THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

SANS Chicago 2016

August 22-27

SANS OFFERS HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

SAVE $400

by registering and paying early!

See page 13 for more details.

Protect your company and advance your career with information security training from SANS!

Nine courses on

CYBER DEFENSE

PEN TESTING

DIGITAL FORENSICS

ICS SECURITY

IT LEGAL

"Thank you SANS! I have doubled my security knowledge."

-Jerome Joseph, Nationwide Insurance

REGISTER AT

www.sans.org/chicago

GIAC-Approved Training

SANS Instructors

SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses. This guarantees that what you learn in class will be up to date and relevant to your job. The SANS Chicago 2016 lineup of instructors includes:

Ted Demopoulos
Certified Instructor

Bryce Galbraith
Principal Instructor

Tim Garcia
SANS Instructor

Jonathan Ham
Certified Instructor

Heather Mahalik
Senior Instructor

Billy Rios
SANS Instructor

Peter Szczepankiewicz
Certified Instructor

Jake Williams
Certified Instructor

Benjamin Wright
Senior Instructor

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 10.

KEYNOTE: ***Analysis of Destructive Cyber Attacks***
Jake Williams

Security Leadership for Everyone: Personal Authority and Beyond
Ted Demopoulos

The Dizzy New World of Cyber Investigations: Law, Ethics, and Evidence
Ben Wright

Be sure to register and pay by June 29th for a $400 tuition discount!

Courses-at-a-Glance

SEC401:

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Aug 22 - Sat, Aug 27
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Tim Garcia

www.giac.org/gsec

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"I really appreciate this instructor and I am utilizing this course so as to improve my practices."
-Margaux Hoaglund, Union Pacific

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

Learn to build a security roadmap that can scale today and into the future.

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization's critical information assets and business systems. This course will show you how to prevent your organization's security problems from being headline news in the *Wall Street Journal*!

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
- Forensic analysts, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

With the rise of advanced persistent threats, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organization's network depends on the effectiveness of the organization's defense. Defending against attacks is an ongoing challenge, with new threats emerging all of the time, including the next generation of threats. Organizations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

- What is the risk?
- Is it the highest priority risk?
- What is the most cost-effective way to reduce the risk?

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you'll need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

Tim Garcia *SANS Instructor*

Timothy Garcia is a seasoned security professional who loves the challenge and continuously changing landscape of defense. Tim started his career as an IT engineer, and after working on a few security incidents related to Code Red and Nimda he realized he had found his calling. Tim currently works as an Information Security Consultant for Wells Fargo and has expertise in systems engineering, project management and information security principles and procedures/compliance. Before Wells Fargo, Tim worked for Intel and served in the military. Tim is as passionate about teaching security as he is performing it and receives the greatest joy when he sees the look in students' eyes when something they never quite understood finally makes sense. Tim holds the CISSP, GSEC, GCIH, and NSA-IAM certifications. He has extensive knowledge of security procedures and legislation such as Sarbanes-Oxley, GLBA, CobiT, COSO, and ISO 1779. When Tim is not defending systems, he enjoys playing sports, snowboarding and, most of all, spending time with his wife and four children. @tbg911

SEC501:

Advanced Security Essentials – Enterprise Defender

SANS

Six-Day Program
Mon, Aug 22 - Sat, Aug 27
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Ted Demopoulos

www.giac.org/gced

SANS Technology Institute
www.sans.edu

www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand

"SEC501 has a nice balance between courseware, labs, and lectures that include examples, reviews, and interesting tidbits of current events to keep everyone involved." -Debra S., Naval Supply Systems Command FLCSD

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. **SEC501: Advanced Security Essentials – Enterprise Defender** builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

Who Should Attend

- Incident response and penetration testers
- Security Operations Center engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

It has been said of security that "prevention is ideal, but detection is a must." However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. This PREVENT – DETECT – RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

"I can't stress enough how important the SEC501 course is for today's network defenders. It's a hostile world, so why settle for anything less than the best? SANS is simply the best!" -John J., Houston PD

Of course, despite an organization's best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organizations need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, looking for indications of an attack, and performing penetration testing and vulnerability analysis against your organization to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

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 ongoing 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. 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. In his spare time, he is a food and wine geek, enjoys flyfishing, and plays with his children. @TedDemop

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Aug 22 - Sat, Aug 27
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor:
Peter Szczepankiewicz

www.giac.org/gcih

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand

"If you love cybersecurity and learning how exploits work, you NEED this course."
-Jaid K., U.S. Navy

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose does not!), 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. ***As defenders, it is essential we understand these hacking tools and techniques.***

Who Should Attend

- Incident handlers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

"SEC504 teaches you methods for testing your defenses and how to identify weaknesses in your network and systems." -Rene Graf, Federal Home Loan Bank

This course will enable you to turn the tables on computer attackers by helping you understand their tactics and strategies in detail. It will give you hands-on experience in finding vulnerabilities and discovering intrusions, and equip you with a comprehensive incident handling plan. The course addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, it provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare for, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a ***hands-on*** workshop that focuses on scanning, exploiting, and defending systems. This will enable you to discover the holes in your system before the bad guys do!

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. ***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.***

"This course really puts the state of things in perspective. We need to be proactive to combat the threats of the Internet, and this is a great place to start."
-Jonathan Mani, McIlhenny Company

Peter Szczepankiewicz *SANS Certified Instructor*

Peter is currently a Senior Security Engineer with IBM. In previous work with the U.S. military, he responded to network attacks and worked with both defensive and offensive red teams. Peter is all too aware that people lead technology, not the other way around. He works daily to bring actionable intelligence out of disparate security devices for customers, making systems interoperable. He believes that putting together networks only to tear them apart is just plain fun, and that it enables students to take the information learned from books, put it into hands-on practice, and take the skills they learn back to their workplaces.

SEC550:

Active Defense, Offensive Countermeasures & Cyber Deception

SANS

Five-Day Program
Mon, Aug 22 - Fri, Aug 26
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Bryce Galbraith

The current threat landscape is shifting. Traditional defenses are failing us. We need to develop new strategies to defend ourselves. Even more importantly, we need to better understand who is attacking us and why. You may be able to immediately implement some of the measures we discuss in this course, while others may take a while. Either way, consider what we discuss as a collection of tools at your disposal when you need them to annoy attackers, determine who is attacking you, and, finally, attack the attackers.

Who Should Attend

- General security practitioners
- Penetration testers
- Ethical hackers
- Web application developers
- Website designers and architects

SEC550: Active Defense, Offensive Countermeasures, and Cyber Deception is based on the Active Defense Harbinger Distribution live Linux environment funded by the Defense Advanced Research Projects Agency (DARPA). This virtual machine is built from the ground up for defenders to quickly implement Active Defenses in their environments. The course is very heavy with hands-on activities – we won't just talk about Active Defenses, we will work through labs that will enable you to quickly and easily implement what you learn in your own working environment.

"SEC550 is the next step in the evolution of cyber defense in learning to make the hackers' job harder, track their movements, and get attribution."
-Mick Leach, Nationwide

"Bryce is one of the best tech instructors I have had to date, both articulate and engaging."
-Jacob Parks, Insperity

You Will Be Able To

- Track bad guys with callback Word documents
- Use Honeybadger to track web attackers
- Block attackers from successfully attacking servers with honeyports
- Block web attackers from automatically discovering pages and input fields
- Understand the legal limits and restrictions of Active Defense
- Obfuscate DNS entries
- Create non-attributable Active Defense Servers
- Combine geolocation with existing Java applications
- Create online social media profiles for cyber deception
- Easily create and deploy honeypots

What You Will Receive

- A fully functioning Active Defense Harbinger Distribution ready to deploy
- Class books and a DVD with the necessary tools and the OCM virtual machine, which is a fully functional Linux system with the OCM tools installed and ready to go for the class and for the students' work environments

Bryce Galbraith *SANS Principal Instructor*

As a contributing author of the international bestseller *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. He has held security positions at global ISPs and Fortune 500 companies, was a member of Foundstone's renowned penetration testing team, and served as a senior instructor and co-author of Foundstone's Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security, where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS Institute's most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, holds several security certifications, and speaks at conferences worldwide. @brycegalbraith

FOR408:
Windows Forensic Analysis

SANS

Six-Day Program
Mon, Aug 22 - Sat, Aug 27
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Heather Mahalik

www.giac.org/gcfe

SANS Technology Institute
www.sans.edu

▶II **Bundle OnDemand**
WITH THIS COURSE
www.sans.org/ondemand

DFIR
digital-forensics.sans.org

"This course helped on both a professional and personal level. The information also helped me better communicate to non-InfoSec professionals the importance of having certain security controls."
-Maria Bello, Federal National Mortgage Association

Master Windows Forensics – You can't protect what you don't know about.

Every organization must prepare for cyber crime occurring on its computer systems and within its networks. Demand has never been greater for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

Who Should Attend

- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

"Current and up-to-date material. Cutting edge!"
-John Powell, SaskTel

FOR408: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and artifacts is a core component of information security. Learn to recover, analyze, and authenticate forensic data on Windows systems. Understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. Use your new skills to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR408 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 10 artifacts.

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

Heather Mahalik *SANS Senior Instructor*

Heather Mahalik is a project manager for Ocean's Edge, where she uses her experience to manage projects focused on wireless cybersecurity and mobile application development. Heather has over 12 years of experience in digital forensics, vulnerability discovery of mobile devices, application reverse engineering and manual decoding. She is currently the course lead for FOR585: Advanced Smartphone Forensics. Previously, Heather headed the mobile device team for Basis Technology, where she led the mobile device exploitation efforts in support of the U.S. government. She also worked as a forensic examiner at Stroz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she focused on high-profile cases. Heather co-authored Practical Mobile Forensics and various white papers, and has presented at leading conferences and instructed classes focused on Mac forensics, mobile device forensics, and computer forensics to practitioners in the field. Heather blogs and hosts work from the digital forensics community at www.smarterforensics.com. @HeatherMahalik

FOR578:
Cyber Threat Intelligence

NEW

SANS

Five-Day Program
Mon, Aug 22 - Fri, Aug 26
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Jake Williams

DFIR
digital-forensics.sans.org

Make no mistake: current computer network defense and incident response contain a strong element of intelligence and counterintelligence that analysts must understand and leverage in order to defend their computers, networks, and proprietary data.

FOR578: Cyber Threat Intelligence will help network defenders and incident responders:

- Construct and exploit threat intelligence to detect, respond to, and defeat advanced persistent threats (APTs)
- Fully analyze successful and unsuccessful intrusions by advanced attackers
- Piece together intrusion campaigns, threat actors, and nation-state organizations
- Manage, share, and receive intelligence on APT adversary groups
- Generate intelligence from their own data sources and share it accordingly
- Identify, extract, and leverage intelligence from APT intrusions
- Expand upon existing intelligence to build profiles of adversary groups
- Leverage intelligence to better defend against and respond to future intrusions

Conventional network defenses such as intrusion detection systems and anti-virus tools focus on the vulnerability component of risk, and traditional incident response methodology pre-supposes a successful intrusion. However, the evolving sophistication of computer network intrusions has rendered these approaches insufficient to address the threats faced by modern networked organizations. Today's adversaries accomplish their goals using advanced tools and techniques designed to circumvent most conventional computer network defense mechanisms, go undetected during the intrusion, and then remain undetected on networks over long periods of time.

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that can be used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture. Threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats.

During a targeted attack, an organization needs a top-notch and cutting-edge incident response team armed with the critical intelligence necessary to understand how adversaries operate and to combat the threat. FOR578 will train you and your team to detect, scope, and select resilient courses of action in response to such intrusions and data breaches.

THERE IS NO TEACHER BUT THE ENEMY!

Who Should Attend

- Incident response team members
- Security Operations Center personnel and information security practitioners
- Experienced digital forensic analysts
- Federal agents and law enforcement officials
- SANS FOR408, FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

"Jake's use of real-life scenarios is very useful, it keeps everything relevant and interesting."
-Hayley Roberts, MOD

Jake Williams *SANS Certified Instructor*

Jake Williams is a Principal Consultant at Rendition Infosec. He has more than a decade of experience in secure network design, penetration testing, incident response, forensics, and malware reverse engineering. Before founding Rendition Infosec, Jake worked with various cleared government agencies in information security roles. He is well versed in cloud forensics and previously developed a cloud forensics course for a U.S. government client. Jake regularly responds to cyber intrusions performed by state-sponsored actors in financial, defense, aerospace, and healthcare sectors using cutting-edge forensics and incident response techniques. He often develops custom tools to deal with specific incidents and malware reversing challenges. Additionally, Jake performs exploit development and has privately disclosed a multitude of zero day exploits to vendors and clients. He found vulnerabilities in one of the state counterparts to healthcare.gov and recently exploited antivirus software to perform privilege escalation. Jake developed Dropsmack, a pentesting tool (okay, malware) that performs command and control and data exfiltration over cloud file sharing services. Jake also developed an anti-forensics tool for memory forensics, Attention Deficit Disorder, that demonstrated weaknesses in memory forensics techniques. @MalwareJake

MGT414:

SANS Training Program for CISSP® Certification

SANS

Six-Day Program
Mon, Aug 22 - Sat, Aug 27
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: Jonathan Ham

www.giac.org/gisp

www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

"This course has been fantastic in terms of boiling down years of IT security trends and best practices into a week of learning."
-Eric Pavlov, InnoMark

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that has been specifically updated to prepare you to pass the 2016 version of the CISSP® exam.

Course authors Eric Conrad and Seth Misenar have revised MGT414 to take into account the 2016 updates to the CISSP® exam and prepare students to navigate all types of questions included in the new version.

MGT414 focuses solely on the eight domains of knowledge as determined by (ISC)^2 that form a critical part of the CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

Who Should Attend

- Security professionals who want to understand 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® eight domains
- Security professionals and managers looking for practical ways to apply the eight domains of knowledge to their current activities

You Will Be Able To:

- Understand the eight domains of knowledge that are covered on the CISSP® exam
- Analyze questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the eight domains of knowledge
- Apply the skills learned across the eight domains to solve security problems when you return to work

Obtaining Your CISSP® Certification Consists of:

- Fulfilling minimum requirements for professional work experience
- Completing the Candidate Agreement
- Review of your 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:
The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)^2.

Take advantage of the SANS CISSP® Get Certified Program currently being offered.
www.sans.org/cissp

Jonathan Ham *SANS Certified Instructor*

Jonathan is an independent consultant who specializes in large-scale enterprise security issues ranging from policy and procedure to staffing and training, 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, and from small startups to the Fortune 500. He's been commissioned to teach NCIS investigators how to use Snort, performed packet analysis from a facility more than 2,000 feet underground, and chartered and trained the CIRT for one of the largest U.S. federal agencies. He has 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. @jhamcorp

LEG523:

Law of Data Security and Investigations

SANS

Five-Day Program
Mon, Aug 22 - Fri, Aug 26
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Benjamin Wright

www.giac.org/gleg

www.sans.edu

Bundle OnDemand
with this course
www.sans.org/ondemand

"Outstanding instructor. Keep doing what you are doing!"
-Paul Mobley, FIS Global

"This course provided depth of subject and firmly reinforced facts and theory with case history. Very high impact combination."
-Mike Bando, U.S. National Park Service

- New for live delivery as of December 2015: The European Union's invalidation of the Privacy Safe Harbor for transferring data to the United States.
- Cyber insurer's lawsuit against hospital to deny coverage after data breach and $4.1 million legal settlement with patients.
- Target's and Home Depot's legal and public statements about payment card breaches.
- New legal tips on confiscating and interrogating mobile devices.
- Lawsuit by credit card issuers against Target's QSA and alleged security vendor, Trustwave.

Who Should Attend

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

New law on privacy, e-discovery and data security is creating an urgent need for professionals who can bridge the gap between the legal department and the IT department. SANS LEG523 provides this unique professional training, including skills in the analysis and use of contracts, policies and records management procedures.

This course covers the law of business, contracts, fraud, crime, IT security, liability and policy – all with a focus on electronically stored and transmitted records. It also teaches investigators how to prepare credible, defensible reports, whether for cyber crimes, forensics, incident response, human resource issues or other investigations.

Each successive day of this five-day course builds upon lessons from the earlier days in order to comprehensively strengthen your ability to help your public or private sector enterprise cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with IT security. We will cover recent stories ranging from Home Depot's legal and public statements about a payment card breach to the lawsuit by credit card issuers against Target's QSA and security vendor, Trustwave.

Recent updates to the course address hot topics such as legal tips on confiscating and interrogating mobile devices, the retention of business records connected with cloud computing and social networks like Facebook and Twitter, and analysis and response to the risks and opportunities surrounding open-source intelligence gathering.

Over the years this course has adopted an increasingly global perspective. Non-U.S. professionals attend LEG523 because there is no training like it anywhere else in the world. For example, a lawyer from the national tax authority in an African country took the course because electronic filings, evidence and investigations have become so important to her work. International students help the instructor, attorney Benjamin Wright, constantly revise the course and include more content that crosses borders.

Benjamin Wright *SANS Senior Instructor*

Benjamin Wright is a practicing attorney and 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 has been quoted in publications around the globe, from the *Wall Street Journal* to the *Sydney Morning Herald*. Mr. Wright is spotlighted in the book *The Devil Inside the Beltway* for his uncommonly insightful advice to LabMD in its now famous cybersecurity law dispute. In 2010, Russian banking authorities tapped him for experience and advice on the law of cyber investigations and electronic payments. He maintains a popular blog at http://hack-igations.blogspot.com. @benjaminwright

ICS410:
ICS/SCADA Security Essentials

SANS

Five-Day Program
Mon, Aug 22 - Fri, Aug 26
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Billy Rios

www.giac.org/gicsp

SANS Technology Institute
www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"The real-world relationship was key to applying the information. The instructor relates his experiences with the attacks."
-Taylor A., Marfor Cyber

"The course content is excellent! I've learned a lot and the course has rejuvenated my interest in ICS security."
-Marcel P. Ablog, San Roque Power

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. **ICS410: ICS/SCADA Security Essentials** provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

Who Should Attend

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

The course will provide you with:

- An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints
- Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals
- A license to Windows 10 and a hardware PLC for students to use in class and take home with them

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as industrial control system penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

When students complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their industrial control system environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

Billy Rios *SANS Instructor*

An accomplished author and speaker, Billy is recognized as one of the world's most respected experts on emerging threats related to industrial control systems (ICS), critical infrastructure (CI), and, medical devices. He has discovered thousands of security vulnerabilities in hardware and software supporting ICS and critical infrastructure. He has been publically credited by the Department of Homeland Security (DHS) over 50 times for his support to the DHS ICS Cyber Emergency Response Team (ICS-CERT). Billy was a Lead at Google, where he led the front line response to externally reported security issues and incidents. Prior to Google, Billy was the Security Program Manager at Internet Explorer (Microsoft). During his time at Microsoft, Billy led the company's response to several high-profile incidents, including the response for Operation Aurora. Before Microsoft, Billy worked as a penetration tester, an intrusion detection analyst, and served as an active duty Marine Corps Officer. Billy currently holds an MBA and a master's of science degree in information systems.. He was a contributing author for several publications including *Hacking, the Next Generation* (O'Reilly), *Inside Cyber Warfare* (O'Reilly), and *The Virtual Battle Field* (IOS Press). @XSSniper

SANS@NIGHT EVENING TALKS

Enrich your SANS training experience!

Evening talks 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:

Analysis of Destructive Cyber Attacks

Jake Williams

Destructive cyber attacks are devastating to organizations, which often struggle to recover after an event. In this talk, Jake will cover the history of destructive cyber attacks, potential motivations, warning signs, and trend analysis. We'll learn how to identify the signs of a destructive attack in your environment. Finally, we'll examine how organizations can prepare so they can effectively mitigate any destructive cyber attack in their environment.

Security Leadership for Everyone: Personal Authority and Beyond

Ted Demopoulos

Security leadership is not a role for only those in charge. A leader is anyone who has followers. Leaders may have followers because they are in a position of power, because they take the initiative, or perhaps simply because they set a good example and people follow their lead.

Leaders have followers because they have some sort of "authority." They may have "positional authority" because they are in charge, or because of their position or title. They may have "personal authority," authority that is earned through actions. Many leaders have both: positional authority because they are in charge and personal authority because they have earned respect through their actions.

In this presentation, part of the Infosec Rock Star series of talks, we look at leadership and authority, discussing both types of authority and concentrating on what it takes to establish personal authority in security.

Security leadership is not reserved for those "in charge" – personal authority can be earned by all of us.

The Dizzy New World of Cyber Investigations: Law, Ethics, and Evidence

Ben Wright

Increasingly, employers and enterprises are engaged in cyber investigations. The explosion of cyber evidence (email, text, meta data, social media, etc.) about every little thing anyone does or says creates a massive need for Human Resources departments, IT departments, internal audit departments, and other investigators to find and sift through this evidence. Surprises abound. These cyber investigations are guided, motivated, and restricted by a blizzard of new laws and court cases. Increasingly enterprises need professionals with backgrounds in cyber forensics, cyber law, and computer privacy.

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events www.sans.org/security-training/by-location/all
Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers

Community SANS www.sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

Private Training www.sans.org/private-training
Live Onsite Training at Your Office Location. Both In-person and Online Options Available

Mentor www.sans.org/mentor
Live Multi-Week Training with a Mentor

Summit www.sans.org/summit
Live IT Security Summits and Training

ONLINE TRAINING

OnDemand www.sans.org/ondemand
E-learning Available Anytime, Anywhere, at Your Own Pace

vLive www.sans.org/vlive
Online Evening Courses with SANS' Top Instructors

Simulcast www.sans.org/simulcast
Attend a SANS Training Event without Leaving Home

OnDemand Bundles www.sans.org/ondemand/bundles
Extend Your Training with an OnDemand Bundle Including Four Months of E-learning

FUTURE SANS TRAINING EVENTS

SANSFIRE 2016
Washington, DC | Jun 11-18

Digital Forensics & Incident Response SUMMIT & TRAINING 2016
Austin, TX | Jun 23-30

Salt Lake City 2016
Salt Lake City, UT | Jun 27 - Jul 2

Rocky Mountain 2016
Denver, CO | Jul 11-16

Minneapolis 2016
Minneapolis, MN | Jul 18-23

San Antonio 2016
San Antonio, TX | Jul 18-23

San Jose 2016
San Jose, CA | Jul 25-30

ICS Security Training – Houston 2016
Houston, TX | Jul 25-30

Boston 2016
Boston, MA | Aug 1-6

Security Awareness SUMMIT & TRAINING 2016
San Francisco, CA | Aug 1-10

Portland 2016
Portland, OR | Aug 8-13

Dallas 2016
Dallas, TX | Aug 8-13

Data Breach Summit
Chicago, IL | Aug 18

Virginia Beach 2016
Virginia Beach, VA | Aug 22 - Sep 2

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

SANS CHICAGO 2016

Hotel Information

Training Campus

The Palmer House Hilton

17 East Monroe Street
Chicago, IL 60603
800-445-8667

www.sans.org/event/chicago-2016/location

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.

Special Hotel Rates Available

A special discounted rate of $199.00 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 20, 2016.

Top 5 reasons to stay at The Palmer House Hilton

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 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 that you won't want to miss!
5. Everything is in one convenient location!

SANS CHICAGO 2016

Registration Information

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

Register online at www.sans.org/chicago

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.

Use code **EarlyBird16** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**6-29-16**	**$400.00**	**7-20-16**	**$200.00**

Some restrictions apply.

SANS Voucher Program

Expand your training budget!

Extend your fiscal year. The SANS Voucher Program provides flexibility and may earn you bonus funds for training.

www.sans.org/vouchers

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 3, 2016 – processing fees may apply.

Open a **SANS Portal Account** today to enjoy these FREE resources:

WEBCASTS

Ask The Expert Webcasts – SANS experts bring current and timely information on relevant topics in IT Security.

Analyst Webcasts – A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

WhatWorks Webcasts – The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.

Tool Talks – Tool Talks are designed to give you a solid understanding of a problem, and to show how a vendor's commercial tool can be used to solve or mitigate that problem.

NEWSLETTERS

NewsBites – Twice-weekly high-level executive summary of the most important news relevant to cybersecurity professionals

OUCH! – The world's leading monthly free security-awareness newsletter designed for the common computer user

@RISK: The Consensus Security Alert – A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data

OTHER FREE RESOURCES

- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQ
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

www.sans.org/security-resources