THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Chicago 2014

Chicago, IL August 24-29

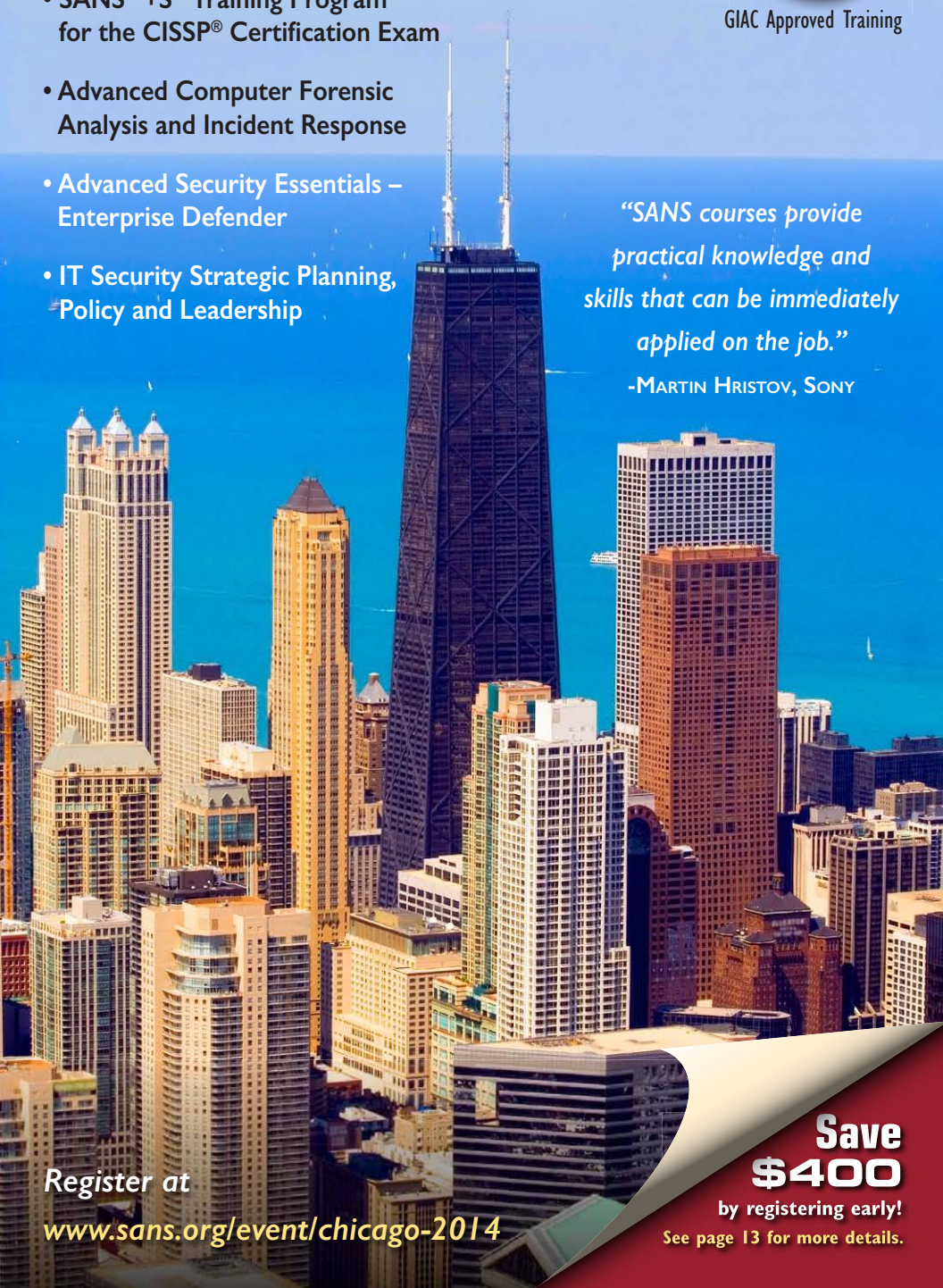
Choose from these popular courses:

- Security Essentials Bootcamp Style
- Hacker Techniques, Exploits, and Incident Handling
- Intrusion Detection In-Depth
- SANS® +S™ Training Program for the CISSP® Certification Exam
- Advanced Computer Forensic Analysis and Incident Response
- Advanced Security Essentials – Enterprise Defender
- IT Security Strategic Planning, Policy and Leadership

GIAC Approved Training

"SANS courses provide practical knowledge and skills that can be immediately applied on the job."

-Martin Hristov, Sony



Register at www.sans.org/event/chicago-2014

Save $400

by registering early!

See page 13 for more details.

We are pleased to invite you to our downtown Palmer House campus for **SANS Chicago 2014**, **August 24-29**. We're bringing you some of our most popular 5- and 6-day courses including SEC401: Security Essentials Bootcamp Style, SEC503: Intrusion Detection In-Depth, SEC504: Hacker Techniques, Exploits, and Incident Handling, and MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam. ***Register and pay for any course by July 2, 2014 and save $400!***

Taught by our top instructors, this event offers an intimate opportunity to learn, network, and practice in a hands-on environment that enables security professionals to develop and master the skills needed to excel in the field of cybersecurity. Learn from an instructor corps considered to be the best in the world. Not only do they meet SANS stringent requirements for excellence, they are all real-world practitioners. What you learn in class will be up-to-date and relevant to your jobs. Our instructors will ensure that what you learn in the classroom, you will be able to use immediately upon returning to the office – the SANS promise in action.

See this brochure for course descriptions and instructor bios. **GIAC** certification holders are recognized as experts in the IT industry and are sought after globally by government, military, and industry to protect the cyber environment, so see the GIAC page for more information on how to register. This brochure will also tell you about which SANS courses have associated GIAC certifications that are aligned with **DoD 8570**. Another thing to look for is how to earn your master's degree or post-baccalaureate certificate program through the **SANS Technology Institute**, the only accredited graduate institution focused solely on cybersecurity. For more information, see the SANS Technology Institute page and apply today!

Our campus is the **Palmer House Hilton Hotel** – a wonderful 140-year-old hotel that has undergone renovations to enhance the spectacular décor. A special discounted rate of $189.00 S/D will be honored based on space availability, see page 13 for details. You will have easy access to Lake Michigan, Millennium Park, and Grant Park where you can see incredible sculpture and gardens. Of course there are many more attractions close to the hotel – go to www.choosechicago.com for a complete list.

Enhance your training by attending our evening talks, complimentary for registered SANS Chicago 2014 students. So let your colleagues and friends know about SANS Chicago 2014. If you can't attend, please pass this brochure to any interested colleagues. We look forward to seeing you in Chicago!

SANS

Here's what SANS alumni have said about the value of SANS training:

"I want to live at SANS until all classes are taken!"
-Cory Flynn, Firewall Experts

"I think this type of security is very valuable to any IT professional. Security should always be at the top of the list."
-Ramon Baez, DOL

"The instructor explains very clearly, and he is very knowledgeable. I really enjoyed this class."
-Roya Kojouri, Brink's Incorporated

SC MAGAZINE AWARDS 2014 WINNER
Honored in the U.S.

Courses-at-a-Glance

		SUN 8/24	MON 8/25	TUE 8/26	WED 8/27	THU 8/28	FRI 8/29
SEC401	Security Essentials Bootcamp Style	Page 1					
SEC501	Advanced Security Essentials - Enterprise Defender	Page 2					
SEC503	Intrusion Detection In-Depth	Page 3					
SEC504	Hacker Techniques, Exploits, and Incident Handling	Page 4					
FOR508	Adv. Computer Forensic Analysis & Incident Response	Page 5					
MGT414	SANS® +S™ Training Program for the CISSP® Cert Exam	Page 6					
MGT514	IT Security Strategic Planning, Policy, and Leadership	Page 7					

@SANSInstitute *Join the conversation:* #SANSChicago

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Sun, Aug 24 - Fri, Aug 29
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Jonathan Ham

- GIAC Cert: GSEC
- Masters Program
- Cyber Guardian
- DoDD 8570

It seems wherever you turn organizations are being broken into, and the fundamental question that everyone wants answered is: Why? Why is it that some organizations get broken into and others do not? Organizations are spending millions of dollars on security and are still compromised. The problem is they are doing good things but not the right things. Good things will lay a solid foundation, but the right things will stop your organization from being headline news in the *Wall Street Journal*. SEC401's focus is to teach individuals the essential skills, methods, tricks, tools and techniques needed to protect and secure an organization's critical information assets and business systems.

This course teaches you the right things that need to be done to keep an organization secure. The focus is not on theory but practical hands-on tools and methods that can be directly applied when a student goes back to work in order to prevent all levels of attacks, including the APT (advanced persistent threat). In addition to hands-on skills, we will teach you how to put all of the pieces together to build a security roadmap that can scale today and into the future. When you leave our training we promise that you will have the techniques that you can implement today and tomorrow to keep your organization at the cutting edge of cyber security. Most importantly, your organization will be secure because students will have the skill sets to use the tools to implement effective security.

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks

"I would definitely recommend SEC401. This is very informative."
-Katrina Bright, GNS Contracting at Dept. of Energy

"SEC401 content is great, and I've learned a lot of useful skills I will be able to use in our organization."
-Brian White, DOJ

Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cyber security, three questions must be answered:

1. What is the risk?
2. Is it the highest priority risk?
3. Is it the most cost-effective way of reducing the risk?

Security is all about making sure you are focusing on the right areas of defense. By attending SEC401, you will learn the language and underlying theory of computer security. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security if you are given the responsibility for securing systems and/or organizations.

www.giac.org

www.sans.edu

www.sans.org/
cyber-guardian


www.sans.org/8570

"SEC401 is a great place to start for a wide range of topics. It is in depth, and leaves you wanting more."
-Todd Condit, Samaritan Health

Jonathan Ham *SANS Certified Instructor*

Jonathan is an independent consultant who specializes in large-scale enterprise security issues, from policy and procedure, through staffing and training, to scalable prevention, detection, and response technology and techniques. With a keen understanding of ROI and TCO (and an emphasis on process over products), he has helped his clients achieve greater success for over 12 years, advising in both the public and private sectors, from small upstarts to the Fortune 500. He's been commissioned to teach NCIS investigators how to use Snort, performed packet analysis from a facility more than 2000 feet underground, and chartered and trained the CIRT for one of the largest U.S. civilian Federal agencies. He has variously held the CISSP, GSEC, GCIA, and GCIH certifications, and is a member of the GIAC Advisory Board. A former combat medic, Jonathan still spends some of his time practicing a different kind of emergency response, volunteering and teaching for both the National Ski Patrol and the American Red Cross.

SECURITY 501

Advanced Security Essentials – Enterprise Defender

SANS
sans.org

Six-Day Program
Sun, Aug 24 - Fri, Aug 29
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Ted Demopoulos

- GIAC Cert: GCED
- Masters Program
- DoDD 8570

Who Should Attend

- Students who have taken Security Essentials and want a more advanced 500-level course similar to SEC401
- People who have foundational knowledge covered in SEC401, do not want to take a specialized 500-level course, and still want 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

Cybersecurity continues to be a critical area for organizations and will increase in importance as attacks become stealthier, have a greater financial impact on an organization, and cause reputational damage. Security Essentials lays a solid foundation for the security practitioner to engage the battle.

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 become 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.

Despite an organization's best effort at preventing attacks and protecting its 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. Understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

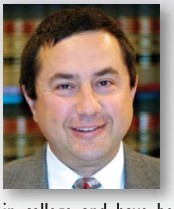
"SEC501 provided excellent information and guidance to share with the network team."
-Brent Steiner, CELink

"SEC501 has "refreshed" my hands-on experience, and familiarization with new software for router/ switches emerging technologies."
-Deneen Farrell, U.S. Cyber Command

www.giac.org

www.sans.edu

www.sans.org/8570



Ted Demopoulos *SANS Certified Instructor*

Ted Demopoulos' first significant exposure to computers was in 1977 when he had unlimited access to his high school's PDP-11 and hacked at it incessantly. He consequently almost flunked out but learned he liked playing with computers a lot. His business pursuits began in college and have been continuous ever since. His background includes over 25 years of experience in information security and business, including 20+ years as an independent consultant. Ted helped start a successful information security company, was the CTO at a "textbook failure" of a software startup, and has advised several other businesses. Ted is a frequent speaker at conferences and other events, quoted often by the press, and maintains Security Certs, a Web site on Security Certifications. He also has written two books on Social Media, has an ongoing software concern in Austin, Texas in the virtualization space, and is the recipient of a Department of Defense Award of Excellence. Ted lives in New Hampshire and more about him is available at Demopoulos Associates. In his spare time, he is also a food and wine geek, enjoys flyfishing, and playing with his children.

SECURITY 503

Intrusion Detection In-Depth

SANS

Six-Day Program
Sun, Aug 24 - Fri, Aug 29
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor:
Johannes Ullrich, Ph.D.

- GIAC Cert: GCIA
- Masters Program
- Cyber Guardian
- DoDD 8570

If you have an inkling of awareness of security (even my elderly aunt knows about the perils of the Interweb!), you often hear the disconcerting news about another high-profile company getting compromised. The security landscape is continually changing from what was once only perimeter protection to a current exposure of always-connected and often-vulnerable. Along with this is a great demand for security savvy employees who can help to detect and prevent intrusions. That is our goal in the **Intrusion Detection In-Depth** course – to acquaint you with the core knowledge, tools, and techniques to prepare you to defend your networks.

Who Should Attend

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

This course spans a wide variety of topics from foundational material such as TCP/IP to detecting an intrusion, building in breadth and depth along the way. It's kind of like the "soup to nuts" or bits to bytes to packets to flow of traffic analysis.

Hands-on exercises supplement the course book material, allowing you to transfer the knowledge in your head to your keyboard using the Packetrix VMware distribution created by industry practitioner and SANS instructor Mike Poor. As the Packetrix name implies, the distribution contains many of the tricks of the trade to perform packet and traffic analysis. All exercises have two different approaches. A more basic one that assists you by giving hints for answering the questions. Students who feel that they would like more guidance can use this approach. The second approach provides no hints, permitting a student who may already know the material or who has quickly mastered new material a more challenging experience. Additionally, there is an "extra credit" stumper question for each exercise intended to challenge the most advanced student.

By week's end, your head should be overflowing with newly gained knowledge and skills; and your luggage should be swollen with course book material that didn't quite get absorbed into your brain during this intense week of learning. This course will enable you to "hit the ground running" once returning to a live environment.

www.giac.org

www.sans.edu

www.sans.org/
cyber-guardian


www.sans.org/8570

"Johannes' excellent knowledge in application protocols has enabled us to get an in-depth understanding of them."
-Karthik, Symantec

"SEC503 gave validation to my own experiences and showed a number of tricks!"
-Richard Orman, U.S. Air Force

Johannes Ullrich, Ph.D. *SANS Senior Instructor*

Dr. Johannes Ullrich is the Dean of Research and a faculty member of the SANS Technology Institute. In November of 2000, Johannes started the DShield.org project, which he later integrated into the Internet Storm Center. His work with the Internet Storm Center has been widely recognized. In 2004, Network World named him one of the 50 most powerful people in the networking industry. Secure Computing Magazine named him in 2005 one of the Top 5 influential IT security thinkers. His research interests include IPv6, Network Traffic Analysis and Secure Software Development. Johannes is regularly invited to speak at conferences and has been interviewed by major publications, radio as well as TV stations. He is a member of the SANS Technology Institute's Faculty and Administration as well as Curriculum and Long Range Planning Committee. As chief research officer for the SANS Institute, Johannes is currently responsible for the GIAC Gold program. 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 maintains a daily security news summary podcast and enjoys blogging about application security.

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

SANS
sans.org

Six-Day Program
Sun, Aug 24 - Fri, Aug 29
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: Christopher Crowley

- GIAC Cert: GCIH
- Masters Program
- Cyber Guardian
- DoDD 8570

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.

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

Who Should Attend

- 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

"The labs in SEC504 were great, and they were real-world activities that I will be able to use going forward."
-Larry Petty, Tribridge

"SEC504 will be beneficial in broadening my security career. The instructor was excellent."
-Christian Pernell, 1st IO Command

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

Christopher Crowley *SANS Certified Instructor*

Christopher Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. Mr. Crowley is the course author for SANS Management 535 - Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GMOB, GPEN, GREM, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the year award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities.

FORENSICS 508

Advanced Computer Forensic Analysis and Incident Response

SANS
sans.org

Six-Day Program
Sun, Aug 24 - Fri, Aug 29
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Hal Pomeranz

- GIAC Cert: GCFA
- Masters Program
- Cyber Guardian
- DoDD 8570

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

This course focuses on providing incident responders with the necessary skills to hunt down and counter a wide range of threats within enterprise networks, including economic espionage, hactivism, and financial crime syndicates. The completely updated FOR508 addresses today's incidents by providing real-life, hands-on response tactics.

Who Should Attend

- Information security professionals
- Incident response team members
- Experienced digital forensic analysts
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 graduates

DAY 0: A 3-letter government agency contacts you to say that critical information was stolen from a targeted attack on your organization. Don't ask how they know, but they tell you that there are several breached systems within your enterprise. You are compromised by an Advanced Persistent Threat, aka an APT – the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Over 90% of all breach victims learn of a compromise from third party notification, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years. Gather your team—it's time to go hunting.

FOR508 will help you determine:

- **How did the breach occur?**
- **What systems were compromised?**
- **What did they take? What did they change?**
- **How do we remediate the incident?**

This course trains digital forensic analysts and incident response teams to identify, contain, and remediate sophisticated threats—including APT groups and financial crime syndicates. A hands-on lab—developed from a real-world targeted attack on an enterprise network—leads you through the challenges and solutions. You will identify where the initial targeted attack occurred and which systems an APT group compromised. The course will prepare you to find out which data were stolen and by whom, contain the threat, and provide your organization the capabilities to manage and counter the attack.

During a targeted attack, an organization needs the best incident responders and forensic analysts in the field. FOR508 will train you and your team to be ready to do this work.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8570

What you will receive with this course

- SIFT Workstation Virtual Machine
- F-Response TACTICAL Edition with a 2 year license
- Best-selling book "File System Forensic Analysis" by Brian Carrier
- Course DVD loaded with case examples, additional tools, and documentation

"I had no idea how much useful information could be acquired from memory analysis. We are definitely going to change the way we do IR from now on."
-Luis Martinez, Salt River Project

"I've taken other network intrusion classes but nothing this in depth. FOR508 is outstanding!"
-Craig Goldsmith, OCRCFL

Hal Pomeranz *SANS Faculty Fellow*

Hal Pomeranz is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft, to employee sabotage, to organized cybercrime and malicious software infrastructures. He has worked with law enforcement agencies in the US and Europe and global corporations. While equally at home in the Windows or Mac environment, Hal is recognized as an expert in the analysis of Linux and Unix systems. His research on EXT4 file system forensics provided a basis for the development of Open Source forensic support for this file system. His EXT3 file recovery tools are used by investigators worldwide. Hal is a SANS Faculty Fellow and Lethal Forensicator, and is the creator of the SANS Linux/Unix Security track (GCUX). He holds the GCFA and GREM certifications and teaches the related courses in the SANS Forensics curriculum. He is a respected author and speaker at industry gatherings worldwide. Hal is a regular contributor to the SANS Computer Forensics blog and co-author of the Command Line Kung Fu blog. @hal_pomeranz

MANAGEMENT 414

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

SANS sans.org

Six-Day Program
Sun, Aug 24 - Fri, Aug 29
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPE/CMU Credits
Laptop NOT Needed
Instructor: Eric Conrad

- GIAC Cert: GISP
- DoDD 8570

Take advantage of SANS CISSP® Get Certified Program currently being offered.

www.sans.org/special/cissp-get-certified-program

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 Attend

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

www.giac.org

www.sans.org/8570

Obtaining your CISSP® certification consists of:

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

Note: CISSP® exams are not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam.

"MGT414 clarifies the various security concepts and makes it easy to better approach the exam."
-William Nana Fabu, Synovus Financial Corp.

"Eric Conrad goes to great lengths to make sure the student is prepared for the exam."
-B. Taylor, U.S. Navy

Eric Conrad *SANS Principal Instructor*

Eric Conrad is lead author of the book "The CISSP Study Guide." Eric's career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and health care. He is now president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing. He is a graduate of the SANS Technology Institute with a master of science degree in information security engineering. In addition to the CISSP, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at www.ericconrad.com.

MANAGEMENT 514

IT Security Strategic Planning, Policy, and Leadership

SANS
sans.org

Five-Day Program
Sun, Aug 24 - Thu, Aug 28
9:00am - 5:00pm
30 CPE/CMU Credits
Laptop Recommended
Instructor: Mark Williams
- Masters Program

Strategic planning is hard for people in IT and IT security because we spend so much time responding and reacting. Some of us have been exposed to a SWOT or something similar in an MBA course, but we almost never get to practice until we get promoted to a senior position, and then we are not equipped with the skills we need to run with the pack.

Who Should Attend

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

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

We will see examples and hear stories from businesses, especially IT and security-oriented businesses, and then work together on labs. Business needs change, the environment changes, new risks are always on the horizon, and critical systems are continually exposed to new vulnerabilities. Strategic planning is a never-ending process. The planning section is hands-on and there is exercise-intensive work on writing, implementing, and assessing strategic plans.

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

www.sans.edu

"As an IT manager, MGT514 opened my eyes to the importance of policy and planning."
-Amur Al-Sarmi, RAFO

"MGT514 provided applicable and actionable knowledge for my InfoSec program. It was an invaluable experience."
-Jeremy Edson, Butler University

"MGT514 contained a lot of good practical information – both professional and personal value."
-Keith Turpin, Boeing

Mark Williams *SANS Instructor*

Mark Williams currently holds the position of Principal Systems Security Officer at BlueCross BlueShield of Tennessee. Mark holds multiple certifications in security and privacy including CISSP, CISA, CRISC, and CIPP/IT. He has authored and taught courses at undergraduate and graduate levels, as well as public seminars around the world. He has worked in public and private sectors in the Americas, Canada, and Europe in the fields of security, compliance, and management. Mark has more than 20 years of international high-tech business experience working with major multinational organizations, governments, and private firms. During this career Mark has consulted on issues of privacy and security, lead seminars, and developed information security, privacy, and compliance related programs.

CHICAGO BONUS SESSIONS

SANS@Night Evening Talks

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

KEYNOTE: The Security Impact of IPv6 *Johannes Ullrich, Ph.D.*

IPv6 is more then just lots of addresses. IPv6 is protocol moving IP into the modern world of gigabit networks connecting billions of machines with gigabytes of RAM. In many ways, this transition is similar to the "DC" to "AC" conversion in the electric world. While we still use DC in many places, AC has shown to be more flexible and scalable. Its initial adoption was hindered by security concerns, and DC supporters like Edison went to great lengths to demonstrate the security problems by stealing pets and electrocuting them in public displays. The fear of IPv6 is in many ways a fear of the unknown. IPv6 has some inherent risks, in particular if the protocol's opportunities are not well understood, and IPv4 thinking is applied to its deployment. We will discuss the impact of IPv6 on security architecture, intrusion detection, and network forensics, without harming anybody's pet.

Continuous Ownage: Why you Need Continuous Monitoring *Eric Conrad*

Repeat after me, "I will be breached." Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous, and the monitoring must match. This talk will help you face this problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring. The talk will also give you a hint at the value you and your organization will gain from attending Seth Misenar and Eric Conrad's new course, SEC511: Continuous Monitoring and Security Operations.

Vendor Security ... Really? *Mark Williams*

So it's time to play twenty questions with your vendor. What do you ask? How far should you go? How do we know if the answers are good/honest? Do we expect that they should be exactly as secure as we are? What if they are not? What if they are better than us? Assessing vendors for information security risk is something many of us are charged with on a regular basis. While we want to make sure vendors secure our information, we do not always have the "big hammer" to swing in terms of insisting on compliance. After all, what if a major vendor of software that you NEED to deal with does not measure up to your company's security posture? So what? Do you care? Should you care? What can you do to make the situation better? In this somewhat irreverent look at assessing vendor security, I will try to dispel some myths, instill a sense of hope, and help you develop the healthy skepticism that is necessary to keep you sane. I will also discuss where the decision should rest (in my humble opinion).

Automating Linux Memory Capture for Analysis *Hal Pomeranz*

Volatility has included support for Linux memory analysis since v2.2. However, practitioners have faced two obstacles: (1) Acquiring memory from a Linux system requires building, loading, and correctly using a third-party kernel module (such as LiME) for each system encountered; and (2) Creating a system-specific volatility "profile" for each system. Even for experts, these tasks are nontrivial and error prone if performed manually. Fortunately, the Linux environment makes scripting and automation straightforward. This session presents a tool to capture actionable information from Linux systems. The tool, which has been tested and used many times, was created to be a simple, automated collection agent that can be installed on a portable USB device. The user should be able to insert the USB device into a system and execute a single command to capture the memory of the system and produce a Volatility profile for use in later analysis. This session covers the basics of Linux memory capture and Volatility profile creation as a manual process, then looks at how to install and use the tool as a portable agent.

SANS 8 Mobile Device Security Steps *Christopher Crowley*

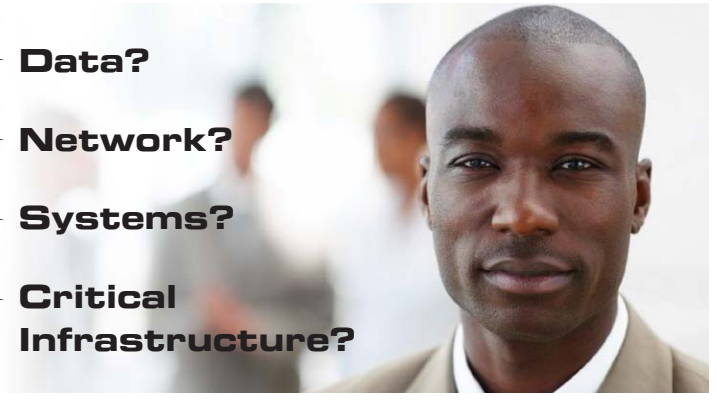
Every organization is challenged to rapidly deploy mobile device security. The SANS 8 Mobile Device Security Steps is a community-driven project to provide the most up-to-date information on the most effective strategies for securing mobile infrastructure. Chris Crowley will discuss the guidance provided in the 8 Steps, including: user authentication and restricting unauthorized access, OS and application management, device monitoring, and key operational components for mobile device management.

Infosec Rock Star: How to be a More Effective Security Professional

Ted Demopoulos

Why are some of us much more effective than others? A very few of us are so effective, and well known, that we might even be called the rock stars of our industry. Now we personally may never be swamped by groupies, but we can learn the skills be more effective, well respected, and well paid. Obviously it's not just about technology; in fact most of us are very good at the technology part. The myth of the geek with zero social skills is just that, a myth. However, the fact is that increasing our skills more on the social and business sides will make most of us more effective at what we do than learning how to read hex better while standing on our heads, becoming 'One with Metasploit' or understanding the latest hot technologies will.

How Are You Protecting Your



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 27 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

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

Get Certified at
www.giac.org

Department of Defense Directive 8570 *(DoDD 8570)*

www.sans.org/8570

Department of Defense Directive 8570 (DoDD 8570) provides guidance and procedures for the training, certification, and management of all government employees who conduct information assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. GIAC provides the most options in the industry for meeting 8570 requirements.

SANS Training Courses for DoDD Approved Certifications

SANS TRAINING COURSE		DoDD APPROVED CERT
SEC401	Security Essentials Bootcamp Style	GSEC
SEC501	Advanced Security Essentials – Enterprise Defender	GCED
SEC503	Intrusion Detection In-Depth	GCIA
SEC504	Hacker Techniques, Exploits, and Incident Handling	GCIH
AUD507	Auditing Networks, Perimeters, and Systems	GSNA
FOR508	Advanced Computer Forensic Analysis and Incident Response	GCFA
MGT414	SANS® +S™ Training Program for the CISSP® Certification Exam	CISSP
MGT512	SANS Security Essentials for Managers with Knowledge Compression™	GSLC

Compliance/Recertification:
To stay compliant with DoDD 8570 requirements, you must maintain your certifications. GIAC certifications are renewable every four years. Go to www.giac.org to learn more about certification renewal.

DoDD 8570 certification requirements are subject to change, please visit http://iase.disa.mil/eta/iawip for the most updated version.

For more information, contact us at 8570@sans.org or visit www.sans.org/8570

FUTURE SANS TRAINING EVENTS

Information on all events can be found at www.sans.org/security-training/by-location/all

SANSFIRE 2014

Baltimore, MD | June 21-30

SANS Capital City 2014

Washington, DC | July 7-12

SANS San Francisco 2014

San Francisco, CA | July 14-19

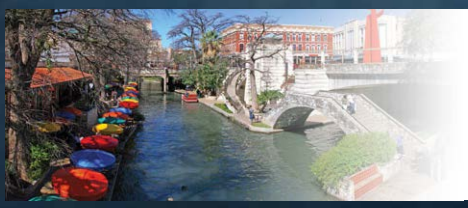
SANS ICS Industrial Control Systems

ICS Security TRAINING 2014 - HOUSTON

Houston, TX | July 21-25

SANS Boston 2014

Boston, MA | July 28 - August 2



SANS San Antonio 2014

San Antonio, TX | August 11-16

SANS Cyber Defense SUMMIT

Nashville, TN | August 13-20

SANS Virginia Beach 2014

Virginia Beach, VA | August 18-29

SANS Crystal City 2014

Crystal City, VA | September 8-13

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events

Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with your Peers

www.sans.org/security-training/by-location/all

Community SANS

Live Training in Your Local Region with Smaller Class Sizes

www.sans.org/community

OnSite

Live Training at Your Office Location

www.sans.org/onsite

Mentor

Live Multi-Week Training with a Mentor

www.sans.org/mentor

Summit

Live IT Security Summits and Training

www.sans.org/summit

ONLINE TRAINING

OnDemand

E-learning Available Anytime, Anywhere, at your Own Pace

www.sans.org/ondemand

vLive

Online, Evening Courses with SANS' Top Instructors

www.sans.org/vlive

Simulcast

Attend a SANS Training Event without Leaving Home

www.sans.org/simulcast

OnDemand Bundles

Extend your training with an OnDemand Bundle Including Four Months of E-learning www.sans.org/ondemand/bundles

SANS CHICAGO 2014

Hotel Information

Training Campus
Palmer House Hilton Hotel

17 East Monroe Street
Chicago, IL 60603
www.sans.org/event/chicago-2014/location

Special Hotel Rates Available

A special discounted rate of $189.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high speed Internet in your room and are only available through July 30, 2014. To make reservations please call 800-445-8667 and ask for the SANS group rate.

140 Years. Countless Stories. The Palmer House didn't become a beloved downtown Chicago hotel by chance. It did so by design. Since 1871, the iconic Chicago hotel has been host to countless celebrated figures. Today, having undergone a meticulous $170 million renovation, the Palmer House awaits those stories yet to be written and forever to be retold. We invite you to share in the inspired story of this downtown Chicago hotel. Even more so, within the walls and halls of the Palmer House, we encourage you to compose your own.

Top 5 reasons to stay at the Palmer House Hilton Hotel

1. All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.
2. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
3. By staying at the Palmer House Hilton Hotel, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
4. SANS schedules morning and evening events at the Palmer House Hilton Hotel that you won't want to miss!
5. Everything is in one convenient location!

SANS CHICAGO 2014

Registration Information

We recommend you register early to ensure you get your first choice of courses.

Register online at www.sans.org/event/chicago-2014/courses

Select your course or courses and indicate whether you plan to test for GIAC certification.

If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**7/2/14**	**$400.00**	**7/23/14**	**$250.00**

Some restrictions apply.

Group Savings (Applies to tuition only)*

10% discount if 10 or more people from the same organization register at the same time
5% discount if 5-9 people from the same organization register at the same time

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

**Early-bird rates and/or other discounts cannot be combined with the group discount.*

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by August 6, 2014 – processing fees may apply.

SANS Voucher Credit Program

Expand your training budget! Extend your Fiscal Year. The SANS Voucher Discount Program pays you credits and delivers flexibility.
www.sans.org/vouchers