SANS

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

ONLINE TRAINING

2013 Course Catalog

OnDemand

vLive

Best-in-Class Courses

Choose from more than 30 courses in:

- IT Security
- Security Management
- Incident Handling
- Computer Forensics
- Penetration Testing
- Software Security
- IT Security Audit
- Legal Issues

The SANS Advantage

- No travel required
- Hyper-current content
- World-class instructors
- Learn it today and apply it tomorrow

Different learning styles. Different learning platforms.

OnDemand • vLive

Simulcast • SelfStudy

Visit

www.sans.org/online-security-training/specials

for current

Online Training specials.

Stephen Northcutt

Dear Colleague,

One thing that SANS understands better than anyone else (aside from what security professionals need to know to excel in their jobs) is that **every person learns differently**. Some people learn best by listening, and others learn best by doing. Some prefer long stretches of class time, and others need short but more frequent sessions. Some value the interactivity of web-based technologies while others prefer the independence of course books.

SANS online training was created with different learning modalities to meet as many student needs as possible. Whatever your personal learning needs, we have an online training platform that meets them. Not sure what each platform entails? Check out pages 2 through 8 for an overview of our four online training options.

As always, **every one of our online courses is developed and taught by SANS' world-class instructors** who represent the top information security professionals working today – from forensics expert Rob Lee to internationally-recognized penetration tester Ed Skoudis. As a result, all of our course content is grounded in industry experience, so everything you learn in class will be applicable – immediately – to your job.

As an information security professional, **you need an arsenal of tools and strategies to stay ahead of cyber threats.** By choosing SANS online training, you'll not only expand your arsenal but also improve its effectiveness. We hope for the best for you in your educational pursuits, and we thank you for choosing SANS.

Best regards,

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

"OnDemand is excellent. I'm able to learn the material as if I were in a classroom, but I'm able to split up and take the training to accommodate my schedule."
-Justin Kear, Lockheed Martin

"The OnDemand training allows a student to go over material multiple times. Taking OnDemand classes provides great flexibility to learn and still maintain one's daily work obligations."
-Evans V. Roberts Jr., AT&T Mobility

"Outstanding, as always, SANS courses offer the best training because they always base the training on real-world scenarios."
-Eric Garcia, U.S. Navy

"I really liked the vLive format; I had flexibilty to attend from home, while on travel, or while stuck late at work. I can replay sessions to review content or get what I missed in class."
-Norman Reese, Honeywell

Table of Contents

OnDemand

Online Training & Quizzes
Anytime, Anywhere

If you're a self-motivated learner whose schedule changes often, then SANS OnDemand is the right learning platform for you. Choose from more than 25 courses, and take them whenever and wherever you want. Each course gives you four months of access to our OnDemand computer-based training platform, which includes a mix of presentation slides, video demonstrations, and quizzes supported with audio of SANS' top instructors teaching the material.

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

"This is the first OnDemand course I have taken from SANS, and I was extremely impressed with not only the content, but the presentation methods and tools used for the training. I would recommend this type of training to my colleagues."

-Robert Delancy, Juniper Networks

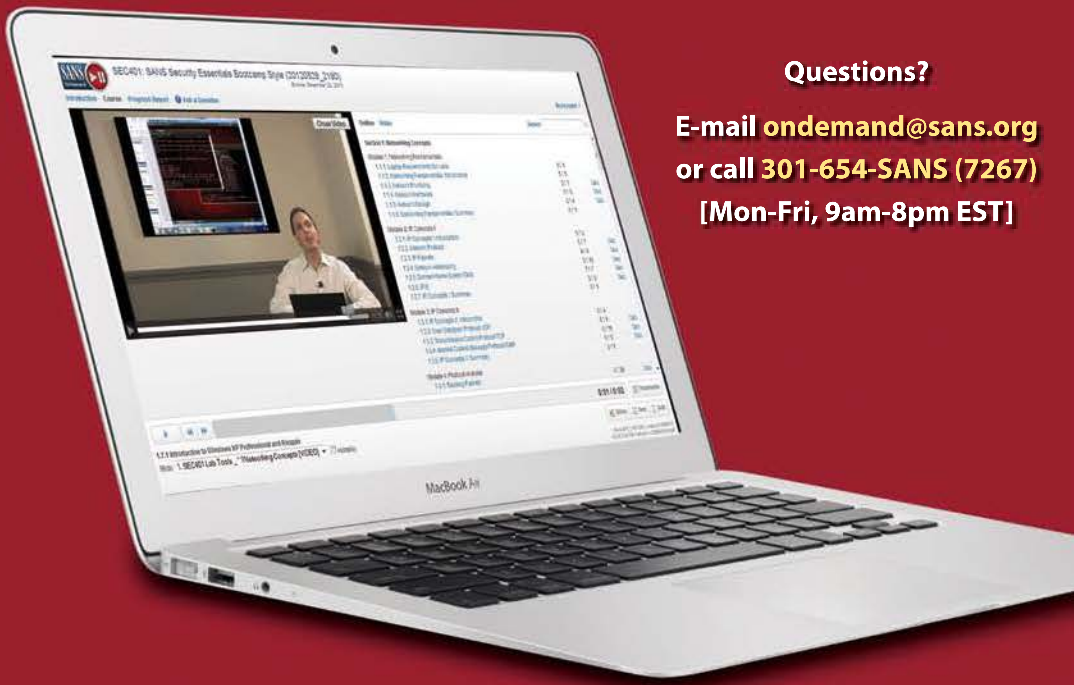
"The OnDemand system is an ideal medium for security training for professionals with rigorous work schedules requiring flexible training solutions."

-Charles Brown III

www.sans.org/ondemand

Reasons to Take SANS OnDemand

- Four months of access to comprehensive online training and quizzes
- Web-based training accessible 24/7 from your desktop, laptop, iPad, or Android Tablet
- Taught by SANS' Top Gun instructors including Dr. Eric Cole, Kevin Johnson, Rob Lee, and Ed Skoudis
- No travel or time away from the office
- Includes video labs and hands-on exercises
- Access to highly-qualified Virtual Mentors
- Complete set of course books and hands-on CDs
- Course Progress Reports
- Over 30 courses available – anytime, anywhere
- Supplemental preparation tool for the GIAC exams



Questions?

E-mail ondemand@sans.org
or call 301-654-SANS (7267)
[Mon-Fri, 9am-8pm EST]

Visit
www.sans.org/online-security-training/specials
for current Online Training specials.

Scan to check out the complete list of OnDemand courses and special offers throughout the year.
www.sans.org/info/113512

vLive

Live Virtual Training
Top SANS Instructors

Real-time access to Certified SANS Instructors

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

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

"I love the vLive format and really appreciate the ability to revisit content or participate asynchronously. I was unable to attend a session during its scheduled time and the recording was top-notch."

-David Fletcher, U.S. Air Force

"After having been through 3 sessions, one thing I am finding really nice about this delivery format is that we get both the vast experience and contextual information provided by the instructors combined with the ability to step back through and 'grep' a lot of the presented information in-between sessions."

-Steve Robinson, Avanade

www.sans.org/virtual-training/vlive

SANS' most popular classes taught by SANS' most popular instructors!

Current list of vLive courses scheduled for 2013

SEC560 - January
DEV541 - January
SEC660 - January
SEC575 - February
SEC505 - February
MGT414 - February
FOR408 - March
FOR508 - March
DEV544 - March
FOR610 - March
SEC504 - April
SEC401 - April
MGT512 - May
MGT414 - May
DEV541 - May
SEC542 - June
LEG523 - June
SEC617 - June
SEC566 - July
SEC642 - July
SEC401 - August
MGT414 - August
AUD507 - September
SEC560 - September
FOR408 - October
FOR508 - October
FOR610 - October
SEC504 - October
SEC503 - November
SEC575 - November
SEC542 - December
SEC566 - December

Schedule subject to change.
Please view the most current schedule at www.sans.org/virtual-training/sessions

Rob Lee
SANS Faculty Fellow

For more information
or to register,
please visit us at
www.sans.org/virtual-training/vlive

Still have questions?
Contact us at
vlive@sans.org.

Visit
www.sans.org/online-security-training/specials
for current Online Training specials.

Scan for a complete list of vLive courses or to register.
www.sans.org/info/113517

Simulcast

Live SANS Instruction in Multiple Locations!

Save on travel costs by training your distributed workforce with Live and Virtual Classrooms.

SANS Simulcast classes are:

COST-EFFECTIVE
You can save thousands of dollars on travel costs, making Simulcast an ideal solution for students working with limited training budgets or travel bans.

ENGAGING
Simulcast classes are live and interactive, allowing you to ask questions and share experiences with your instructor and classmates.

CONDENSED
Complete your course quickly; Event Simulcast classes run all day in real time with select courses being held at our live training events. Custom Simulcast classes are just that, classes that can be customized to your training requirements.

REPEATABLE
Simulcast classes are recorded and placed in an online archive in case you have to miss part of the class or just wish to view the material again at a later date.

COMPLETE
You will receive the same books and course materials that conference students receive, and you will see and hear the same material presented to students at the events.

To learn more about Simulcasts please e-mail us at simulcast@sans.org.

> *"Excellent course, excellent instructor and content. Truly enjoyed the learning experience. The vLive tool and moderator support was also excellent. This was my first SANS course, and I look forward to more training with your organization."*
> - Claudia Salguero, TELUS

To register or schedule your simulcast, visit
www.sans.org/virtual-training/event-simulcast

SANS Simulcast = The Best of Both Worlds

Using the same technology platform as vLive, SANS Simulcast provides real-time training for groups of 15 or more, regardless of location. Choose one of two options:

Event Simulcast

Want to attend a SANS event but can't because of budgetary or time constraints? Event Simulcast makes it possible for you to be a virtual event attendee and participate in the same class session as your event attendees.

Upcoming SANS Simulcasts

Security East 2013 (January)

SANS 2013 (March)

Security West 2013 (May)

SANSFIRE 2013 (June)

Boston 2013 (August)

Network Security 2013 (September)

Baltimore 2013 (October)

Cyber Defense Initiative 2013 (December)

Custom Simulcast

If you work at a company with offices in multiple states (or even countries), then our Custom Simulcast offering may be the perfect training solution for you and your colleagues. A SANS instructor teaches at one office location while remote employees attend class virtually, enabling you and your colleagues to receive the same group training at the same time.

To receive more information or to schedule a Custom Simulcast, please e-mail us at simulcast@sans.org.

James Tarala
SANS Senior Instructor

Online Delivery Methods Comparison

Choose the virtual method that works the best for you:

	OnDemand	vLive	Simulcast	SelfStudy
SANS top-notch computer security training	✓	✓	✓	✓
Suited for individual or group learning	✓	✓	✓	✓
Uses web-based training software available 24/7	✓			
Scheduled class sessions using webcast technology and collaboration software		✓	✓	
Integrated quizzes to enhance learning	✓			
Real-time access to certified SANS instructors		✓	✓	
Access to virtual mentors	✓			
Online access to MP3 audio files of instructor lectures	✓	✓	✓	✓
Includes supplemental materials, e.g., course books, MP3s, and when applicable, hands-on CDs and virtual labs	✓	✓	✓	✓
Includes practice tests with GIAC certification exams	✓	✓	✓	✓
Visit the website to find more info or to register	www.sans.org/ondemand	www.sans.org/vlive	www.sans.org/virtual-training/event-simulcast	www.sans.org/selfstudy

Additional SANS Training Options

Live Training Events

Training

The Most Trusted Name for Information Security Training

Nothing beats a SANS multi-course training event with live instruction from SANS' top faculty, a vendor solutions expo, bonus evening sessions, and networking with your peers. Our intensive, immersion courses are 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. SANS offers live training throughout the year in many major US cities as well as in Europe, Australia, Canada, Asia, India, and Dubai. SANS is the best place to network with other information security professionals, gain information on new vendor products, participate in challenges and contests, and hear world-class guest speakers! **www.sans.org/security-training/bylocation/index_all.php**

Community SANS

Community

Live Training in Your Community

Community SANS offers the most popular SANS courses in your local community in a small classroom setting – most classes have fewer than 25 students. The course material is delivered just like it would be at a larger SANS event; but with SANS training brought to your community, you'll save money on tuition and travel. **www.sans.org/community**

SANS OnSite

OnSite

Live Training at Your Location

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

SANS Mentor

Mentor

Intimate Live Instruction

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

SANS Summit Series

Summit

Live IT Security Summits and Training

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

SANS SelfStudy

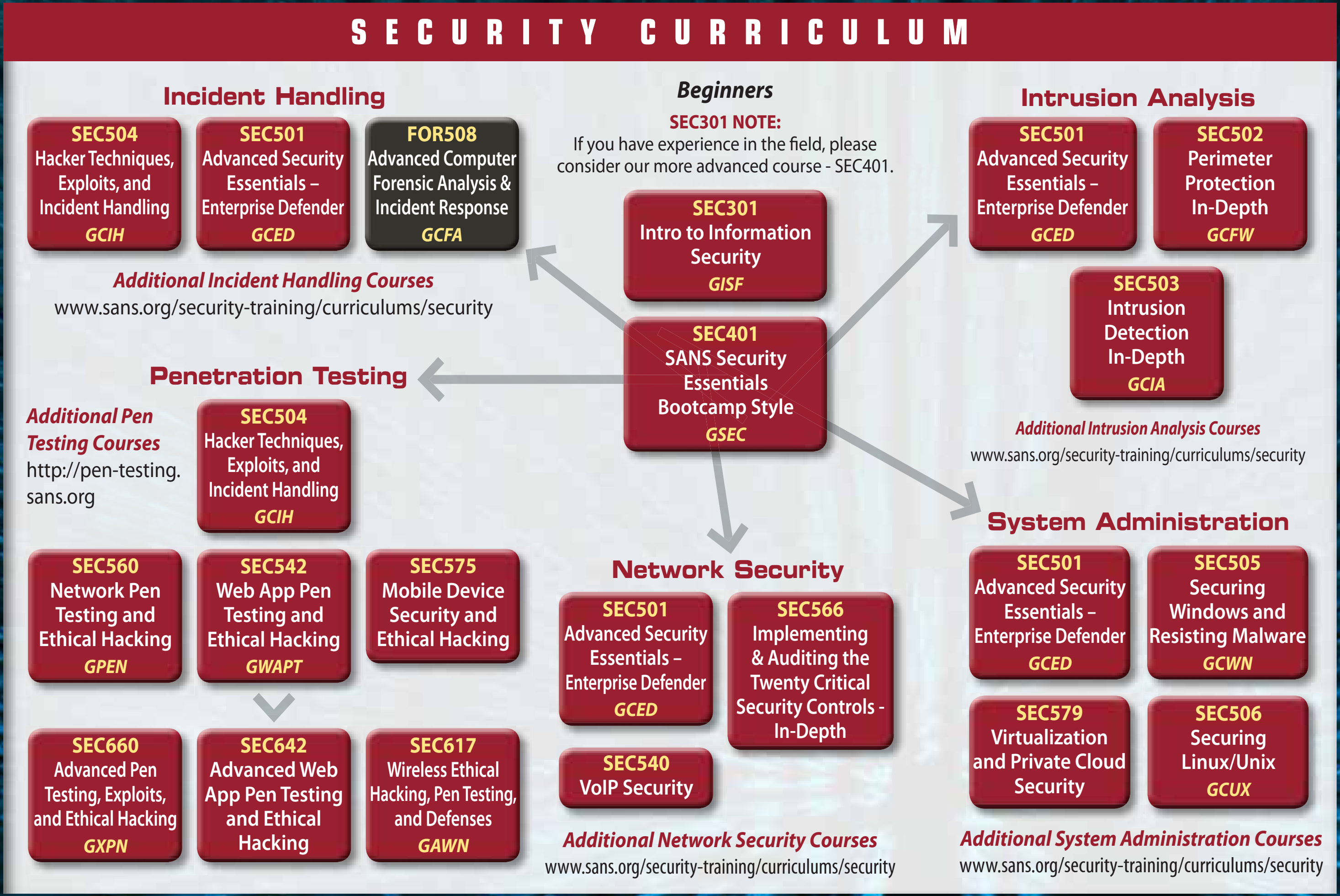
SelfStudy

Independent Study with Books and MP3s

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

SANS IT Security Training and Your Career Roadmap

SECURITY CURRICULUM



Beginners

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

SEC301 Intro to Information Security *GISF*

SEC401 SANS Security Essentials Bootcamp Style *GSEC*

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
www.sans.org/security-training/curriculums/security

Penetration Testing

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

- SEC504 Hacker Techniques, Exploits, and Incident Handling *GCIH*
- SEC560 Network Pen Testing and Ethical Hacking *GPEN*
- SEC542 Web App Pen Testing and Ethical Hacking *GWAPT*
- SEC575 Mobile Device Security and Ethical Hacking
- SEC660 Advanced Pen Testing, Exploits, and Ethical Hacking *GXPN*
- SEC642 Advanced Web App Pen Testing and Ethical Hacking
- SEC617 Wireless Ethical Hacking, Pen Testing, and Defenses *GAWN*

Network Security

- SEC501 Advanced Security Essentials – Enterprise Defender *GCED*
- SEC566 Implementing & Auditing the Twenty Critical Security Controls - In-Depth
- SEC540 VoIP Security

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

Intrusion Analysis

- SEC501 Advanced Security Essentials – Enterprise Defender *GCED*
- SEC502 Perimeter Protection In-Depth *GCFW*
- SEC503 Intrusion Detection In-Depth *GCIA*

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

System Administration

- SEC501 Advanced Security Essentials – Enterprise Defender *GCED*
- SEC505 Securing Windows and Resisting Malware *GCWN*
- SEC579 Virtualization and Private Cloud Security
- SEC506 Securing Linux/Unix *GCUX*

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

MANAGEMENT CURRICULUM

SEC301 Intro to Information Security *GISF*

SEC301 Intro to Information Security *GISF*

SEC401 SANS Security Essentials Bootcamp Style *GSEC*

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

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

MGT514 IT Security Strategic Planning, Policy, and Leadership

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

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

FORENSICS CURRICULUM

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

FOR508 Advanced Computer Forensic Analysis & Incident Response *GCFA*

FOR558 Network Forensics

FOR563 Mobile Device Forensics

FOR610 REM: Malware Analysis Tools & Techniques *GREM*

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

AUDIT CURRICULUM

SEC301 Intro to Information Security *GISF*

SEC401 SANS Security Essentials Bootcamp Style *GSEC*

AUD507 Auditing Networks, Perimeters, and Systems *GSNA*

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

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

LEGAL CURRICULUM

SEC301 Intro to Information Security *GISF*

SEC401 SANS Security Essentials Bootcamp Style *GSEC*

LEG523 Law of Data Security and Investigations *GLEG*

GIAC

GIAC certification available for courses indicated with GIAC acronyms

SOFTWARE SECURITY CURRICULUM

Defense

DEV522 Defending Web Applications Security Essentials *GWEB*

Secure Coding

JAVA

DEV541 Secure Coding in Java/JEE *GSSP-JAVA*

.NET

DEV544 Secure Coding in .NET *GSSP-.NET*

C & C++

DEV543 Secure Coding in C & C++

PCI

DEV536 Secure Coding for PCI Compliance

Attack

SEC542 Web App Pen Testing and Ethical Hacking *GWAPT*

SEC642 Advanced Web App Pen Testing and Ethical Hacking

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

Just Starting a Career in Security and Need a Good Foundation?

SECURITY 301

Intro to Information Security

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

We begin by covering basic terminology and concepts and then move to the basics of computers and networking, discussing Internet Protocol, routing Domain Name Service, and network devices. We cover the basics of cryptography and wireless networking; then we look at policy as a tool to effect change in your organization. In conclusion, 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.

Who Should Register:

- **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**

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.

All online courses provide students with course books, MP3s, and when applicable, hands-on CDs and virtual labs.

Fred Kerby *SANS Senior Instructor*

Fred is an engineer, manager, and security practitioner whose experience spans several generations of networking. He was the Information Assurance Manager at the Naval Surface Warfare Center, Dahlgren Division for more than sixteen years. His team is one of the recipients of the SANS Security Technology Leadership Award as well as the Government Technology Leadership Award. Fred received the Navy Meritorious Civilian Service Award in recognition of his technical and management leadership in computer and network security. A frequent speaker at SANS, Fred's presentations reflect his opinions and are not the opinions of the Department of the Navy.

GISF

GIAC Certification
www.giac.org

SECURITY 401

Security Essentials Bootcamp Style

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. Security Essentials is designed to give anyone interested in network security the skills required to be an effective player in this space. This in-depth, comprehensive course provides the essential, up-to-the-minute knowledge and skills required for securing systems and/or organizations. It also gives you the language and theory of computer security, all of it taught by 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.

Who Should Register:

- **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**

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 Security Essentials and the Bootcamp, we have really captured the critical aspects of security and enhanced those topics with examples to drive home the key points. After attending Security 401, I am confident you will walk away with solutions to problems you have had for a while plus solutions to problems you did not even know you had.

All online courses provide students with course books, MP3s, and when applicable, hands-on CDs and virtual labs.

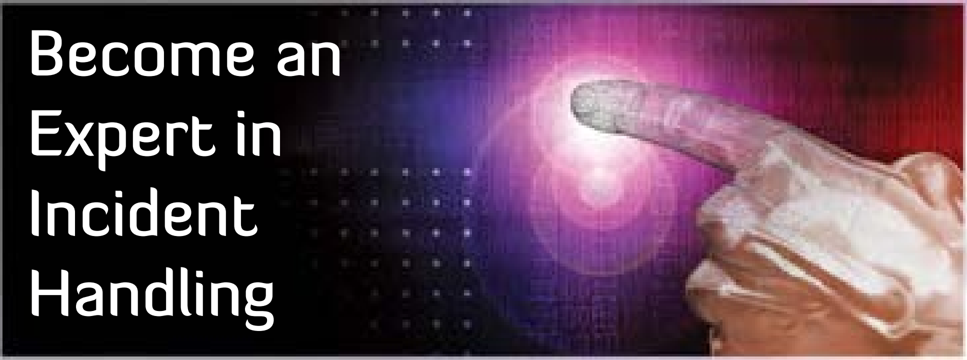
Dr. Eric Cole *SANS Faculty Fellow*

Dr. Eric Cole is an industry-recognized security expert with over 20 years of hands-on experience. Cole currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. 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. 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.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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



Become an Expert in Incident Handling

SECURITY 504

Hacker Techniques, Exploits & Incident Handling

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

Who Should Register:

- **Incident handlers**
- **Penetration testers**
- **Ethical hackers**
- **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**

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.

Ed Skoudis *SANS Faculty Fellow*

Ed Skoudis is a founder and senior security consultant with InGuardians. Ed's expertise includes hacker attacks and defenses, the information security industry, and computer privacy issues, with over fifteen years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (SEC560) and incident response (SEC504), helping over three thousand information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in financial, high technology, healthcare, and other industries. Ed conducted a demonstration of hacker techniques against financial institutions for the United States Senate and is a frequent speaker on issues associated with hacker tools and defenses. He has published numerous articles on these topics as well as the Prentice Hall best sellers ***Counter Hack Reloaded*** and ***Malware: Fighting Malicious Code***. Ed was also awarded 2004-2009 Microsoft MVP awards for Windows Server Security and is an alumnus of the Honeynet Project. Previous to InGuardians, Ed served as a security consultant with International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips. **http://blog.commandlinekungfu.com**

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

SECURITY 501

Advanced Security Essentials - Enterprise Defender

Cyber Security Survival Course - Security Enterprise Defender

Cyber security continues to be a critical area for organizations and 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. Security 501 is a follow up to SEC401: SANS Security Essentials (with no overlap) and continues to focus on more technical areas that are needed to protect an organization. The core focus of the course is on:

Prevention - configuring a system or network correctly

Detection - identifying that a breach has occurred at the system or network level

Reaction - responding to an incident and moving to evidence collection/forensics

A key theme is that prevention is ideal, but detection is a must. We need to be able to ensure that we constantly improve our security to prevent as many attacks as possible. This prevention/protection occurs on two fronts - 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 no matter whether it resides on a server, in a robust network architecture, or on a portable device.

Who Should Register:

- **Students who have taken SEC401: SANS 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**

Despite an organization's best effort at preventing attacks and protecting their 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 that is 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 is detected we must react to it 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.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

FORENSICS 508

Advanced Computer Forensic Analysis and Incident Response

Our adversaries are good and getting better. Are we learning how to counter them? Yes we are. Learn how.

FOR508 will give you the tools and techniques necessary to master advanced incident response, investigate data breach intrusions, find tech-savvy rogue employees, counter the Advanced Persistent Threat, and conduct complex digital forensic cases.

This course uses the popular SIFT Workstation to teach investigators how to investigate sophisticated crimes. SIFT contains hundreds of free and open source tools, easily matching any modern forensic tool suite. It demonstrates that advanced investigations and incident response can be accomplished using frequently updated, cutting-edge open source tools.

See the full course description at **www.sans.org/ondemand/courses.php**.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Want to Specialize in Pen Testing?

SECURITY 560

Network Penetration Testing & Ethical Hacking

Security vulnerabilities, such as weak configurations, unpatched systems, and botched architectures, continue to plague organizations. Enterprises need people who can find these flaws in a professional manner to help eradicate them from our infrastructures. Many 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 misunderstandings. We then discuss a time-tested methodology for penetration and ethical hacking across the network, evaluating the security of network services and the operating systems behind them.

Who Should Register:

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

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

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

All online courses provide students with course books, MP3s, and when applicable, hands-on CDs and virtual labs.

"Can't overemphasize the value in getting wisdom from a seasoned, experienced penetration tester."

-Sean Verity, MSUFCU

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

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.

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.

Who Should Register:

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

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.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

SECURITY 642

Advanced Web App Penetration Testing and Ethical Hacking

This course is designed to teach you the advanced skills and techniques required to test web applications today. This advanced pen testing course uses a combination of lecture, real-world experiences, and hands-on exercises to educate you in the techniques used to test the security of enterprise applications. The final day of the course culminates in a Capture the Flag (CtF) event, which tests the knowledge you will have acquired the previous five days.

This course will enhance your exploitation and defense skill sets as well as fulfill a need to teach more advanced techniques than can be covered in the foundational course, Security 542: Web Application Penetration Testing and Ethical Hacking.

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. 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 senior 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.

SECURITY 617

Wireless Ethical Hacking, Penetration Testing, and Defenses

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

To be a wireless security expert, you need to have a comprehensive understanding of the technology, the threats, the exploits, and the defense techniques along with hands-on experience in evaluating and attacking wireless technology. Not limiting your skill-set to WiFi, you'll need to evaluate the threat from other standards-based and proprietary wireless technologies as well. This course takes an in-depth look at the security challenges of many different wireless technologies, exposing you to wireless security threats through the eyes of an attacker. Using readily available and custom-developed tools, you'll navigate your way through the techniques attackers use to exploit WiFi networks, including attacks against WEP, WPA/WPA2, PEAP, TTLS, and other systems, including developing attack techniques leveraging Windows 7 and Mac OS X. We'll also examine the commonly overlooked threats associated with Bluetooth, ZigBee, DECT, and proprietary wireless systems. As part of the course, you'll receive the SWAT Toolkit, which will be used in hands-on labs to back up the course content and reinforce wireless ethical hacking techniques.

Who Should Register:

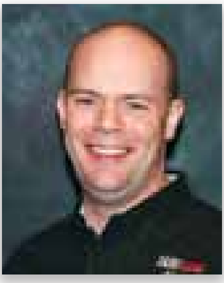
- **Ethical hackers and penetration testers**
- **Network security staff**
- **Network and system administrators**
- **Incident response teams**
- **Information security policy decision makers**
- **Technical auditors**
- **Information security consultants**
- **Wireless system engineers**
- **Embedded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

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

SWAT Toolkit consists of:

- **Sena Bluetooth USB Adapter UD100**
- **GlobalSat BU-353 USB GPS Navigation Receiver**
- **ALFA AWUS051NH: 802.11a/b/g/n 500mW USB Adapter**
- **[ONLINE STUDENTS ONLY] Linksys WRT54GL Router**

All online courses provide students with course books, MP3s, and when applicable, hands-on CDs and virtual labs.



Josh Wright *SANS Senior Instructor*

Joshua Wright is an independent information security analyst and senior instructor with the SANS Institute. A widely recognized expert in the wireless security field, Josh has worked with private and government organizations to evaluate the threat surrounding wireless technology and evolving threats. As an open-source enthusiast, Josh has developed a variety of tools that can be leveraged for penetration testing and security analysis. Josh publishes his tools, papers, and techniques for effective security analysis on his website at **www.willhackforsushi.com**.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Learn to detect malicious code and respond on the fly. You'll learn how your networks appear to hackers, how they gain access with special emphasis on the newer attack vectors, and what they do when they get in – especially in manipulating the system to hide their work. Master the proven six-step process of incident handling so you are prepared to be the technical leader of the incident handling team.

See the full course description on page 14 or visit www.sans.org/ondemand/courses.php.

SECURITY 575

Mobile Device Security and Ethical Hacking

Mobile phones and tablets have become essential to enterprise and government networks, from small organizations to Fortune 500 companies and large-scale agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient email access as well as managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from ERP to project management. With increased reliance on these devices, organizations are quickly recognizing that mobile phones and tablets need greater security implementations than a simple screen protector and clever password.

This course was designed to help organizations struggling with mobile device security by equipping personnel with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and mobile code analysis to penetration testing and ethical hacking, this course will help you build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in your organization.

Who Should Register:

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

You will gain hands-on experience in designing a secure mobile phone network for local and remote users and learn how to make critical decisions to support devices effectively and securely. You will also be able to analyze and evaluate mobile software threats, and learn how attackers exploit mobile phone weaknesses so you can test the security of your own deployment. With these skills, you will be a valued mobile device security analyst, fully able to guide your organization through the challenges of securely deploying mobile devices.

SECURITY 660

Advanced Penetration Testing, Exploits, and Ethical Hacking

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. Students with the prerequisite knowledge to take this course will walk through dozens of real world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered include weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, Return Oriented Programming (ROP), Windows exploit-writing, and much more!

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Advance Your Intrusion Analysis Skills

SECURITY 503

Intrusion Detection In-Depth

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

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

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

Who Should Register:

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

> *"This class heightens your security awareness on protecting your network and provides excellent examples, in detail, on how to accomplish this."*
>
> -Laura Freeman, DND

All online courses provide students with course books, MP3s, and when applicable, hands-on CDs and virtual labs.

Mike Poor *SANS Senior Instructor*

Mike is a founder and senior security analyst for the DC firm InGuardians, Inc. In the past he has worked for Sourcefire as a research engineer and for SANS leading their intrusion analysis team. As a consultant Mike conducts incident response, breach analysis, penetration tests, vulnerability assessments, security audits, and architecture reviews. His primary job focus, however, is in intrusion detection, response, and mitigation. Mike currently holds the GCIA certification and is an expert in network engineering and systems and network and web administration. Mike is an author of the international best-selling ***Snort*** series of books from Syngress, a member of the Honeynet Project, and a handler for the SANS Internet Storm Center.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

SECURITY 502

Perimeter Protection In-Depth

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

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.

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. 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.

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

Who Should Register:

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

Tanya Baccam *SANS Senior Instructor*

Tanya is a SANS senior instructor, as well as a SANS courseware author. With more than 10 years of information security experience, Tanya has consulted with a variety of clients about their security architecture in areas such as perimeter security, network infrastructure design, system audits, Web server security, and database security. Currently, Tanya provides a variety of security consulting services for clients, including system audits, vulnerability and risk assessments, database assessments, web application assessments, and penetration testing. She has previously worked as the director of assurance services for a security services consulting firm and served as the manager of infrastructure security for a healthcare organization. She also served as a manager at Deloitte & Touche in the Security Services practice. Tanya has played an integral role in developing multiple business applications and currently holds the CPA, GIAC GCFW, GIAC GCIH, CISSP, CISM, CISA, CCNA, and OCP DBA certifications. Tanya completed a bachelor of arts degree with majors in accounting, business administration and management information systems.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

Specialize in System Administration

SECURITY 506

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.

Throughout this course you will become skilled at utilizing freely available tools to handle security issues, including SSH, AIDE, sudo, lsof, and many others. SANS' practical approach with hands-on exercises every day ensures that you can start using these tools as soon as you return to work. We will also put these tools to work in a special section that covers simple forensic techniques for investigating compromised systems.

A Sampling of Topics:

- Memory Attacks, Buffer Overflows
- File System Attacks, Race Conditions
- Trojan Horse Programs and Rootkits
- Monitoring and Alerting Tools
- Unix Logging and Kernel-Level Auditing
- Building a centralized logging infrastructure
- Network Security Tools
- SSH for Secure Administration
- Server "lockdown" for Linux and Unix
- Controlling root access with sudo
- SELinux and chroot() for application security
- DNSSEC deployment and automation
- mod_security and Web Application Firewalls
- Secure Configuration of BIND, Sendmail, Apache
- Forensic Investigation

Who Should Register:

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

All online courses provide students with course books, MP3s, and when applicable, hands-on CDs and virtual labs.

Hal Pomeranz *SANS Faculty Fellow*

Hal Pomeranz is the founder and technical lead for Deer Run Associates, a consulting company focusing on Digital Forensics and Information Security. He is a SANS Faculty Fellow and the creator of the SANS/GIAC Securing Linux/Unix course (GCUX) as well as being an instructor in the SANS Forensics curriculum. An expert in the analysis of Linux and Unix systems, Hal provides forensic analysis services through his own consulting firm and by special arrangement with MANDIANT. He has consulted on several major cases for both law enforcement and commercial clients. Hal is a regular contributor to the SANS Computer Forensics blog, and co-author of the weekly Command-Line Kung Fu blog. **http://blog.commandlinekungfu.com**

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

SECURITY 505

Securing Windows and Resisting Malware

In April of 2014, Microsoft will stop releasing any new security patches for Windows XP. Like it or not, migrating off Windows XP is no longer optional, the clock is counting down. The Securing Windows and Resisting Malware course is fully updated for Windows Server 2012, Windows 8, Server 2008-R2, and Windows 7.

This course is about the most important things to do to secure Windows and how to minimize the impact on users of these changes. You'll see the instructor demo the important steps live, and, if you bring a laptop, you can follow along too. The manuals are filled with screenshots and step-by-step exercises, so you can do the steps alongside the instructor in seminar or later on your own time if you prefer.

We've all got anti-virus scanners, but what else needs to be done to combat malware and intruders using Advanced Persistent Threat (APT) techniques? Today's weapon of choice for hackers is stealthy malware with remote control channels, preferably with autonomous worm capabilities, installed through client-side exploits. While other courses focus on detection or remediation, the goal of this course is to prevent the infection in the first place (after all, first things first).

Especially in Server 2012 and beyond, PowerShell dominates Windows scripting and automation. It seems everything can be managed through PowerShell now. And if there's a needed skill that will most benefit the career of a Windows specialist, it's being able to write PowerShell scripts because most of your competition will lack scripting skills, so it's a great way to make your resume stand out. This course devotes an entire day to PowerShell scripting, but you don't need any prior scripting experience.

Who Should Register:

- Windows security engineers and system administrators
- Anyone who wants to learn PowerShell
- Anyone who wants to implement the SANS Critical Security Controls
- Those who must enforce security policies on Windows hosts
- Anyone who needs a whole drive encryption solution
- Those deploying or managing a PKI or smart cards
- IIS administrators and webmasters with servers at risk

This course will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) certification exam to help prove your security skills and Windows expertise. You are encouraged to bring a virtual machine running Windows Server 2012 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 2012 from Microsoft's web site (just do a search on "site:microsoft.com Server 2012 evaluation trial"). You can use Hyper-V, VMware, VirtualBox, or any other virtual machine software you wish.

This is a fun course and a real eye-opener even for Windows administrators with years of experience. Whether you're taking SEC505 live or in OnDemand, get the PowerShell scripts now for the course from **www.sans.org/windows-security** (go to the Downloads link). There is no prior registration required, and all scripts are in the public domain.

All online courses provide students with course books, MP3s, and when applicable, hands-on CDs and virtual labs.

Jason Fossen *SANS Faculty Fellow*

Jason Fossen is a principal security consultant at Enclave Consulting LLC, a published author, and a frequent public speaker on Microsoft security issues. He is the sole author of the SANS' week-long Securing Windows course (SEC505), maintains the Windows day of Security Essentials (SEC401.5), and has been involved in numerous other SANS' projects since 1998. He graduated from the University of Virginia, received his master's degree from the University of Texas at Austin, and holds a number of professional certifications. He currently lives in Dallas, Texas. Jason blogs about Windows Security Issues on the SANS Windows Security Blog.
http://blogs.sans.org/windows-security

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

Advance Your Auditing Security Skills

AUDIT 507

Auditing Networks, Perimeters, and Systems

This course is the end product of over one hundred skilled system, network and security administrators working with one common goal: to improve the state of information security.

Audit 507, like all SANS courses, is based on known and validated threats and vulnerabilities. These threats and vulnerabilities are explained based on validated information from real-world situations that can be used to raise awareness within an organization and build an understanding of why auditing is important. From these threats and vulnerabilities, we build the countermeasures and defenses including instrumentation, metrics and auditing. The course begins with a high-level introduction on methods and audit programs. It then takes you through all the particulars of how to actually audit devices and IT systems that range from firewalls and routers all the way down to the underlying operating systems.

You'll be able to use what you learn the day you get home. Five of the six days in the course will include hands-on exercises with the tools discussed during the lecture sections. Each student is invited to bring their own Windows 2000 or higher laptop for use during class. The hands-on exercises will allow you to experiment with the audit tools discussed in class and to actually perform audit functions against SANS-provided servers in class. A great audit is more than marks on a checklist; it is the understanding of the best practices, system analysis and forensics. Sign up for this course and experience the mix of theory, hands-on, and practical knowledge.

Who Should Register:

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

David Hoelzer *SANS Faculty Fellow*

David Hoelzer is a high-scoring certified SANS instructor and author of more than twenty sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past twenty-five years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a BS in IT, Summa Cum Laude, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University. David blogs about IT Audit issues at **https://blogs.sans.org/it-audit**.

GSNA

GIAC Certification
www.giac.org

SANS

STI Graduate School
www.sans.edu

All online courses provide students with course books, MP3s, and when applicable, hands-on CDs and virtual labs.

AUDIT/SECURITY 566

Implementing and Auditing the Twenty Critical Security Controls - In-Depth

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

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

Who Should Register:

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

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

All online courses provide students with course books, MP3s, and when applicable, hands-on CDs and virtual labs.

James Tarala *SANS Senior Instructor*

James Tarala is a principal consultant with Enclave Security and is based out of Venice, Florida. He is a regular speaker and senior instructor with the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years architecting large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them in their security management, operational practices, and regulatory compliance issues, and he often times performs independent security audits and assists internal audit groups to develop their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications.

Want to Specialize in Forensics?

FORENSICS 408

Computer Forensic Investigations - Windows In-Depth

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 such as Access Data's Forensic Toolkit (FTK), Guidance Software's EnCase, Registry Analyzer, FTK Imager, Prefetch Analyzer, and much more.

Who Should Register:

- 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

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

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

- **Tableau T35es Write Blocker (Read-Only)**
- **IDE Cable/Adapters**
- **SATA Cable/Adapters**
- **FireWire and USB Cable Adapters**
- **DVD loaded with case examples, tools, and documentation**
- **And More!**

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Rob Lee *SANS Faculty Fellow*

Rob Lee is an entrepreneur and consultant in the Washington D.C. area and currently the Curriculum Lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years' experience in computer forensics, vulnerability and exploit development, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and earned his MBA from Georgetown University. He served in the U.S. Air Force as a member of the 609th Information Warfare Squadron (IWS), the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI) where he led a team computer crime investigations and incident response. Over the next 7 years, he worked directly with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for a vulnerability discovery and an exploit development team, lead for a cyber-forensics branch, and lead for a computer forensic and security software development team. Most recently, Rob was a Director for MANDIANT, a commercial firm focusing on responding to advanced adversaries such as the APT. Rob co-authored the book ***Know Your Enemy***, 2nd Edition. Rob is also co-author of the MANDIANT threat intelligence report M-Trends: The Advanced Persistent Threat. Rob frequently contributes articles at the SANS Blog **http://computer-forensics.sans.org**.

FORENSICS 508

Advanced Computer Forensic Analysis and Incident Response

Over the past two years, we have seen a dramatic increase in sophisticated attacks against organizations. Cyber-attacks originating from China named the Advanced Persistent Threat (APT) have proved difficult to suppress. Financial attacks from Eastern Europe and Russia obtain credit card, and financial data resulting in millions of dollars stolen. Hackivist groups attacking government and Fortune500 companies are becoming bolder.

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 and avoid detection by standard host-based security measures. Every action that adversaries make leaves a trace; you merely need to know where to look.

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

This course utilizes the popular SIFT Workstation to teach investigators how to investigate sophisticated crimes. The free SIFT Workstation can match any modern forensic tool suite. It demonstrates that advanced investigations and responding to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

Our adversaries are good and getting better.

Are we learning how to counter them?

Yes we are. Learn how.

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

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

All online courses provide students with course books, MP3s, and when applicable, hands-on CDs and virtual labs.

FORENSICS 610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

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

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

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

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Want to Learn Security from a Management Perspective?

MANAGEMENT 414

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

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

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

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

Who Should Register:

- **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**
- **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**

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

GIAC Certification
www.giac.org

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will gain 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.

Who Should Register:

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

Essential security topics covered in this management track include: network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, Web application security, offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression™, special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA's CAQC program for Security + 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

All online courses provide students with course books, MP3s, and when applicable, hands-on CDs and virtual labs.

There are three goals for this course and certification:

- Establish a minimum standard for IT security knowledge, skills, and abilities. In a nutshell, this course covers all of the non-operating system topics that are in SANS Security Essentials, though not to the same depth. The goal is to enable managers and auditors to speak the same language as system, security, and network administrators.
- Establish a minimum standard for IT management knowledge, skills, and abilities. I keep running into managers that don't know TCP/IP, and that is OK; but then they don't know how to calculate total cost of ownership (TCO), leaving me quietly wondering what they do know.
- Save the up-and-coming generation of senior and rapidly advancing managers a world of pain by sharing the things we wish someone had shared with us. As the saying goes, it is OK to make mistakes, just make new ones.

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.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Stephen Northcutt *SANS Faculty Fellow*

Stephen Northcutt founded the GIAC certification and currently serves as president of the SANS Technology Institute, a postgraduate level IT security college (**www.sans.edu**). Stephen is author/coauthor of ***Incident Handling Step-by-Step***, ***Intrusion Signatures and Analysis***, ***Inside Network Perimeter Security*** 2nd Edition, ***IT Ethics Handbook***, ***SANS Security Essentials***, ***SANS Security Leadership Essentials***, and ***Network Intrusion Detection*** 3rd edition. He was the original author of the Shadow Intrusion Detection system before accepting the position of Chief for Information Warfare at the Ballistic Missile Defense Organization. Stephen is a graduate of Mary Washington College. Before entering the field of computer security, he worked as a Navy helicopter search and rescue crewman, white water raft guide, chef, martial arts instructor, cartographer, and network designer. Stephen also blogs at the SANS Security Leadership blog. **www.sans.edu/research/security-laboratory**

MANAGEMENT 305

Technical Communication and 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.

MANAGEMENT 411

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.

The strength of this document is derived from the meticulous attention to detail provided by the many contributing authors and organizations as well as the applicability of the standard to the realities of doing business today. The standard seeks to offer best practice guidance regarding all manner of security issues and can assist any organization that chooses to adopt it to develop a truly security minded corporate culture. Using our tested method for developing and applying controls using the ISO 27000 standard, you will learn to implement the guidance contained in ISO-27000 with step-by-step pragmatic examples to move quickly into compliance with the specification.

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. While the standard is very well written, anyone who has actually tried to shift to an ISO-27000 structured security organization knows that there can be some significant hurdles to overcome. This course will give you the information you need to go back to your organization with a plan of action to get the job done!

GIAC Certification
www.giac.org

MANAGEMENT 421

SANS Leadership and Management Competencies

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

Our focus in MGT421 is purely leadership-centric; we are not security-centric or technology-centric with this training opportunity. We discuss leadership skills that apply to commercial business, non-profit, not-for-profit, or other organizations. This course is designed to develop existing and new supervisors and managers who aspire to go beyond being the boss. It will help you build leadership skills to enhance the organization's climate and team-building skills to support the organization's mission, its growth in productivity, workplace attitude/satisfaction, and staff and customer relationships.

MANAGEMENT 433

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

Organizations have invested in information security for years now. Unfortunately, almost all of this effort has been focused on technology with little, if any, effort on the human factor. As a result, the human is now the weakest link. From RSA and Epsilon to Oak Ridge National Labs and Google, the simplest way for cyber attackers to bypass security is to target your employees. One of the most effective ways to secure the human is an active awareness and education program that goes beyond compliance and changes to behaviors. 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 develop metrics to measure the impact of your program and demonstrate value. Finally, through a series of labs and exercises, you will develop your own project and execution plan, so you can immediately implement your customized awareness program upon returning to your organization.

Want to Learn Security from a Legal Perspective?

LEGAL 523

Law of Data Security and Investigations

New laws regarding privacy, e-discovery, and data security are creating an urgent need for professionals who can bridge the gap between the legal department and the IT department. The professional training needed to accomplish this is uniquely available in SANS' LEG523 series of courses, which is designed to build skills in the analysis and use of contracts, policies, and records management procedures.

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

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

Who Should Register:

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

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

GIAC Certification
www.giac.org

Special Features! **This legal offering will cover many important 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.**

STI Graduate School
www.sans.edu

Benjamin Wright *SANS Senior Instructor*

Benjamin Wright is the author of several technology law books, including Business Law and Computer Security, published by the SANS Institute. With 26 years in private law practice, he has advised many organizations, large and small, on privacy, e-commerce, computer security, and e-mail discovery and been quoted in publications around the globe, from the ***Wall Street Journal*** to the ***Sydney Morning Herald***. In 2010, Russian banking authorities tapped him for experience and advice on the law of cyber investigations and electronic payments. Ben maintains a popular blog at **http://legal-beagle.typepad.com**.

DEVELOPER 522

Defending Web Applications Security Essentials

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

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

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

This class goes beyond classic web applications and includes coverage of Web 2.0 technologies, like AJAX and web services. We also arm you with knowledge to defend yourself against cutting-edge attackers, such as various protective HTTP headers and new generation of browser-based web application protections. To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding level implementation.

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

Who Should Register:

- 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

All online courses provide students with course books, MP3s, and when applicable, hands-on CDs and virtual labs.

Dr. Johannes Ullrich

SANS Senior Instructor

Dr. Johannes Ullrich is Dean of Faculty, Chief Research Officer and a faculty member. Johannes also serves on the following SANS Technology Institute committees: Faculty and Administration, Curriculum and Long Range Planning. As chief research officer for the SANS Institute, Johannes is currently responsible for the SANS Internet Storm Center (ISC) and the GIAC Gold program. He founded DShield.org in 2000, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. Prior to working for SANS, Johannes worked as a lead support engineer for a web development company and as a research physicist. Johannes holds a PhD in Physics from SUNY Albany and is located in Jacksonville, Florida. He also enjoys blogging about application security tips. **http://software-security.sans.org/blog**

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

DEVELOPER 541

Secure Coding in Java/JEE: Developing Defensible Applications

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.

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

Who Should Register:

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

Rather than teaching students to use a set of tools, we're teaching students concepts of secure programming. This involves looking at a specific piece of code, identifying a security flaw, and implementing a fix for flaws found on the Top 10 and CWE/SANS Top 25 Most Dangerous Programming Errors. The class culminates in a Secure Development Challenge where you perform a security review of a real-world open source application. You will conduct a code review, perform security testing to actually exploit real vulnerabilities, and finally, using the secure coding techniques that you have learned in class, implement fixes for these issues.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

DEVELOPER 544

Secure Coding in .NET: Developing Defensible Applications

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

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

Who Should Register:

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

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

GIAC Certification
www.giac.org

The SANS Discount Program That Pays You Credits and Delivers Flexibility

www.sans.org/vouchers

SANS Voucher Program – Overview

The SANS Voucher Program offers significant savings on our hands-on and job-based training as well as GIAC certification.

Universal Credit Benefits

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

Create a Voucher Account

Follow the steps below and contact us at vouchers@sans.org if you have any questions.

1. Designate a Point of Contact (POC) that will have the responsibility of allocating funds from your Voucher Program account.
2. Decide how much money to deposit into your Voucher Program account.
3. Submit the SANS Voucher Program Agreement form found at www.sans.org/vouchers

***PLEASE NOTE:** Due to the pre-negotiated discounts SANS Voucher Programs offer, they cannot be combined with any other promotions. Prices are subject to change, so please see www.sans.org/vouchers for current pricing.*

Universal Credit

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

SANS Universal Credit allows you to invest today, earn instant credits, and decide later how to spend your training credits over the next 12 months to maximize your investment and extend your fiscal year.

Universal Credit Pricing

Minimum Investment	Maximum Investment	Bonus	Example
$25,000	$75,000	10%	$50,000 investment = $55,000
$75,001	$150,000	20%	$100,000 investment = $120,000
$150,001	$300,000	25%	$200,000 investment=$250,000
$300,001	Call	Ask for quote	Contact Your Account Manager Vouchers@sans.org

Questions? E-mail vouchers@sans.org
or call 301-654-SANS (7267) [Mon-Fri, 9am-8pm EST]

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.

Master of Science Degree in Information Security Management (MSISM)

Master of Science Degree in Information Security Engineering (MSISE)

SANS Technology Institute Knowledge for Peace

www.sans.edu
info@sans.edu
720.941.4932

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.

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

Global Information Assurance Certification GIAC www.giac.org

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.

How the Program Works

This program begins with hands-on core courses that will build and increase your knowledge and skills. 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
  CISSP certification

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.

Online Training Registration Information

OnDemand

For SANS OnDemand, visit:
www.sans.org/ondemand

vLive

For SANS vLive, visit:
www.sans.org/virtual-training/vlive

Simulcast

For SANS Simulcast, visit:
www.sans.org/virtual-training/event-simulcast

SelfStudy

For SANS SelfStudy, visit:
www.sans.org/selfstudy

OnDemand and vLive Course Fees

AUD507	Auditing Networks, Perimeters & Systems	$4,220
AUD/SEC566	Implementing and Auditing the Twenty Critical Security Controls - In-Depth	$3,970
DEV522	Defending Web Applications Security Essentials	$4,220
DEV541	Secure Coding in Java/JEE: Developing Defensible Applications	$2,250
DEV544	Secure Coding in .NET: Developing Defensible Applications	$2,250
FOR408	Computer Forensic Investigations - Windows In-Depth	$4,600
FOR508	Advanced Computer Forensic Analysis and Incident Response	$4,600
FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	$3,970
LEG523	Law of Data Security and Investigations	$3,970
MGT305	Technical Communication and Presentation Skills for Security Professionals	$990
MGT411	SANS 27000 Implementation & Management	$3,800
MGT414	SANS® +S™ Training Program for the CISSP ® Certification Exam	$3,800
MGT421	Leadership and Management Competencies	$1,090
MGT433	Securing the Human: Building and Deploying an Effective Security Awareness Program	$1,710
MGT512	SANS Security Leadership Essentials For Managers with Knowledge Compression™	$4,510
SEC301	Intro to Information Security	$3,970
SEC401	SANS Security Essentials Bootcamp Style	$4,410
SEC501	Advanced Security Essentials - Enterprise Defender	$4,410
SEC502	Perimeter Protection In-Depth	$4,410
SEC503	Intrusion Detection In-Depth	$4,410
SEC504	Hacker Techniques, Exploits and Incident Handling	$4,600
SEC505	Securing Windows & Resisting Malware	$4,410
SEC506	Securing Linux/Unix	$4,410
SEC542	Web App Penetration Testing and Ethical Hacking	$4,410
SEC560	Network Penetration Testing and Ethical Hacking	$4,600
SEC575	Mobile Device Security and Ethical Hacking	$4,600
SEC617	Wireless Ethical Hacking, Penetration Testing, and Defenses	$4,410
SEC660	Advanced Penetration Testing, Exploits, and Ethical Hacking	$4,600
SEC642	Advanced Web App Penetration Testing and Ethical Hacking	$4,410

Please check the website for an up-to-date course list & current fees.
www.sans.org/online-security-training

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.

SANS Training:

- **Offers intensive, hands-on immersion training with the highest quality courseware in the industry**
- **Is taught by incomparable instructors and authors, the industry experts and practitioners who 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**

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 they 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.