer these questions and far more.

## Prerequisites

- **Experience with programming in ASP.NET using either Visual Basic or C#. All class work will be performed in C#.**
- **While this class briefly reviews basic web attacks, some prior understanding of issues such as XSS and SQL injection is recommended.**

## What You Will Learn

- Web Application Attacks
  - Cross-Site Scripting
  - Cross-Site Request Forgery (CSRF)
  - SQL Injection
  - HTTP Response Splitting
  - Parameter Manipulation
- Web Application Proxies
- Using Fiddler
- Code Access Security
- Assemblies
- Global Assembly Cache
- Execution Model
- Authentication
  - IIS / ASP.NET pluggable authentication architecture
  - Basic & Digest Authentication
  - .NET Form Based Authentication Framework
  - Windows Authentication
  - Authorization, OS security, and Impersonation
  - SSL Client Certificates
  - Authentication Policies
- NET Encryption Services
  - Encryption Principals
  - Securing communications
  - Protecting data at rest
- Strong and Weak Named Assemblies
- The Common Language Runtime
- Security Zones
- Evidence
- Code Groups
- Permissions
- Hacking .NET Security

*"Again SANS has managed to take incredibly complicated material and make it easy to understand."* -Marc Stoufer, Meijer

**Delivery Methods** *(Visit pages 46-47 for more details)*

Live Events • OnDemand • OnSite

**Four-Day Course**
**24 CPE/CMU Credits**
**Laptop Required**

### 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

**GIAC Certification**
www.giac.org

**STI Masters Program**
www.sans.edu

### Looking for a great software development resource?

**SANS Software Security Institute website (www.sans-ssi.org)** is a community-focused site offering AppSec professionals a one-stop resource to learn, discuss, and share current developments in the field. It also provides information regarding SANS AppSec 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 application security, developer, and IT security professionals.

AUD407

# Foundations of Auditing Information Systems

Six-Day Course
36 CPE/CMU Credits
Laptop Required

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

## 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

***This course is designed for security and assurance professionals, system administrators, 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 System scare 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 and the types of audits performed, 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**

*James Tarala*

## AUTHOR STATEMENT

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

**Delivery Methods** *(Visit pages 46-47 for more details)*
Live Events • OnSite

# Auditing Networks, Perimeters, and Systems

## AUD507

*CND Auditor for the Department of Defense Baseline Certification for 8570*

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

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise. What systems really matter? How should the firewall and routers be configured? What settings should be checked on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? All of these questions and more will be answered by the material covered in this course.

This course is organized specifically to provide a risk driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practice, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation will be given from real-world examples.

> *"This course allowed me to have hands-on experience with powerful tools and professional guidance all at the same time."*
>
> -Neal Francom, LDS Church

One of the struggles that IT auditors face today is assisting management to understand the relationship between the technical controls and the risks to the business that these affect. In this course these threats and vulnerabilities are explained based on validated information from real-world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organization to build an understanding of why these controls specifically and auditing in general is important. 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.

### AUTHOR STATEMENT

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. 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

**Six-Day Course**
**36 CPE/CMU Credits**
**Laptop Required**

### Who Should Attend

- Auditors seeking to identify key controls in IT systems
- Audit professionals looking for technical details on IT auditing
- Managers responsible for overseeing the work of an IT 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

**GIAC Certification**
www.giac.org

**STI Masters Program**
www.sans.edu

# Additional SANS Training Courses

## SIX-DAY SECURITY 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.

### SEC509 Securing Oracle

SANS recognizes the need for comprehensive Oracle security training to help organizations protect their most critical information resources. In this course, the student is lead through the process of auditing and securing Oracle by defining the risks to data, using auditing techniques for detecting unauthorized access attempts, using Oracle access controls and user management functions, and developing reliable backup and restore processes and techniques to secure the Oracle database, as well as applications.

### 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).

## TWO- & FOUR-DAY SECURITY COURSES

### SEC334 SANS Training for the CompTIA Security+ Cert

Prepare for the CompTIA Security+ Certification exam with SANS unparalleled training.

### SEC434 Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting

This first-ever dedicated log management class for IT and security managers will cover system, network, and security logs and that management at an organization. Students will learn to leverage logs for critical tasks related to incident response, forensics, and operational monitoring.

### SEC440 20 Critical Security Controls: Planning, Implementing, and Auditing

This course helps you master specific, proven techniques and tools needed to implement and audit the Top Twenty Most Critical Security Controls.

### 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.

### 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.

### 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.

## HALF- & ONE-DAY SECURITY 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.

### 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.

### SEC531 Windows Command-Line Kung Fu In-Depth for Info Sec Pros

Maximize your value in handling incidents, analyzing systems, conducting forensics analyses, and performing penetration tests. In this fun and engaging session, we'll discuss in depth one of the most powerful command-line tools built into Windows, wmic, and how it can greatly improve the capabilities of security personnel, incident handlers, and even auditors.

### 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.

### SEC556 Comprehensive Packet Analysis

This class will give you the skills necessary to decode network traffic with open-source tools available for Unix and Windows systems. Students will learn advance pcap packet filtering methods to decode and manipulate network traffic using tcpdump and use Wireshark to extract files (pictures, documents, executable, etc) from a data stream for malware recovery, incident response, and forensics analysis.

## FIVE-DAY DEVELOPER COURSE

### (ISC)$^2$® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program

The (ISC)$^2$ 5-day CSSLP CBK Education Program is the exclusive way to learn security best practices and industry standards for the software lifecycle – critical information to a CSSLP.

## TWO- & FOUR-DAY DEVELOPER COURSES

### DEV530 Essential Secure Coding in Java/JEE

This two-day version of DEV541 is intended to cover the essential Java/JEE topics that are relevant to a large number of web application developers and therefore does not cover all the material that may be present on the GSSP-Java certification exam. DEV541: Secure Coding in Java/JEE: Developing Defensible Applications is recommended for students who wish to pursue the GSSP-Java certification.

### DEV532 Essential Secure Coding in ASP.NET

During this two-day course we will analyze the defensive strategies and technical underpinnings of ASP.NET and learn where, as a developer, you can leverage defensive technologies in the framework and where you need to build security in by hand.

### 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. Coupled with the lectures, there are more than ten hands-on exercises where the students will have the opportunity to test out their new skills identifying flaws in code, fixing code, and writing secure code. All of the exercises are available in Perl, PHP, C/C++, Ruby, and Java.

## ONE-DAY DEVELOPER COURSE

### DEV304 Software Security Awareness

This awareness course discusses design and implementation of software applications to reduce the risk from hackers and attacks. The concept is to engineer software so that it continues to function correctly under malicious attack.

## ONE-DAY FORENSICS COURSE

### FOR526 Advanced Filesystem Recovery and Memory Forensics

This advanced course is perfect for the diligent student familiar with core forensic methodology and techniques. It 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.

## SIX-DAY MANAGEMENT COURSE

### MGT411 SANS 27000 Implementation & Management

The International Standards Organization (ISO) has recently revised what has become the de facto document for creating and maintaining a secure enterprise, today known as the ISO/IEC 27000 standard. 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.

## TWO- & FOUR- DAY MANAGEMENT COURSES

### MGT433 Securing the Human: Building and Deploying an Effective Security Awareness Program

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. In addition you will learn how to measure your program's impact with metrics you can use and show to senior management.

### 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. Students will learn techniques for how to perform risk assessments for new vulnerabilities, compliance violations, new IT projects, and how to qualify the current risk level for presentation to executive level management.

## ONE-DAY MANAGEMENT COURSES

### MGT305 Technical Communication & Presentation Skills for Security Professionals

This course is designed for every IT professional in your organization. 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.

### MGT421 SANS Leadership and Management Competencies

Leadership is a capability that must be learned and developed to better ensure organizational success. Our focus is purely leadership-centric; we are not security-centric or technology-centric with this training opportunity. We help an individual develop 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 and build leadership skills to enhance their organizational climate through team building to enhance the organizational mission through growth in productivity, workplace attitude/satisfaction, and staff and customer relationships.

### MGT432 Information Security for Business Executives

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. The additional reading is sent in advance as well as included in the workbooks.

### MGT438 How to Establish a Security Awareness Program

Security awareness is a never ending process. We must invest in teaching our users what to do and what not to do when using the Internet in order to achieve an acceptable level of risk. MGT438 includes certification in SEC351 and a license to teach SEC351 at your organization free for one year, with a reasonable site fee thereafter. This course is based on NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program."

## ONE- & TWO-DAY AUDIT COURSES

### AUD305 Technical Communication & Presentation Skills for Security Professionals

This course is designed for every IT professional in your organization. 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.

### AUD429 IT Security Audit Essentials Bootcamp

This hands-on bootcamp course will help you get started in the field of information technology and security auditing. This class is not a CISA prep course; instead, this course fills in all of the technical how-to blanks, giving you real-world hands-on audit practice for technologies currently in use.

### AUD440 20 Critical Security Controls: Planning, Implementing and Auditing

This course helps you master specific, proven techniques and tools needed to implement and audit the Top Twenty Most Critical Security Controls.

### AUD521 Meeting the Minimum: PCI/DSS 2.0: Becoming and Staying Compliant

The payment card industry has been working over the past several years to formalize a standard for security practices that are required for organizations who process or handle payment card transactions. The fruit of this labor is the Payment Card Industry Data Security Standard. This standard, which started life as the Visa Digital Dozen, is a set of focused comprehensive controls for managing the risks surrounding payment card transactions, particularly over the Internet. Of course, compliance validation is one of the requirements. This course was created to allow organizations to exercise due care by performing internal validations through a repeatable, objective process. While the course will cover all of the requirements of the standard, the primary focus is on the technical controls and how they can be measured.

***There are specialty courses not listed above that are available, see www.sans.org/specialty-courses for full listings.***

# SANS Training Formats

## SANS Training Events

SANS offers classes throughout the year in many major US cities as well as in Europe, Australia, Canada, Asia, India, and Dubai. These training events feature anywhere from one to over fifty classes at the same location. SANS events offer much more than just training – this is the place to network with other information security professionals, gain information on new vendor products, participate in onsite/online challenges and contests, and listen to world-class guest speakers. **www.sans.org/training/bylocation**

## Community SANS

***Bringing live SANS Training Events to Your Community***

The Community SANS format offers the most popular SANS courses in your local community in a small classroom setting; most courses have fewer than 25 students. The instructors are pulled from the best of our SANS Mentor program and are trained by top-rated SANS instructors like Eric Cole and Ed Skoudis. The course material is delivered over a six-day period, just like it is at a larger SANS event, and you receive all the same content, audio files, and other materials along with the opportunity to network with other security professionals and associations within your local Community. We provide continental breakfast and breaks to encourage networking among students and faculty.
**www.sans.org/community_sans**

## SANS Mentor and @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 can study in between sessions on their own and work with the Mentor during class to discuss material, answer questions and work on exercises and labs such as Capture the Flag.

Mentor @work classes also give you the flexibility of a Mentor course right at your workplace with a group as small as 4 students. These private classes allow students to apply their newfound knowledge directly to their workplace environment during the actual class session with the consultative help of the Mentor. **www.sans.org/mentor**

## SANS Onsite

***Your Location – Your Schedule***

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. For organizations that need to train a large number of professionals, the SANS OnSite program is hard to beat! **www.sans.org/onsite**

## SANS vLive!

***Live Virtual Training – SANS Top Instructors***

SANS vLive! delivers live instruction via the web using various Internet-based technologies. Streaming audio, instant messaging, online forums, and e-mail are all leveraged to make the student's online learning experience as fun and engaging as possible.
**www.sans.org/vlive**

## SANS Partnership Series

The SANS Partnership Series is an outreach program created to provide deeply discounted training to support constituencies (EDU, State & Local Government) that have:

- A clear impact on national security
- Large numbers of information security practitioners
- Budget constraints that limit access to necessary training

The secret to this successful program is cost reduction realized by delivering the courses to large classes (100 or more).
**www.sans.org/partnership**

## SANS OnDemand

***Online Security Training & Assessments***

When you want 'anytime, anywhere' access to SANS' high quality training, choose SANS OnDemand, our advanced, online delivery method. The program is designed to provide a convenient, comprehensive, and highly effective means for information security professionals to receive the same intensive, immersion training that SANS is known for. OnDemand students receive training from the same top-notch SANS instructors who teach at our live training events to bring the true SANS experience right to your home or office. Plus our integrated courseware, online assessments, hands-on exercises, and online mentor allow students to really grasp the material being taught!
**www.sans.org/ondemand**

## SelfStudy

***Self-Paced Independent Training***

For the motivated student who enjoys working independently, we offer the SANS SelfStudy program. Students receive SANS course books (and CDs when applicable) and online access to MP3 files of SANS' world-class instructors teaching the material. Study texts and listen to the lectures at your own convenience and pace! In addition, students who register for GIAC Certification will receive TWO free GIAC practice tests. These practice tests show the student what to expect on the GIAC examination. Since many students may have been out of school for a long time, practicing test taking skills can improve their chances of passing the GIAC exams. **www.sans.org/selfstudy**

## SANS WhatWorks Summit Series

***Your IT Security Connection***

The SANS What Works Summits play an important role in educating security professionals in all types of positions on the latest trends, techniques and best practices to help you do your job more efficiently. The two-day format gives you full access to a series of one-hour discussions and panel dialogues with world class experts who will help you to improve your enterprise's security practices. The Summit also provides attendees with a unique opportunity to see leading vendors in a one-on-one environment which allows them to research options and learn cutting edge solutions they can implement immediately upon returning to their job. Attend a SANS Summit event today and you'll return equipped with solid techniques and solutions that will enable you to remain ahead of the competition.
**www.sans.org/summit**

## Community SANS

***Community SANS brings live SANS training to your local community.***

***Community SANS is SANS in your community!***

That's right – live training, live instructor, and live people from your own community. Your experience includes a top-notch SANS instructor, trained by people like Ed Skoudis, Dr. Eric Cole, or Rob Lee. Our small class setting gives you the added benefit of interacting and networking with your professional peers over a six day period. Most classes are offered in Bootcamp style to ensure you get the hands-on immersion experience SANS' students ask for.

Imagine the convenience and savings when you attend some of SANS' most popular courses without having to travel! You can then earn your GIAC certification right where you are – Dallas, Seattle, New York, Chicago, Pensacola, Sacramento, Boulder, Long Beach, Saint Louis, Albuquerque, Honolulu, Vancouver, Toronto, Ottawa, San Diego, Boston, Herndon, Portland, Columbus, San Antonio, New Jersey, Atlanta, Birmingham, Oklahoma City, Raleigh, San Jose, Indianapolis, and more. Check out our full schedule and locations at **www.sans.org/community**.

Want to bring SANS live training events to your community? Contact **community@sans.org**.

## Mentor SANS

***Intimate Live Instruction***

**SANS Mentor** multi-week sessions gives you time to absorb and master the same material commonly taught at SANS six-day conferences, with the guidance of a trained network security professional, right in your home town. Your mentor is highly qualified to help you learn and certify.

Mentor is your opportunity to participate in SANS training without the expense and inconvenience of travel or taking time out of the workday in a small classroom setting. You also get the opportunity to network with other security professionals in your area. Sign up today! **www.sans.org/mentor**

COMING SOON!

# SANS @Night

*SANS @Night is a series of talks given by top industry leaders to help compliment your infosec training experience.*

When you attend a SANS event, you not only get the best security training available, you also have the opportunity to absorb even more cutting-edge infosec knowledge from SANS instructors and subject matter experts through the **SANS @Night** talk series. All students who register and pay for a long course at any SANS training event WILL have free and unlimited live and online access to most evening talks for four months.

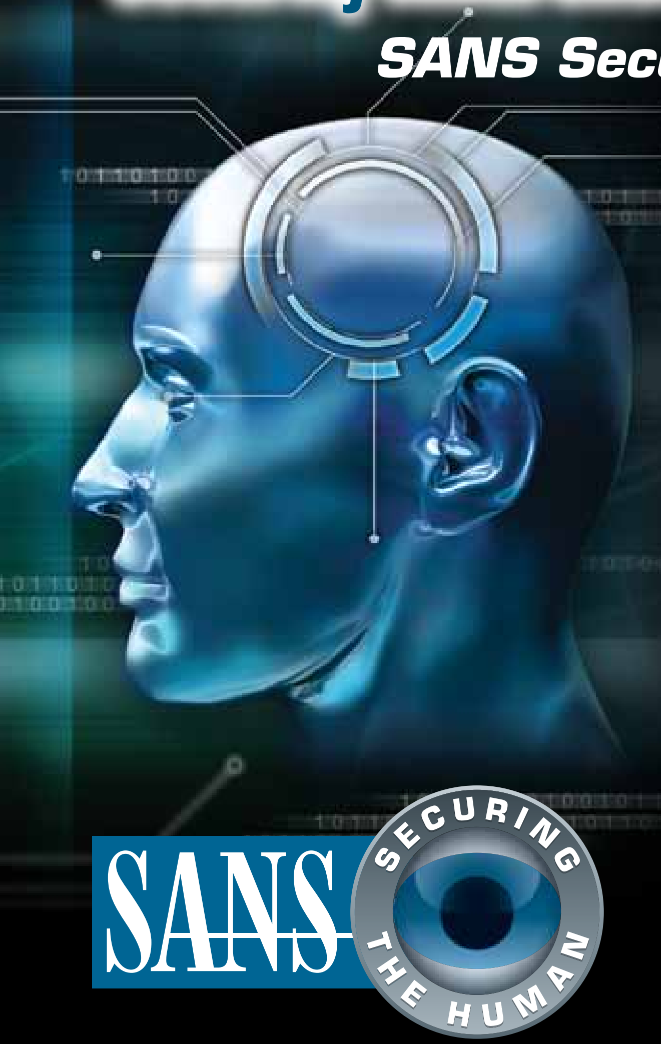
## Not Able to Attend an Event?

Coming soon, you will be able to participate in the **SANS @Night** talks, even if you cannot take advantage of our rigorous security training at conference. You will have unlimited access to **SANS @Night** talks, as well as have an opportunity to virtually mingle with thought leaders and network with fellow security professionals. You will also receive online access to the recorded talks for four months.

To register and see a list of available talks, go to
**www.sans.org/night**

# Security Awareness for the 21st Century

## *SANS Securing The Human*



The SANS Securing The Human Program addresses everything your organization needs to secure your employees, contractors, IT staff, and management. Our approach is to firstly motivate your employees by demonstrating who is targeting them, show them how they are being attacked, and explain why. Personalizing the training teaches your employees how to protect both themselves, their families and your organization. This has been demonstrated to ensure highest understanding and adoption.

We break your Awareness Training program into training modules. Each module focuses on a specific topic and has its own unique set of resources, including; video training, posters, newsletters and screensavers. Each module also has its own distinctive images, ensuring that the different materials for each module share the same look and feel, thereby reinforcing the same key message. The program can also be customized for the unique policies and requirements of your organization, including translation into multiple languages.

***For more information or to demo the training***

| | |
|---|---|
| info@securingthehuman.org | US +1 646 257 5875 |
| www.securingthehuman.org | UK +44 779 257 9875 |

SANS
Simulcast
*Powered by vLive!*

SANS Simulcast is designed to provide live training to teams of 20 or more, regardless of location, by combining webcast technology with live classroom instruction. If you have multiple people in multiple locations, and you want to experience live instruction from SANS' top instructors, then SANS Simulcast is the solution.

*"This is the first web-based training course I have done and was wondering if it would actually be worthwhile. It surpassed my expectations! The software and technology worked really well, the presenter kept everything moving along nicely and was quick to pick up on participants' comments during the lecture segments. The IM component adds value – lots of good information/comments from the class."*
-Jeremy Gay, Montana State University

## How SANS Simulcast Works

Cutting-edge webcast technology and live instruction combine to deliver a fun and engaging remote learning experience. All students, whether they attend live or remotely, will also receive six-months' access to an archived copy of the class to use as a reference tool or to catch up on a missed session.

The platform is web-based so students simply need a solid internet connection to participate.

A SANS instructor can teach the course from your facility or from one of our virtual classrooms.

- Remote students can log in as individuals or arrange for groups to meet in remote classrooms.
- Remote classrooms can also be staffed by a SANS facilitator.

## Schedule a SANS Simulcast

- To set up a Simulcast session or to inquire into setting up a "Remote Host Site" for an existing Simulcast event, please contact the SANS Simulcast team at simulcast@sans.org.
- Private group sessions can be added with as few as 20 students. Some open Simulcast sessions can be attended by single registrants. To learn more, please contact us today at simulcast@sans.org.

## Add the SANS Simulcast Feature to an Existing SANS OnSite Class

SANS Simulcast can be added to any existing SANS OnSite with as few as 5 remote students, just contact your account representative or send an e-mail to onsite@sans.org to find out more.

SANS OnDemand + SANS vLIVE!

- A 12-month Online Training Pass for groups or individuals, valid for OnDemand and vLive! training
- Learn on your own schedule – anytime, anywhere
- Save 100% of your travel budget
- Save up to 40% on the cost of training

> *"Hands down, SANS OnDemand is the best training money can buy! With budget cuts taking place in all organizations – big and small – SANS OnDemand provides a cost effective approach for a company to get their employees trained at a fraction of the cost of traditional classroom training."* -Matt Austin, Symantec Corporation

## GROUP FLEX PASS OPTIONS

Allows companies the flexibility to purchase a deeply discounted 12-month online training pass consisting of multiple courses which can be used among employees, at the convenience of the company and employees.

| Options | Allows you to take... | Training Value | Discount | Cost |
|---|---|---|---|---|
| #1 Group Flex Pass+ | 50 job-based (long) courses | $178,750 | Save 35% | $116,187 |
| #2 Group Flex Pass+ | 25 job-based (long) and 25 skill-based (short) courses | $89,375 | Save 25% | $67,031 |
| #3 Group Flex Pass+ | 10 job-based (long) courses | $35,750 | Save 20% | $30,387 |

## INDIVIDUAL FLEX PASS OPTIONS

Allows individuals to stock up on SANS training with the best discounts available! Our individual flex passes are designed for those who have the desire to flex their brain and training dollars with continuous training throughout the year.

| Options | Allows you to take... | Training Value | Discount | Cost |
|---|---|---|---|---|
| #1 Group Flex Pass+ | 4 job-based (long) and 4 skill-based (short) courses | $20,280 | Save 25% | $15,210 |
| #2 Group Flex Pass+ | 4 job-based (long) courses | $14,300 | Save 20% | $11,440 |
| #3 Group Flex Pass+ | 4 skill-based (short) courses | $5,980 | Save 10% | $5,382 |

## CUSTOM FLEX PASS OPTIONS

Write to us at flexpass@sans.org for a customized Flex Pass+ that will meet the training needs of your organization. We have account managers available to work with you to fulfill your needs.

*Prices subject to change. Please check www.sans.org/security-training/flexpass/index.php for current pricing.*

WEB www.sans.org/ondemand/flexpass.php

E-MAIL flexpass@sans.org PHONE (301) 654-7267 (Mon-Fri, 9am-8pm EST)

SANS

# Voucher Program

***"Maximize your Training Budget! Extend your Fiscal Year"***

## SANS Voucher Credit - Overview

SANS offers a Voucher Credit program that pays you for choosing SANS for your information security training needs. It is simply a prepayment program that rewards you with additional voucher credits deposited into your credit account. You can use your credits to pay for SANS training services of your choice. It is like purchasing a gift card, only with SANS, we give you additional money to spend!

SANS Voucher Credits are a great solution for flexibility, cost savings, and value. It is perfect when you know that you will have a variety of IT security training needs in the next 12 months, but have not decided who you will train, what delivery format to use, or when to do it. Voucher Credits are also perfect when you have discretionary training funds to spend for long-term professional development.

SANS Voucher Credits can be redeemed for any of the following:

- SANS Public Training Events (SANSFIRE, Network Security, etc)
- SANS OnSite (Private Classes)
- SANS vLive!
- Community SANS
- SANS OnDemand
- SANS Mentor
- SelfStudy
- GIAC Exams & Practice Exams

*The SANS discount program that pays you credits and delivers flexibility*

## SANS Voucher Credit - Benefits

***Valid for live classroom training, online learning, and GIAC certification***

- Cost savings (expand your training budget)
- Flexibility (extend your fiscal year)
- Free Learning Management Tool (online enrollment and usage reports)
- Real-time access to GIAC Certification results & OnDemand usage
- Fully transferable
- One procurement
- Perfect for year-end budgets
- Great way to motivate and retain your valued employees
- Security of knowing that you will get information security training from the best source

## SANS Voucher Credit - How to Create an Account

1. Designate a point of contact (POC) that will have the responsibility of allocating funds from your Voucher Credit account.
2. Decide how much money to deposit into your Voucher Credit account.
3. Submit the "SANS Order Survey Form" online.
4. After payment has been received, SANS will provide the POC with a receipt, voucher certificate, and instructions on how to use your Voucher Credit account.

WEB **www.sans.org/vouchers**

E-MAIL **vouchers@sans.org** PHONE **(301) 654-7267** (Mon-Fri, 9am-8pm EST)

# Real Threats, Real Skills, Real Success

*The SANS Cyber Guardian program is a unique opportunity for information security individuals or organizational teams to develop specialized skills in incident handling, perimeter protection, forensics, and penetration testing.*

## How the Program Works

This program begins with hands-on core courses that will build and increase your knowledge and skills with each course. These skills will be reinforced by taking and passing the associated GIAC certification exam. After completing the core courses, you will choose a course and certification from either the Red or Blue Team. The program concludes with participants taking and passing the GIAC Security Expert (GSE) certification.

Contact us at onsite@sans.org to get started!

## Program Prerequisites

- Five years of industry-related experience
- A GSEC certification (with a score of 80 or above)

or

- A CISSP certification

### *Core Courses*

| | |
|---|---|
| SEC503 | Intrusion Detection In-Depth (GCIA) |
| SEC504 | Hacker Techniques, Exploits, and Incident Handling *(GCIH)* |
| SEC560 | Network Penetration Testing and Ethical Hacking *(GPEN)* |
| FOR508 | Advanced Computer Forensic Analysis and Incident Response *(GCFA)* |

*After completing the core courses, students must choose one course and certification from either the Blue or Red Team*

### *Blue Team Courses*

| | |
|---|---|
| SEC502 | Perimeter Protection In-Depth *(GCFW)* |
| SEC505 | Securing Windows *(GCWN)* |
| SEC506 | Securing Linux/Unix *(GCUX)* |

### *Red Team Courses*

| | |
|---|---|
| SEC542 | Web App Penetration Testing and Ethical Hacking *(GWAPT)* |
| SEC617 | Wireless Ethical Hacking, Penetration Testing, and Defenses *(GAWN)* |
| SEC660 | Advanced Penetration Testing, Exploits, and Ethical Hacking<br>*(Written Assignment – White Paper)* |

*Become a SANS Cyber Guardian and stay one step ahead of the threats as well as know what to do when a breach occurs.*

*Learn more about the SANS Cyber Guardian Program at*
**www.sans.org/cyber-guardian**

# Future SANS Events Schedule

## SANS AppSec 2011: Summit & Training

San Francisco, CA • March 7-14, 2011

www.sans.org/appsec-2011

## SANS 2011

Orlando, FL • March 26 - April 4, 2011

www.sans.org/sans-2011

## SANS Northern Virginia 2011

Reston , VA • April 15-23, 2011

www.sans.org/northern-virginia-2011

## SANS Security West 2011

San Diego, CA • May 3-12, 2011

www.sans.org/security-west-2011

## SANS Cyber Guardian 2011

Baltimore, MD • May 15-22, 2011

www.sans.org/cyber-guardian-2011

*WhatWorks in*

## Forensics & Incident Response Summit 2011

Austin, TX • June 7-14, 2011

www.sans.org/forensics-incident-response-summit-2011

## SANS Rocky Mountain 2011

Denver, CO • June 23-30, 2011

www.sans.org/rocky-mountain-2011

*WhatWorks in*

## Security Impact of IPv6 Summit 2011

Washington, DC • July 14-15, 2011

www.sans.org/ipv6-summit-2011

For a full list of training events, please visit **www.sans.org.** *Dates and locations are subject to change.*

# Future SANS Events Schedule

## SANSFIRE 2011

Washington, DC • July 15-24, 2011
www.sans.org/sansfire-2011

## SANS Ottawa 2011

Ottawa, ON • August 28 - September 2, 2011
www.sans.org/ottawa-2011

## SANS Boston 2011

Boston, MA • August 8-13, 2011
www.sans.org/boston-2011

## SANS Virginia Beach 2011

Virginia Beach, VA • August 22 - September 2, 2011
www.sans.org/virginia-beach-2011

## SANS Network Security 2011

Las Vegas, NV • September 18-26, 2011
www.sans.org/network-security-2011

## SANS Forensics 2011

Baltimore, MD • October 9-14, 2011
www.sans.org/forensics-2011

## SANS Seattle 2011

Seattle, WA • November 2-7, 2011
www.sans.org/seattle-2011

## SANS Cyber Defense Initiative 2011

Washington, DC • December 6-16, 2011
www.sans.org/cyber-defense-initiative-2011

**For a full list of training events, please visit www.sans.org.** *Dates and locations are subject to change.*

SANS
8120 Woodmont Avenue
Suite 205
Bethesda, MD 20814

PROMO CODE

**CC11**

**Please enter your Promo Code when registering.**

## Setting the Standard for Security Training

SANS

***SANS is the most trusted and by far the largest source for information 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! See inside for details.

***Save up to $400 by registering early!***

**Check www.sans.org for information for all events**

### 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!"***