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

SANS Houston 2016

Houston, TX May 9-14

SANS OFFERS HANDS-ON, IMMERSION-STYLE SECURITY TRAINING COURSES TAUGHT BY REAL-WORLD PRACTITIONERS

"I not only learned security essentials but renewed and advanced my general IT skillset. I wish I had this training years ago.

-James Patzer,
Discover Financial Services

Protect your company and advance your career with these crucial courses:

- Network Penetration Testing & Ethical Hacking NEW!
- Security Essentials Bootcamp Style
- Hacker Tools, Techniques, Exploits & Incident Handling
- Continuous Monitoring and Security Operations
- Intrusion Detection In-Depth
- Windows Forensic Analysis
- IT Project Management, Effective Communication, and PMP® Exam Prep
- Law of Data Security and Investigations

GIAC Approved Training

Save $400
by registering early!
See page 13 for more details.

REGISTER AT sans.org/houston-2016

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 become SANS instructors. This guarantees that what you learn in class will be up-to-date and relevant to your job. The SANS Houston 2016 line-up of instructors includes:

David Cowen
SANS Instructor

Adrien de Beaupre
Certified Instructor

Ted Demopoulos
Certified Instructor

Jeff Frisk
Certified Instructor

Bryce Galbraith
Principal Instructor

Jonathan Ham
Certified Instructor

Johannes Ullrich, PhD
Senior Instructor

Benjamin Wight
Senior Instructor

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 9.

How to Bring Some Advanced Persistent Trickery to Your Fight Against Advanced Persistent Threats – Bryce Galbraith

Automating Correlation with DFIR, Python, and ElasticSearch – David Cowen

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

Complete Web Application Pwnage via Multi-POST XSRF – Adrien de Beaupre

Instant Expert: Legitimately and Ethically – Ted Demopoulos

Be sure to register and pay by March 16th for a $400 tuition discount!

Courses-at-a-Glance

SEC401:
Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, May 9 - Sat, May 14
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Ted Demopoulos

- GIAC Cert: GSEC
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

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!*

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

With the advanced persistent threat, 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.

AVAILABLE VIA SIMULCAST
sans.org/simulcast

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

"SEC401 was an excellent introduction to networking security fundamentals that every IT person should attend."
-Fawad Sami, Vermilian

GSEC
giac.org

SANS Technology Institute
sans.edu

sans.org/cyber-guardian

sans.org/8570

Bundle OnDemand
with this course
sans.org/ondemand

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. 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 also a food and wine geek, enjoys flyfishing, and plays with his children. @TedDemop

SEC503:
Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, May 9 - Sat, May 14
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor:
Johannes Ullrich, PhD

- GIAC Cert: GCIA
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

Reports of prominent organizations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?

Who Should Attend

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

SEC503: Intrusion Detection In-Depth delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to configure and master different open-source tools like tcpdump, Wireshark, Snort, Bro, and many more. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material. In addition, most exercises include an "extra credit" stumper question intended to challenge even the most advanced student.

Industry expert Mike Poor has created a VMware distribution, Packetrix, specifically for this course. As the name implies, Packetrix contains many of the tricks of the trade to perform packet and traffic analysis. It is supplemented with demonstration "pcaps," which are files that contain network traffic. This allows students to follow along on their laptops with the class material and demonstrations. The pcaps also provide a good library of network traffic to use when reviewing the material, especially for certification.

Preserving the security of your site in today's threat environment is more challenging than ever before. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and often vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in **SEC503: Intrusion Detection In-Depth** is to acquaint you with the core knowledge, tools, and techniques to defend your networks. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

AVAILABLE VIA SIMULCAST
sans.org/simulcast

"The threats to our businesses and government agencies are ever increasing. We need to focus our IDS/IPS on our critical data and SEC503 helps us achieve that."
-Ed Brewster, SAIC, Inc.

"SEC503 covers the best processes for intrusion analysis, how to cut out most of the network noise, and identify the important traffic."
-Mike Boya, Warner Bros.

GCIA
giac.org

SANS Technology Institute
sans.edu

sapere aude
sans.org/cyber-guardian

sans.org/8570

Bundle OnDemand
with this course
sans.org/ondemand

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

As Dean of Research for the SANS Technology Institute, Johannes is currently responsible for the SANS Internet Storm Center (ISC) and the GIAC Gold program. He founded DShield.org in 2000, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. Prior to joining 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 based in Jacksonville, Florida. His daily podcast summarizes current security news in a concise format. @johullrich

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, May 9 - Sat, May 14
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Bryce Galbraith

- GIAC Cert: GCIH
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

sans.org/simulcast

"This training gives you the knowledge to think like an attacker, and it better equips you to defend your networks."
-Sheryll Tiauzon, Coca-Cola Company

"This course helped me fill in the finer details and gaps in my knowledge. I understood the higher level concepts. I have worked with a few of the tools but this helped put it all together."
-Jenna Esparza, Los Alamos National Laboratory

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
- 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

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, this course helps you turn the tables on computer attackers. It addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course 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, 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 for, exploiting, and defending systems. It 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.

giac.org

sans.edu

sans.org/
cyber-guardian

sans.org/8570

Bundle OnDemand
with this course
sans.org/ondemand

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. Bryce 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 around the world. @brycegalbraith

SEC511:

Continuous Monitoring and Security Operations

New in 2016! Extended-Hours Bootcamp to Enhance Your Skills

SANS

Six-Day Program
Mon, May 9 - Sat, May 14
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Laptop Required
Instructor: Jonathan Ham

- GIAC Cert: GMON
- Master's Program
- OnDemand Bundle

AVAILABLE VIA SIMULCAST

sans.org/simulcast

"SEC511 delivers the practical methodologies and granular information that can help bridge the communications gaps that may exist between analysts, engineers, and operations."
-Patrick Nolan, Intel Security Foundstone

"[SEC511] develops very practical skills as opposed to theoretical. I can go back to work and actually use this."
-Charles Hill, SEC

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying to prevent and combat cyber attacks, but despite this tremendous effort organizations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses.

The underlying challenge for organizations victimized by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organizations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach is early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

Who Should Attend

- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center (SOC) analysts
- SOC engineers
- SOC managers
- CND analysts
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)

GMON

giac.org

SANS Technology Institute

sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Jonathan Ham *SANS Certified Instructor*

Jonathan is an independent consultant who specializes in large-scale enterprise security issues 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 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 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

SEC560:

Network Penetration Testing and Ethical Hacking

NEW

SANS

Six-Day Program
Mon, May 9 - Sat, May 14
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Adrien de Beaupre

- GIAC Cert: GPEN
- Cyber Guardian
- STI Master's Program
- OnDemand Bundle

AVAILABLE VIA SIMULCAST

sans.org/simulcast

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red and blue team members
- Forensics specialists who want to better understand offensive tactics

"SEC560 has helped me have a more in-depth knowledge of penetration testing. The instructor's flow and method made it easier to understand."
-Mithra Ravendran, BAE Systems Applied Intelligence

As a cybersecurity professional, you have a unique responsibility to find and understand your organization's vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this task head-on.

SEC560 is the must-have course for every well-rounded security professional.

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step-by-step and end-to-end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with over 30 detailed hands-on labs throughout. The course is chock full of practical, real-world tips from some of the world's best penetration testers to help you do your job safely, efficiently…and masterfully.

Learn the best ways to test your own systems before the bad guys attack.

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test – and on the last day of the course you'll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the knowledge you've mastered in this course.

This course equips security organizations with comprehensive penetration testing and ethical hacking know-how.

You will learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover run-of-the-mill options and configurations, we'll also go over the lesser-known but super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.

GPEN
giac.org

SANS Technology Institute
sans.edu

sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Adrien de Beaupre *SANS Certified Instructor*

Adrien de Beaupre works as an independent consultant in beautiful Ottawa, Ontario. His work experience includes technical instruction, vulnerability assessment, penetration testing, intrusion detection, incident response and forensic analysis. He is a member of the SANS Internet Storm Center (isc.sans.edu). He is actively involved with the information security community, and has been working with SANS since 2000. Adrien holds a variety of certifications including the GXPN, GPEN, GWAPT, GCIH, GCIA, GSEC, CISSP, OPST, and OPSA. When not geeking out he can be found with his family, or at the dojo. @adriendb

FOR408:
Windows Forensic Analysis

SANS

Six-Day Program
Mon, May 9 - Sat, May 14
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: David Cowen

- GIAC Cert: GCFE
- STI Master's Program
- OnDemand Bundle

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

DFIR
digital-forensics.sans.org

"Awesome content, awesome instructor! Everyone needs this course, not just forensics, but any security personnel."
-Thomas Farley, Raytheon

"I like the fact that the whole course is centered around the same data and that there is so much data available. I can't wait to try this out at work!"
-Greg Dub, National Center for Policy Analysis

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 for validating security tools, enhancing vulnerability assessments, identifying insider threats, tracking hackers, and improving 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.

GCFE
giac.org

SANS Technology Institute
sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

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

David Cowen *SANS Instructor*

David Cowen is a Partner at G-C Partners, LLC, where his team of expert digital forensics investigators pushes the boundaries of what is possible on a daily basis. He has been working in digital forensics and incident response since 1999 and has performed investigations covering thousands of systems in the public and private sectors. Those investigations have involved everything from revealing insider threats to serving as an expert witness in civil litigation and providing the evidence to put cyber criminals behind bars. David has authored three series' of books on digital forensics: *Hacking Exposed Computer Forensics* (1st-3rd editions); *Infosec Pro Guide to Computer Forensics*; and the *Anti Hacker Toolkit* (Third Edition). His research into file system journaling forensics has created a new area of analysis that is changing the industry. Combined with Triforce products, David's research enables examiners to go back in time to find previously unknown artifacts and system interactions. @hecfblog

MGT525:

IT Project Management, Effective Communication, and PMP® Exam Prep

SANS

Six-Day Program
Mon, May 9 - Sat, May 14
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jeff Frisk

- GIAC Cert: GCPM
- STI Master's Program

Recently updated to fully prepare you for the 2016 PMP® Exam, **SANS MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep** is a PMI Registered Education Provider (R.E.P.). R.E.P.s provide the training necessary to earn and maintain the Project Management Professional (PMP®) and other professional credentials. During this class you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. We will utilize project case studies that highlight information technology services as deliverables. MGT525 follows the basic project management structure from the *PMBOK® Guide* (Fifth Edition) and also provides specific techniques for success with information assurance initiatives. Throughout the week, we will cover all aspects of IT project management – from initiating and planning projects to managing cost, time, and quality while your project is active, and completing, and closing, and then documenting as your project finishes. A copy of the *PMBOK® Guide* (Fifth Edition) is provided to all participants. You can reference the guide and use your course material along with the knowledge you gain in class to prepare for the 2016 updated PMP® Exam and the GIAC Certified Project Manager Exam.

Who Should Attend

- Individuals who need to prepare for the Project Management Professional (PMP®) Exam
- Security professionals who are interested in understanding the concepts of IT project management
- Managers who want to understand the critical areas of making projects successful
- Individuals working with time, cost, quality, and risk-sensitive projects and applications
- Anyone who would like to utilize effective communication techniques and proven methods to relate better to people
- Anyone in a key or lead engineering/design position who works regularly with project management staff

"Honestly, this is one of the best courses I have had to date. I feel like I have thousands of things to take back to my job."
-Ryan Spencer, Reed Elsevier

"[MGT525] helped me bridge the gap between my technical background and my future PM duties."
-Stacie Packard, GCI

The project management process is broken down into core process groups that can be applied across multiple areas of any project, in any industry. Although our primary focus is the application to the InfoSec industry, our approach is transferable to any projects that create and maintain services as well as general product development. We cover in-depth how cost, time, quality, and risks affect the services we provide to others. We will also address practical human resource management as well as effective communication and conflict resolution. You will learn specific tools to bridge the communications gap between managers and technical staff.

GCPM
giac.org

SANS Technology Institute
sans.edu

Jeff Frisk *SANS Certified Instructor*

Jeff Frisk currently serves as the director of the GIAC certification program and is a member of the STI Curriculum Committee. Jeff holds the PMP® certification from the Project Management Institute and GIAC GSEC credentials. He also is the course author for MGT525. He has worked on many projects for SANS and GIAC, including courseware, certification, and exam development. Jeff has an engineering degree from the Rochester Institute of Technology and more than 15 years of IT project management experience with computer systems, high-tech consumer products, and business development initiatives. Jeff has held various positions including managing operations, product development, and electronic systems/computer engineering. He has many years of international and high-tech business experience working with both big and small companies to develop computer hardware/software products and services.

LEG523:

Law of Data Security and Investigations

SANS

Five-Day Program
Mon, May 9 - Fri, May 13
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Benjamin Wright

- GIAC Cert: GLEG
- STI Master's Program
- OnDemand Bundle

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

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.

Who Should Attend

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

"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

GLEG
giac.org

SANS Technology Institute
sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

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

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.

How to Bring Some Advanced Persistent Trickery to Your Fight Against Advanced Persistent Threats

Bryce Galbraith

You know you have intruders in your house...but this is your house and no one knows it better than you. Don't sit back and wait. It's game on! This presentation will explore ways that you can frustrate, annoy, and potentially reveal advanced persistent threats with active defense, offensive countermeasures and cyber deception – and how to do it legally and ethically.

Automating Correlation with DFIR, Python, and ElasticSearch

David Cowen

How do you start correlating forensic artifacts from multiple sources when no one tool will give you everything you need? In this talk you will see what can be done when you start centralizing reports from all your favorite tools to help you correlate artifacts via indexing with Elastic and some python scripting. You'll be able to quickly identify what was exfiltrated via external devices, the history of a given file, recent activity, and more.

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 HR 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. Enterprises increasingly need professionals with backgrounds in cyber forensics, cyber law, and computer privacy.

Complete Web Application Pwnage via Multi-POST XSRF

Adrien de Beaupre

This talk will discuss the risk posed by Cross-site Request Forgery (XSRF), which is also known as session riding or transaction injection. Many applications are vulnerable to XSRF, and mitigation is difficult because it often requires re-engineering the entire application, and because the threat posed by XSRF is often misunderstood. The presentation will feature a live demo that identifies the vulnerability and exploits it by performing multiple unauthorized transactions in a Multi-POST attack.

Instant Expert: Legitimately and Ethically

Ted Demopoulos

This presentation is part of the InfoSec Rock Star Series of talks. We naturally build expertise with experience, but we don't necessarily build "expert status." What are some of the reasons to develop this expert status?

- Expert status gives you more influence
- People listen to experts readily
- Experts can make a bigger and more positive impact
- Experts are well paid
- Experts have a lot of flexibility to follow their passions in life

Even the mere concept of what constitutes an expert confuses most people. An expert is defined as "a person with extensive knowledge or ability," which means that this person knows significantly more than others. It is a relative term, however. It doesn't mean #1 Expert in the world. It doesn't mean there is nothing else left to learn. Chances are that you are already an expert on several topics. In this talk we examine exactly what an expert is, and the multiple ways to quickly, legitimately, and yes, sometimes even nearly instantly, develop expert status.

Build Your Best Career

WITH:

SANS

Add an

OnDemand Bundle & GIAC Certification Attempt

to your course within seven days of this event for just $659 each.

SPECIAL PRICING

OnDemand Bundle

- Four months of supplemental online review
- 24/7 online access to your course lectures, materials, quizzes, and labs
- Subject-matter expert support to help you increase your retention of course material

"The course content and OnDemand delivery method have both exceeded my expectations."

-Robert Jones, Team Jones, Inc.

GIAC Certification

- Distinguish yourself as an information security leader
- 30+ GIAC certifications to choose from
- Two practice exams included
- Four months of access to complete the attempt

"GIAC is the only certification that proves you have hands-on technical skills."

-Christina Ford, Department of Commerce

MORE INFORMATION

www.sans.org/ondemand/bundles www.giac.org

*GIAC and OnDemand Bundles are only available for certain courses.

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events 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 sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

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

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

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

ONLINE TRAINING

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

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

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

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

FUTURE SANS TRAINING EVENTS

NORTHERN VIRGINIA
McLean 2016
McLean, VA | Feb 15-20

ICS Security
SUMMIT & TRAINING 2016
Orlando, FL | Feb 16-23

Anaheim 2016
Anaheim, CA | Feb 22-27

RSA Conference 2016
San Francisco, CA | Feb 28-29

Philadelphia 2016
Philadelphia, PA | Feb 29 - Mar 5

SANS 2016
Orlando, FL | Mar 12-21

Reston 2016
Reston, VA | Apr 4-9

Atlanta 2016
Atlanta, GA | Apr 4-9

Threat Hunting and Incident Response
SUMMIT & TRAINING 2016
New Orleans, LA | Apr 12-19

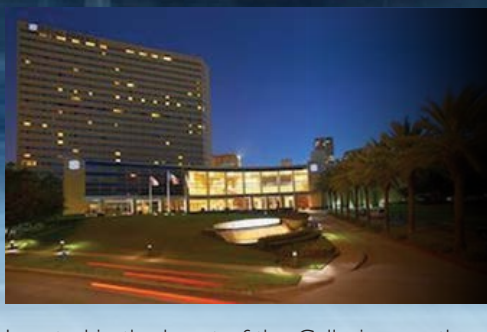
Pen Test Austin 2016
Austin, TX | Apr 18-23

Security West 2016
San Diego, CA | April 29 - May 6

Baltimore Spring 2016
Baltimore, MD | May 9-14

Security Operations Center
SUMMIT & TRAINING 2016
Crystal City, VA | May 19-26

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



SANS HOUSTON 2016

Hotel Information

Training Campus

Royal Sonesta Hotel Houston

2222 West Loop South
Houston, TX 77027
713-627-7600
sans.org/event/houston-2016/location

Located in the heart of the Galleria area, the newly renovated, AAA-rated Four Diamond Royal Sonesta Hotel Houston is in the shopping, dining, and entertainment hub of Uptown Houston. It is conveniently positioned near key destinations including downtown Houston, the Museum and Theater districts, and Reliant Park.

Special Hotel Rates Available

A special discounted rate of $189.00 S/D will be honored based on space availability.
Should the prevailing government per diem rate fall below the SANS group rate, government per diem rooms will be made 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 April 18, 2016.

Top 5 reasons to stay at the Royal Sonesta Hotel Houston

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

SANS HOUSTON 2016

Registration Information

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

Register online at sans.org/houston-2016/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.

Use code **EarlyBird16** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**3-16-16**	**$400.00**	**4-6-16**	**$200.00**

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 sans.org/security-training/discounts prior to registering.

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 April 20, 2016 – 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.
sans.org/vouchers

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)

sans.org/security-resources

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

BROCHURE CODE

Save $400 when you pay for any long course and enter the code "EarlyBird16" before March 16th.