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

SANS Minneapolis 2017

June 19-24

PROTECT YOUR COMPANY AND ADVANCE YOUR CAREER
WITH HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Eight courses in:

CYBER DEFENSE
PENETRATION TESTING
MOBILE DEVICE SECURITY
SECURE DEVELOPMENT
ETHICAL HACKING
MANAGEMENT | LEGAL

SAVE $400

Register and pay by April 26th – Use code **EarlyBird17**

GIAC CERTIFICATIONS

GIAC-Approved Training

"SANS training is very relevant to today's technologies. The skills I have learned I will be able to take back and use in the office."

-David Smith, ManTech International

SANS NETWARS EXPERIENCE

www.sans.org/minneapolis

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 Minneapolis 2017 lineup of instructors includes:

Adrien de Beaupre
Certified Instructor
@adriendb

Ted Demopoulos
Principal Instructor
@TedDemop

Bryce Galbraith
Principal Instructor
@brycegalbraith

G. Mark Hardy
Certified Instructor
@g_mark

David Mashburn
Instructor
@d_mashburn

Tim Medin
Certified Instructor
@timmedin

Dr. Johannes Ullrich
Senior Instructor
@johullrich

Benjamnen Wright
Senior Instructor
@benjaminwright

Evening Bonus Sessions

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

KEYNOTE: ***Infosec Rock Star: Geek Will Only Get You So Far***
Ted Demopoulos

Anti-Ransomware: How to Turn the Tables
G. Mark Hardy

Color My Logs: Understanding the Internet Storm Center
Johannes Ullrich

You've Got Ransomeware! Managing the Legal Risk of Cyber Fraud
Benjamin Wright

Save $400 when you register and pay by April 26th using code EarlyBird17

Courses at a Glance

	MON 6-19	TUE 6-20	WED 6-21	THU 6-22	FRI 6-23	SAT 6-24
SEC401 Security Essentials Bootcamp Style	Page 1					
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	Page 2					
SEC560 Network Penetration Testing and Ethical Hacking	Page 3					
SEC575 Mobile Device Security and Ethical Hacking	Page 4					
MGT512 SANS Security Leadership Essentials for Managers with Knowledge Compression™	Page 5					
MGT514 IT Security Strategic Planning, Policy, and Leadership	Page 6					
LEG523 Law of Data Security and Investigations	Page 7					
DEV522 Defending Web Applications Security Essentials	Page 8					
Core NetWars Experience				Page 11		

SEC401

Security Essentials Bootcamp Style

GSEC Certification
Security Essentials

www.giac.org/gsec

Six-Day Program
Mon, June 19 - Sat, June 24
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Bryce Galbraith

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
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic specialists, penetration testers, and auditors who need a solid foundation of security principles to be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

"Everyone in cyber should attend this course because it covers many aspects of security and emerging trends."
-Pamela Livingston-Spruill, DOE/NNSA

This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. You'll 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.

STOP and ask yourself the following questions:

- **Do you fully understand why some organizations get compromised and others do not?**
- **If there were compromised systems on your network, are you confident that you would be able to find them?**
- **Do you know the effectiveness of each security device and are you certain that they are all configured correctly?**
- **Are proper security metrics set up and communicated to your executives to drive security decisions?**

If you do not know the answers to these questions, SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

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. Our 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 rise in 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 will 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.

SANS Technology Institute
www.sans.edu

www.sans.org/8140

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

Bryce Galbraith *SANS Principal Instructor*

As a contributing author of the internationally bestselling book *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, he was a member of Foundstone's renowned penetration testing team, and he 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**

SEC504

Hacker Tools, Techniques, Exploits, and Incident Handling

GCIH Certification
Incident Handler

www.giac.org/gcih

Six-Day Program
Mon, June 19 - Sat, June 24
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: David Mashburn

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

"SANS offers very valuable, practical training which makes it possible to return to the workplace and immediately implement improvements and strategies."

-Jill Stuart, Reserve Bank of Australia

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.

"[This course is a] good foundation for security incidents. It's a must-have for security incident handlers/managers."

-Wu Peihui, Citibank

This course enables you to turn the tables on computer attackers by helping you understand their 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. 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 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. **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.

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

www.sans.org/8140

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

David Mashburn *SANS Instructor*

David Mashburn is currently the IT Security Manager for a global non-profit organization in the Washington, D.C. area. He also has experience working as an IT security professional for several civilian federal agencies, and over 15 years of experience in IT. He holds a masters degree in computer science from John Hopkins University, and a B.S. from the University of Maryland at College Park. David holds multiple security-related certifications, including CISSP, GPEN, GCIH, GCIA, and CEH. He is also a member of the SANS/GIAC Advisory Board, and has previously taught courses in the cybersecurity curriculum at the University of Maryland – University College. @d_mashburn

SEC560

Network Penetration Testing and Ethical Hacking

GPEN Certification
Penetration Tester

www.giac.org/gpen

Six-Day Program
Mon, June 19 - Sat, June 24
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Adrien de Beaupre

Who Should Attend

- Security personnel whose jobs involve 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

"Commercial tools are something I wish I knew more of and this course is teaching me just that, plus I'm learning from someone who has massive amounts of real-world experience."

-Travis Peska, Mantech

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 more than 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.

You will bring comprehensive penetration testing and ethical hacking know-how back to your organization.

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.

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

Bundle OnDemand
WITH THIS COURSE
www.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**

SEC575

Mobile Device Security and Ethical Hacking

GMOB Certification
Mobile Device Security Analyst
www.giac.org/gmob

Six-Day Program
Mon, June 19 - Sat, June 24
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Tim Medin

Who Should Attend

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

"SEC575 provides a pretty comprehensive overview of different attack vectors and vulnerabilities in the mobile field. It covers many topics in enough depth to really get a foothold in the subject. I wish I had taken this course several years ago when first entering the mobile landscape."
-Jeremy Erickson, Sandia National Lab

SANS Technology Institute
www.sans.edu

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

Imagine an attack surface spread throughout your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports numerous different wireless technologies all ripe for attack. You don't need to imagine any further because this already exists today: **mobile devices**. These devices are the biggest attack surface in most organizations, yet these same organizations often don't have the skills needed to assess them.

Mobile devices are no longer a convenience technology: they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores throughout the world. Users rely on mobile devices more today than ever before – we know it, and the bad guys do too.

This course is designed to give you the skills you need to understand the security strengths and weaknesses in Apple iOS, Android, and wearable devices including Apple Watch and Android Wear. With these skills, you will evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption, and how to manipulate Android apps to circumvent obfuscation techniques. You'll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You'll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS devices, and you'll exploit lost or stolen devices to harvest sensitive mobile application data.

Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you'll review the ways in which we can effectively communicate threats to key stakeholders. You'll leverage tools including Mobile App Report Cards to characterize threats for management and decision-makers, while identifying sample code and libraries that developers can use to address risks for in-house applications as well.

You'll then use your new skills to apply a mobile device deployment penetration test in a step-by-step fashion. Starting with gaining access to wireless networks to implement man-in-the-middle attacks and finishing with mobile device exploits and data harvesting, you'll examine each step in conducting such a test with hands-on exercises, detailed instructions, and tips and tricks learned from hundreds of successful penetration tests. By building these skills, you'll return to work prepared to conduct your own test, and you'll be better informed about what to look for and how to review an outsourced penetration test.

Mobile device deployments introduce new threats to organizations including advanced malware, data leakage, and the disclosure of enterprise secrets, intellectual property, and personally identifiable information assets to attackers. Further complicating matters, there simply are not enough people with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you'll be able to differentiate yourself as being prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test – all critical skills to protect and defend mobile device deployments.

Tim Medin *SANS Certified Instructor*

Tim Medin is a Senior Technical Analyst at Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through the course of his career, Tim has performed penetration tests on a wide range of organizations and technologies. Prior to Counter Hack, Tim was a Senior Security Consultant for FishNet Security, where most of his focus was on penetration testing. He gained information security experience in a variety of industries, including previous positions in control systems, higher education, financial services, and manufacturing. Tim regularly contributes to the SANS Penetration Testing Blog (**pen-testing.sans.org/blog**) and the Command Line Kung Fu Blog (blog.commandlinekungfu.com). He is also project lead for the Laudanum Project, a collection of injectable scripts designed to be used in penetration testing. **@timmedin**

MGT512

GSLC Certification
Security Leadership

www.giac.org/gslc

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program
Mon, June 19 - Fri, June 23
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop Recommended
Instructor: Ted Demopoulos

Who Should Attend

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

"MGT512 is one of the most valuable courses I've taken with SANS. It really did help bridge the gap from security practitioner to security orchestrator. Truly a gift!"

-John Madick, Epiq Systems, Inc.

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

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

Knowledge Compression™

Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class that aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

SANS Technology Institute
www.sans.edu

www.sans.org/8140

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

Ted Demopoulos *SANS Principal 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 playing with his children. **@TedDemop**

MGT514

GIAC CERTIFICATION COMING SOON!

IT Security Strategic Planning, Policy, and Leadership

Five-Day Program
Mon, June 19 - Fri, June 23
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: G. Mark Hardy

Who Should Attend

- CISOs
- Information security officers
- Security directors
- Security managers
- Aspiring security leaders
- Other security personnel who have team lead or management responsibilities

"I moved into management a few years ago and am currently working on a new security strategy/ roadmap and this class just condensed the past two months of my life into a one-week course and I still learned a lot!"
-Travis Evans, SiriusXM

SANS Technology Institute
www.sans.edu

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

As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to do three things:

• Develop Strategic Plans
Strategic planning is hard for people in IT and IT security because we spend so much time responding and reacting. We almost never get to practice until we get promoted to a senior position and then we are not equipped with the skills we need to run with the pack. Learn how to develop strategic plans that resonate with other IT and business leaders.

• Create Effective Information Security Policy
Policy is a manager's opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and your response was, "No way, I am not going to do that!"? Policy must be aligned with an organization's culture. We will break down the steps to policy development so that you have the ability to develop and assess policy to successfully guide your organization.

• Develop Management and Leadership Skills
Leadership is a capability that must be learned, exercised and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organization's mission. Learn to utilize management tools and frameworks to better lead, inspire, and motivate your teams.

How the Course Works

Using case studies from Harvard Business School, team-based exercises, and discussions that put students in real-world scenarios, students will participate in activities that they can then carry out with their own team members when they return to work.

The next generation of security leadership must bridge the gap between security staff and senior leadership by strategically planning how to build and run effective security programs. After taking this course you will have the fundamental skills to create strategic plans that protect your company, enable key innovations, and work effectively with your business partners.

G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and president of the National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. He serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 sailors. He also served as wartime Director, Joint Operations Center for U.S. Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for InfoSec, public key infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he holds a bachelor's degree in computer science, BA in mathematics, masters in business administration, and a masters in strategic studies, and holds the GSLC, CISSP, CISM, and CISA certifications. **@g_mark**

LEG523

Law of Data Security and Investigations

GLEG Certification
Law of Data Security & Investigations
www.giac.org/gleg

Five-Day Program
Mon, June 19 - Fri, June 23
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Benjamin Wright

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 changed the way I think about legal issues in the workplace and at home."
-Jon Mark Allen, Gamestop

SANS Technology Institute
www.sans.edu

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

NEW!

- **EU's new General Data Protection Regulation and its impact around the world.**
- **The impact of Trump presidency and Brexit on data security law and regulatory enforcement.**
- **The EU's adoption of "Privacy Shield" to replace "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.**

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 fraud, crime, policy, contracts, liability, IT security and active defense – 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 enterprise (public or private sector) cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with IT security.

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, U.S. attorney Benjamin Wright, constantly revise the course and include more content that crosses borders.

"I have gained many valuable ideas and tools to support and defend my organization and to strengthen security overall. I wish I'd taken LEG523 3-4 years ago."
-Tom S., Case Western Reserve Univ.

Benjamin Wright *SANS Senior Instructor*

Benjamin Wright is the author of several technology law books, including *Business Law and Computer Security*, published by the SANS Institute. With 26 years in private law practice, he has advised many organizations, large and small, on privacy, e-commerce, computer security, and e-mail discovery and has been quoted in publications around the globe, from the *Wall Street Journal* to the *Sydney Morning Herald*. He is known for spotting and evaluating trends, such as the rise of whistleblowers wielding small video cameras. In 2010, Russian banking authorities tapped him for experience and advice on the law of cyber investigations and electronic payments. **@benjaminwright**

DEV522

Defending Web Applications Security Essentials

GWEB Certification
Security Leadership

www.giac.org/gweb

Six-Day Program
Mon, June 19 - Sat, June 24
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Johannes Ullrich, Ph.D.

Who Should Attend

- Application developers
- Application security analysts or managers
- Application architects
- Penetration testers who are interested in learning about defensive strategies
- Security professionals who are interested in learning about web application security
- Auditors who need to understand defensive mechanisms in web applications
- Employees of PCI compliant organizations who need to be trained to comply with PCI requirements

"DEV522 is absolutely necessary to all techies who work on web applications. I do not think developers understand the great necessity of web security and why it is so important."

-Mahesh Kandru, Cabela's

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

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

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

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding-level implementation.

DEV522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting web applications. It is particularly well suited to application security analysts, developers, application architects, pen testers, auditors who are interested in recommending proper mitigations for web security issues, and infrastructure security professionals who have an interest in better defending their web applications.

The course will also cover additional issues the authors have found to be important in their day-to-day web application development practices. The topics that will be covered include:

- **Infrastructure security**
- **Server configuration**
- **Authentication mechanisms**
- **Application language configuration**
- **Application coding errors like SQL injection and cross-site scripting**
- **Cross-site request forging**
- **Authentication bypass**
- **Web services and related flaws**
- **Web 2.0 and its use of web services**
- **XPATH and XQUERY languages and injection**
- **Business logic flaws**
- **Protective HTTP headers**

The course will make heavy use of hands-on exercises and conclude with a large defensive exercise that reinforces the lessons learned throughout the week.

SANS Technology Institute
www.sans.edu

Bundle OnDemand
WITH THIS COURSE
www.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. In 2000, he founded DShield.org, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. Prior to working for SANS, Johannes worked as a lead support engineer for a web development company and as a research physicist. Johannes holds a PhD in physics from SUNY Albany and is based in Jacksonville, Florida. His daily podcast summarizes current security news in a concise format. **@johullrich**

Bonus Sessions

Enrich your SANS training experience! SANS@Night 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.

Infosec Rock Star: Geek Will Only Get You So Far

Ted Demopoulos

This presentation is based on the recently published book of the same title. Some of us are so effective, and well known, that the term "rock star" is entirely accurate. What kind of skills do Rock Stars have and wannabe Rock Stars need to develop? Although we personally may never be swamped by groupies, we can learn the skills to be more effective, well respected, and well paid. Obviously it's not just about technology; in fact most of us are very good at the technology part. Although the myth of the geek with zero social skills is just that – a myth – the fact is that increasing our skills on the social and business side will make most of us more effective at what we do than learning how to read hex better while standing on our heads, becoming "one with metasploit," or understanding the latest hot technologies.

Drawing on the expertise of the real Rock Stars of InfoSec, the topics for this talk will include:

- The 5 Levels to Rock Star
- Positioning – why "they" don't like us or security and what we can do about it.
- The Science of Influence - ruthless social engineering or effective professional skills?
- Getting Things Done – Brutal Time Management and The Art of Saying "No" without upsetting too many people.
- How to let people know you rock – You might be the best in the world, but if no one knows it you're not going to do much good.

Anti-Ransomware: How to Turn the Tables

G. Mark Hardy

"OMG! We just got hit with ransomware!" What you don't usually hear next is, "LOL!" You can build defenses that prevent ransomware from paralyzing your organization – we'll show you how. Ransomware is a billion dollar industry, and it's growing tremendously. Lost productivity costs far more than the average ransom, so executives just say, "Pay the darn thing." But what if you could stop ransomware in its tracks? We'll demonstrate tools and methodologies that are battle-proven and ACTUALLY WORK as evidenced by fully contained ransomware "explosions" that went nowhere. We'll offer insights into the future of this attack vector, and venture predictions on how this industry will evolve and what to expect next.

Color My Logs: Understanding the Internet Storm Center

Johannes Ullrich, Ph.D.

The Internet Storm Center is a global collaborative information security community. Founded originally in 1999 as incidents.org, the Internet Strom Center in collaboration with DShield is a unique open resource to explore global threats, understand the attack "background radiation" and find more context for events you may be investigating. The Internet Storm Center offers several data feeds, APIs and tools to help you add "color" to your events, and to allow you to share data easily. You will learn how to use these data feeds and how to integrate them into your tools. You will also learn how to collaborate and contribute to the Internet Storm Center's data collection and how to give back to our global information security community.

You've Got Ransomeware! Managing the Legal Risk of Cyber Fraud

Benjamin Wright

Today most fraud has a cyber component, and most fraud investigations involve digital evidence. Cyber fraud like ransomware can trigger a legal crisis for your firm or your client. Mr. Wright will share insights on how to manage the legal risk. He will examine legal measures such as disclaimers, cyber insurance and invocation of attorney confidentiality rules.

Enhance Your Training Experience

Add an
OnDemand Bundle & GIAC Certification Attempt* to your course within seven days of this event for just $689 each.

SPECIAL PRICING

Extend Your Training Experience with an 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.

Get Certified with GIAC Certifications

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- 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

Whether you choose to attend a training class live or online, the entire SANS team is dedicated to ensuring your training experience exceeds expectations.

Live Classroom Instruction

Premier Training Events

Our most recommended format, live SANS training events deliver SANS' top instructors teaching multiple courses at a single time and location. This allows for:

- Focused, immersive learning without the distractions of your office environment
- Direct access to SANS Certified instructors
- Interacting with and learning from other professionals
- Attending SANS@Night events, NetWars tournaments, vendor presentations, industry receptions, and many other activities

Our premier live training events in North America, serving thousands of students, are held in Orlando, Washington DC, Las Vegas, New Orleans, and San Diego. Regional events with hundreds of students are held in most major metropolitan areas during the year. See page 12 for upcoming Training Events in North America.

Summits

SANS Summits focus one or two days on a single topic of particular interest to the community. Speakers and talks are curated to ensure the greatest applicability to participants.

Community SANS Courses

Same SANS courses, courseware, and labs, taught by up-and-coming instructors in a regional area. Smaller classes allow for more extensive instructor interaction. No need to travel; commute each day to a nearby location.

Private Classes

Bring a SANS Certified instructor to your location to train a group of your employees in your own environment. Save on travel and address sensitive issues or security concerns in your own environment.

Online Training

SANS Online successfully delivers the same measured learning outcomes to students at a distance that we deliver live in classrooms. More than 30 courses are available for you to take whenever or wherever you want. Thousands of students take our courses online and achieve certification each year.

Top reasons to take SANS courses online:

- Learn at your own pace, over four months
- Spend extra time on complex topics
- Repeat labs to ensure proficiency with skills
- Save on travel costs
- Study at home or in your office

Our SANS OnDemand, vLive, Simulcast, and SelfStudy formats are backed by nearly 100 professionals who ensure we deliver the same quality instruction online (including support) as we do at live training events.

CORE NETWARS EXPERIENCE

JUNE 22 & 23

REGISTRATION IS LIMITED AND FREE
for students attending any long course at Minneapolis 2017
(NON-STUDENT ENTRANCE FEE IS $1,520).

The Core NetWars Experience is a computer and network security challenge designed to test a participant's experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals. Many enterprises, government agencies, and military bases are using NetWars to help identify skilled personnel and as part of extensive hands-on training. With Core NetWars, you'll build a wide variety of skills while having a great time.

Who Should Attend

- Security professionals
- System administrators
- Network administrators
- Ethical hackers
- Penetration testers
- Incident handlers
- Security auditors
- Vulnerability assessment personnel
- Security Operations Center staff

Introducing Experience 5.0 "A Whole New Experience!"

www.sans.org/minneapolis

Future Training Events

SANS 2017 Orlando, FL Apr 7-14

Baltimore Spring	Baltimore, MD	Apr 24-29

Security West San Diego, CA May 9-18

Northern Virginia – Reston	Reston, VA	May 21-26
Atlanta	Atlanta, GA	May 30 - June 4
Houston	Houston, TX	June 5-10
San Francisco Summer	San Francisco, CA	June 5-10
Rocky Mountain	Denver, CO	June 12-17
Charlotte	Charlotte, NC	June 12-17
Minneapolis	Minneapolis, MN	June 19-24
Columbia	Columbia, MD	June 26 - July 1
Los Angeles – Long Beach	Long Beach, CA	July 10-15

SANSFIRE Washington, DC July 22-29

San Antonio	San Antonio, TX	Aug 6-11
Boston	Boston, MA	Aug 7-12
New York City	New York, NY	Aug 14-19
Salt Lake City	Salt Lake City, UT	Aug 14-19
Chicago	Chicago, IL	Aug 21-26
Virginia Beach	Virginia Beach, VA	Aug 21 - Sep 1
Tampa – Clearwater	Clearwater, FL	Sep 5-10
San Francisco Fall	San Francisco, CA	Sep 5-10

Future Summit Events

Threat Hunting and IR	New Orleans, LA	Apr 18-25
Automotive Cybersecurity	Detroit, MI	May 1-8
Security Operations Center	Washington, DC	June 5-12
Digital Forensics	Austin, TX	June 22-29
ICS & Energy	Houston, TX	July 10-14
Security Awareness	Nashville, TN	July 31 - Aug 9
Data Breach	Chicago, IL	Sep 25 - Oct 2

Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit **www.sans.org/community** for up-to-date Community course information.

Hotel Information

Millennium Hotel Minneapolis

1313 Nicollet Mall
Minneapolis, MN 55403
Phone: 612-332-6000
www.sans.org/event/minneapolis-2017/location

Situated along the tree-lined streets of Nicollet Mall, Millennium Hotel Minneapolis is the closest full-service hotel to the Minneapolis Convention Center and is also moments away from the city's cultural districts. This hotel's 321 guest rooms and suites combine contemporary elegance with a residential feel and feature stunning views. Come stay, and experience the delights of the Twin Cities.

Special Hotel Rates Available

A special discounted rate of $179.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID and can only be booked by calling the hotel directly at 612-332-6000 and mentioning you are a SANS government attendee. These rates include high-speed Internet in your room and are only available through **May 29, 2017**.

Top 5 reasons to stay at the Millennium Hotel Minneapolis

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

Registration Information

Register online at **www.sans.org/minneapolis**

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

Select your course 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.

Pay Early and Save*

Use code **EarlyBird17** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**4-26-17**	**$400.00**	**5-17-17**	**$200.00**

*Some restrictions apply. Early-bird discounts do not apply to Hosted courses.

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 & Access Policy

If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. All substitution requests must be submitted by email to **registration@sans.org**. If an attendee must cancel and no substitute is available, a refund can be issued for any received payments by **May 31, 2017**. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.

Open a **SANS 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 FAQs
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

www.sans.org/account