SANS CyberCon 2012

Virtual Conference

Intense courses. Top instructors. No travel.

SANS' first-ever 100% VIRTUAL training event!

October 8-13, 2012

Four of our top courses being offered:

SEC504:

Hacker Techniques, Exploits, and Incident Handling

Instructors: Ed Skoudis and John Strand

SEC542:

Web App Penetration Testing and Ethical Hacking

Instructor: Kevin Johnson

FOR408:

Computer Forensic Investigations – Windows In-Depth

Instructor: Ovie Carroll

MGT414:

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

Instructor: Dr. Eric Cole

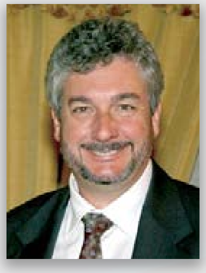
> *"I was surprised how much I liked this format, (live virtual delivery) since I have attended other SANS classes in person. I was skeptical, but I loved it."*
>
> -Jon Truan, Oak Ridge National Laboratory

Register at
www.sans.org/cybercon-2012

SANS

The Most Trusted Source
for Information and
Software Security Training

Dear Colleague,



Stephen Northcutt

For several years SANS has been perfecting the ability to deliver world-class training LIVE over the internet, and we are now ready to unveil SANS' first live online training event: SANS CyberCon 2012! SANS CyberCon 2012 will be your chance to experience a SANS training event without ever leaving home.

At SANS CyberCon 2012, you will learn directly from the top practitioners in the industry. SANS CyberCon 2012 will include a kick-off keynote address from Dr. Eric Cole, lunch talks, evening presentations, and other special touches that make a SANS Training Event so special.

All courses will meet live in virtual classrooms and will be fully interactive. You will receive the live conference benefits at the location of your choice. How is this different from SANS' other online training? Here's what is included:

- **The ability to ask questions, network with classmates, and master new skills!**
- **You will receive the same materials and complete the same labs and exercises as all other SANS students.**
- **You will also receive four months' access to an online archive of your class at no extra charge. These recordings of your class will allow you to review your class later if you need to step out or if you want to reinforce a challenging concept.**
- **The lunch and evening presentations will also be available in the online archives for four months.**

When you attend SANS CyberCon 2012, you will see the SANS promise in action – what you learn in the classroom you will able to use immediately upon returning to the office.

With a reputation for being the most trusted source for information security training, SANS is the best choice for your IT security education. Let your colleagues and friends know about SANS CyberCon 2012. We look forward to seeing you there!

Kind regards,

Stephen Northcutt
President
SANS Technology Institute, a postgraduate computer security college

Courses At A Glance

		MON 10/8	TUE 10/9	WED 10/10	THU 10/11	FRI 10/12	SAT 10/13
SEC504	Hacker Techniques, Exploits, and Incident Handling	PAGE 6					
SEC542	Web App Penetration Testing and Ethical Hacking	PAGE 7					
FOR408	Computer Forensic Investigations – Windows In-Depth	PAGE 8					
MGT414	SANS® +S™ Training Program for the CISSP® Certification Exam	PAGE 9					

Get the Most Out of Training

Avoid interruptions.

Schedule your training time, and let your boss and co-workers know that you are focusing on the course.

Plan where to attend.

Find a place that is free from distractions and has a strong internet connection.

Communicate.

Remember that your course is a live virtual environment and is fully interactive. Make sure to ask questions and network with your classmates.

Don't miss the bonus sessions.

The course and SANS@Night will be archived and available to you for four months following the conference. These recordings will allow you to review your class later if you need to step out or if you want to reinforce a challenging concept.

"The quality of the tool used for managing the online course has been rock solid in terms of both stability and performance. The tool is very user friendly."

-Kenneth Lowry, Northrop Grumman

How Are You Protecting Your

- Data
- Network
- Systems
- Critical Infrastructure

Risk management is a top priority. The security of these assets depends on the skills and knowledge of your security team. Don’t take chances with a one-size fits all security certification.
Get GIAC certified!

GIAC offers over 20 specialized certifications in security, forensics, penetration testing, web application security, audit and management.

GIAC Certification opportunities being offered at this event:

CERT	CERT DESCRIPTION	SANS COURSE
GISP	Information Security Professional	MGT414
GCIH	Certified Incident Handler	SEC504
GWAPT	Web Application Penetration Tester	SEC542
GCFE	Certified Forensic Examiner	FOR408

> *“GIAC is the only certification that proves you have hands-on technical skills.”*
>
> -Christina Ford, Department of Commerce

Learn more about
GIAC and how to
Get Certified at
www.giac.org

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

DoD 8570 Required Certifications

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!

DoD Baseline IA Certifications

TECH II: GSEC

TECH III: GCIH • GCED • CISSP • CISA

MGT I: GSLC • GISF

MGT II: GSLC • CISSP

MGT III: GSLC • CISSP

Computer Environment (CE) Certifications

SEC505: GCWN

SEC506: GCUX

Information Assurance System Architecture & Engineering (IASAE) Certifications

IASAE I: CISSP

IASAE II: CISSP

Computer Network Defense (CND) Certifications

CND Analyst: GCIA • GCIH

CND Incident Responder: GCIH

CND Auditor: GSNA • CISA

Training for Certifications

GSNA:	AUD507:	Auditing Networks, Perimeters, and Systems
CISSP:	MGT414:	SANS® +S™ Training Program for the CISSP® Certification Exam
GSLC:	MGT512:	SANS Security Leadership Essentials For Managers with Knowledge Compression™
GISF:	SEC301:	Intro to Information Security
GSEC:	SEC401:	SANS Security Essentials Bootcamp Style
GCIA:	SEC503:	Intrusion Detection In-Depth
GCIH:	SEC504:	Hacker Techniques, Exploits, and Incident Handling

"As our C4 systems become netcentric and more linked with our weapons systems, it is essential that our IA workforce be up to the task of securing our networks. I am proud to be on the cyber defense line with such a competent industry partner that understands the needs of the defense department and is willing to work with us to help accomplish this difficult task."

-Mike Knight, Naval NetWar Command

SANS @Night Evening Talks

Enrich your SANS training experience! Evening talks given by our instructors and selected subject matter experts help you broaden your knowledge, get the most for your training dollar, and hear from the voices that matter in computer security.

Everything They Told Me About Security Was Wrong

John Strand

If you were to believe the vendors and the trade shows, you would think everything was "OK" with IT security. You would think AV works. You would think "plug and play" IDS was effective. You would think that Data Loss Prevention would prevent data loss. Why, then, is it that very large organizations are still getting compromised? Organizations with very large budgets and staff still get compromised in advanced and persistent ways. Something is very wrong in this industry.

Let's find out what is wrong and how we can fix it.

In this presentation we will cover many of the common misconceptions about computer security. A few misconceptions we will destroy with harsh words and live demos are:

- AV will keep malware off my system
- Firewalls will keep the attackers out
- If my system is patched, I cannot be hacked
- Apple computers are far safer than Windows
- Linux is more secure than Windows
- My users are dumb

In this presentation we will have multiple live demonstrations including: hacking a Mac, and hacking a Linux system and bypassing AV. However, the most important thing about this presentation is that we will cover how we need to change our defensive mindset.

After all, if information security was easy it would not take six days to cover the essentials.

Ninja Assessments: Stealth Security Testing for Organizations *Kevin Johnson*

Organizations today need to be able to easily integrate security testing within their existing processes. In this talk, Kevin Johnson of Secure Ideas will explore various techniques and tools to help organizations assess the security of the web applications. These techniques are designed to be implemented easily and with little impact on the work load of the staff.

For dates, times, and complete information, please visit www.sans.org/cybercon-2012/night.php

Vendor-Sponsored Sessions by:

QUALYS®

TENABLE Network Security®

Infogressive, Inc. *Aggressive* Information Security

Security 504

Hacker Techniques, Exploits & Incident Handling

Six-Day Program • Mon, Oct 8 - Sat, Oct 13
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Ed Skoudis & John Strand

If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth.

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

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.

What Students Are Saying

"This course will open your eyes wider than you thought they could open. Great class."
-Migeul Escobedo, USMC

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 track, they know they'll be ready when a bad guy launches an attack against their systems. And being ready to thwart the bad guys is what it's all about. -Ed Skoudis

Who Should Attend:

- Incident handlers
- Leaders of incident handling teams
- Penetration Testers
- Ethical Hackers
- 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

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cybercon-2012/event.php.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

Security 542

Web App Penetration Testing and Ethical Hacking

Six-Day Program • Mon, Oct 8 - Sat, Oct 13
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Kevin Johnson

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 Web sites 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.

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

Who Should Attend:

- **General security practitioners**
- **Penetration testers**
- **Ethical hackers**
- **Web application vulnerability assessors**
- **Website designers and architects**
- **Developers**

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cybercon-2012/event.php.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

Kevin Johnson *SANS Senior Instructor*

Kevin Johnson is a security consultant and founder of Secure Ideas. Kevin came to security from a development and system administration background. He has many years of experience performing security services for fortune 100 companies, and in his spare time he contributes to a large number of open source security projects. Kevin's involvement in open-source projects is spread across a number of projects and efforts. He is the founder of many different projects and has worked on others. He founded BASE, which is a Web front-end for Snort analysis. He also founded and continues to lead the SamuraiWTF live DVD. This is a live environment focused on Web penetration testing. He also founded Yokoso! and Laudanum, which are focused on exploit delivery. Kevin is a certified instructor for SANS and the author of Security 542: Web Application Penetration Testing and Ethical Hacking. He also presents at industry events, including DEFCON and ShmooCon, and for various organizations, like Infragard, ISACA, ISSA, and the University of Florida.

Forensics 408

Computer Forensic Investigations – Windows In-Depth

Six-Day Program • Mon, Oct 8 - Sat, Oct 13
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Ovie Carroll

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

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

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

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

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

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

Ovie Carroll *SANS Certified Instructor*

Ovie Carroll has over 20 years of federal law enforcement experience. Ovie was a special agent for the Air Force Office of Special Investigations (AFOSI) and Chief of the Washington Field Office Computer Investigations and Operations Branch responsible for investigating all national level computer intrusions into USAF computer systems. Following his career with the AFOSI he was the Special Agent in Charge of the Postal Inspector General's computer crimes unit where he was responsible for all computer intrusion investigations and for providing all computer forensic analysis in support of USPS-OIG investigations. Ovie is currently the Director for the Cybercrime Lab at the Department of Justice, Computer Crime and Intellectual Property Section (CCIPS) and an adjunct professor at George Washington University teaching computer crime investigations. In addition to his career fighting computer crime, Ovie has conducted investigations into a variety of offenses including murder, fraud, bribery, theft, gangs and narcotics.

Who Should Attend:

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

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cybercon-2012/event.php.

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

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Management 414

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

Six-Day Program • Mon, Oct 8 - Sat, Oct 13
9:00am - 7:00pm (Day 1) • 8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6) • 46 CPE/CMU Credits
Laptop NOT Required • Instructor: Dr. Eric Cole

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**

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

Who Should Attend:

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

Obtaining your CISSP® certification consists of:

- **Fulfilling minimum requirements for professional work experience**
- **Completing the Candidate Agreement**
- **Review of Resume**
- **Passing the CISSP® 250 multiple-choice question exam with a scaled score of 700 points or greater**
- **Submitting a properly completed and executed Endorsement Form**
- **Period Audit of CPEs to maintain the credential**

Bootcamp

This program has extended hours.

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

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

Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Dr. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. Dr. Cole has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. Dr. Cole is the author of several books, including *Hackers Beware, Hiding in Plain Site, Network Security Bible*, and *Insider Threat*. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is founder of Secure Anchor Consulting in which he provides state of the art security services and expert witness work. He also served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is actively involved with the SANS Technology Institute (STI) and SANS working with students, teaching, and maintaining and developing courseware. He is a SANS faculty Fellow and course author.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cybercon-2012/event.php.

GIAC INFORMATION SECURITY PROFESSIONAL GISP

GIAC Certification
www.giac.org

What's Your Next Career Move?

The information security field is growing and maturing rapidly; are you positioned to win? A Master's Degree in Information Security from the SANS Technology Institute will help you build knowledge and skills in management or technical engineering.

STI Offers Two Master's Degree Programs:

Master of Science in Information Security Engineering

Master of Science in Information Security Management

> *"The STI program prepares me in both technical aptitude and leadership skills. The instructors have extensive real-world experience - you walk out of every class with skills you can use immediately.“*
>
> -Courtney Imbert, MSISE Student

Three of the courses being offered at CyberCon may be applied towards and STI Master's Degree.

SANS Technology Institute
Knowledge for Peace
Scientia Pro Pace

www.sans.edu

info@sans.edu

720.941.4932

SANS CYBER GUARDIAN PROGRAM

www.sans.org/cyber-guardian

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

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!

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 (GXPN)

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

SANS Training Options

Training

Training Events

www.sans.org/security-training/bylocation/index_all.php

Community

Community

Community SANS

www.sans.org/community

OnSite

OnSite

Live Training at Your Location

www.sans.org/onsite

Mentor

Mentor

Intimate Live Instruction

www.sans.org/mentor

Summit

Summit Series

Live IT Security Summits and Training

www.sans.org/summit

OnDemand

OnDemand

All the Course Content at Your Own Pace

www.sans.org/ondemand

vLive

vLive

Virtual Live Training from Your Home or Office

www.sans.org/virtual-training/vlive

Simulcast

Simulcast

Attend Event Training From Your Location

www.sans.org/virtual-training/event-simulcast
www.sans.org/virtual-training/custom-simulcast

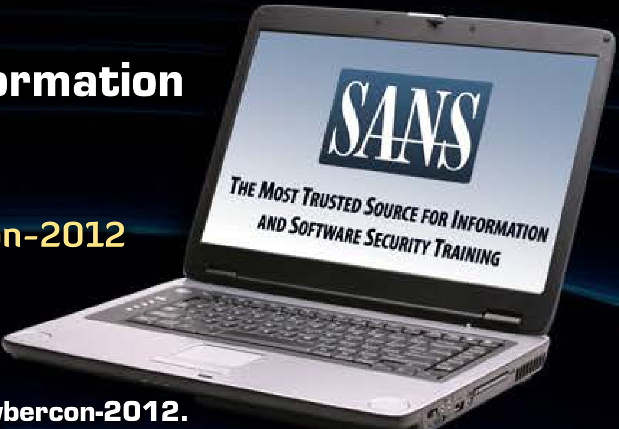
SelfStudy

SelfStudy

Independent Study with Books and MP3s

www.sans.org/selfstudy

Registration Information


SANS
The Most Trusted Source for Information
and Software Security Training

Register online at
www.sans.org/cybercon-2012

How to Register

1. Go to www.sans.org/cybercon-2012.
Select your course or courses and indicate whether you plan to test for GIAC certification. If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. We do not take registrations by phone.

2. Provide payment information.
Even if you do not want to submit your payment information online, still complete the online form! There is an option to submit credit card information for payment by fax or phone once the online form is completed and you have your invoice number. SANS ACCEPTS ONLY US and CANADIAN FEDERAL GOVERNMENT PURCHASE ORDERS

If you normally use a PO and are not part of the federal government, please see our additional PO information on the tuition information page: www.sans.org/cybercon-2012/tuition.php

3. Print your invoice.
If you need one, you must print YOUR OWN INVOICE at the end of the online registration process. The invoice will pop up automatically when the registration is successfully submitted. You may also access your invoice at https://portal.sans.org/history.

4. E-mail confirmation will arrive soon after you register.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	8/22/12	$500.00	9/5/12	$250.00

Some restrictions apply.

Group Savings (Applies to tuition only)

15% discount if 12 or more people from the same organization register at the same time
10% discount if 8 - 11 people from the same organization register at the same time
5% discount if 4 - 7 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at www.sans.org/security-training/discounts.php prior to registering.

Cancellation

You may subsitute another person in your place at any time by sending an e-mail request to registration@sans.org or a fax request to 301-951-0140. There is a $300 cancellation fee per registration. Cancellation requests must be received by Wednesday, September 19, 2012, by fax or mail-in order to receive a refund.

Scan the QR code to register by August 22nd and **SAVE $500** on CyberCon courses.

www.sans.org/info/106714

To download a free QR reader
www.mobile-barcodes.com/qr-code-software

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

PROMO CODE

HOU

Register using this Promo Code

Save $500 when you register by August 22nd
www.sans.org/cybercon-2012

To be removed from future mailings, please contact unsubscribe@sans.org or (301) 654-SANS (7267). Please include name and complete address.