INFORMATION SECURITY TRAINING

Dallas 2018
February 19-24

Protect Your Business | Advance Your Career
Eight hands-on, immersion-style courses taught by real-world practitioners

See inside for courses offered in:
- Cyber Defense
- Penetration Testing
- Ethical Hacking
- Monitoring & Detection
- CISSP® Preparation
- Digital Forensics
- Legal

“The depth and practical experience makes SANS training outstanding.”
-Derrick Lawson, Splunk

SAVE $400
Register and pay by Dec 27th
Use code EarlyBird18

www.sans.org/dallas
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, which guarantees what you learn in class will be up to date and relevant to your job. The SANS Dallas 2018 lineup of instructors includes:

Evening Bonus Sessions
Take advantage of these extra evening presentations and add more value to your training. Learn more on page 11.

KEYNOTE: Convergence Forensics: Leveraging Multiple Skills to Analyze Evidence
Heather Mahalik

You’ve Got Ransomware! Managing the Legal Risk of Cyber Fraud
Benjamin Wright

Save $400 when you register and pay by December 27th using code EarlyBird18

Courses at a Glance

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>Page 2</td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>Page 3</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>Page 4</td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td>Page 5</td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td>Page 6</td>
</tr>
<tr>
<td>FOR585</td>
<td>Advanced Smartphone Forensics</td>
<td>Page 7</td>
</tr>
<tr>
<td>MGT414</td>
<td>SANS Training Program for CISSP® Certification</td>
<td>Page 8</td>
</tr>
<tr>
<td>LEG523</td>
<td>Law of Data Security and Investigations</td>
<td>Page 9</td>
</tr>
</tbody>
</table>
Securing Approval and Budget for Training

Write a formal request

- All organizations are different, but because training requires a significant investment of both time and money, most successful training requests are made via a written document (short memo and/or a few PowerPoint slides) that justifies the need and benefit. Most managers will respect and value the effort.

- Provide all the necessary information in one place. In addition to your request, provide all the right context by including the summary pages on Why SANS?, the Training Roadmap, the instructor bio, and additional benefits available at our live events or online.

Be specific

- How does the course relate to the job you need to be doing? Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context for the decision.

- Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled “You Will Be Able To.” Be sure to include this in your request so that you make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Establish longer-term expectations

- Information security is a specialized career path within IT with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense—not a once-and-done item.

- Take a GIAC Certification exam to prove the training worked. Employers value the validation of skills and knowledge that a GIAC Certification provides. Exams are psychometrically designed to establish competency for related job tasks.

- Consider offering trade-offs for the investment. Many professionals build annual training expenses into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.
Six-Day Program
Mon, Feb 19 - Sat, Feb 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

This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques you can directly apply when you get back to work. You’ll learn tips and tricks from the experts so you can win the battle against the wide range of cyber adversaries who 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 you would be able to find them?
> Do you know the effectiveness of each security device and are you certain 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.

Bryce Galbraith  SANS Principal Instructor
As a contributing author to 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

Brenda Galbraith  Foundstone Principal Consultant
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

Bryce Galbraith  Foundstone Principal Consultant
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

SANS Institute
www.sans.edu

Foundstone
www.foundstone.com

Layered Security
www.layeredsecurity.com

 GIAC Certification
Security Essentials
www.giac.org/gsec

“An amazing class that every professional security practitioner should take.”
EFREN IZQUIERDO-RAMIREZ, GENERAL DYNAMICS

-"An amazing class that every professional security practitioner should take."

EFREN IZQUIERDO-RAMIREZ, GENERAL DYNAMICS

Register at www.sans.org/dallas | 301-654-SANS (7267)
Intrusion Detection In-Depth

Six-Day Program
Mon, Feb 19 - Sat, Feb 24
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Donald Williams

Who Should Attend
> Intrusion detection (all levels), system, and security analysts
> Network engineers and administrators
> Hands-on security managers

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?

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 sometimes 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 with insight and awareness. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

Mark Twain said, “It is easier to fool people than to convince them that they’ve been fooled.” Too many IDS/IPS solutions provide a simplistic red/green, good/bad assessment of traffic and too many untrained analysts accept that feedback as the absolute truth. This course emphasizes the theory that a properly trained analyst uses an IDS alert as a starting point for examination of traffic, not as a final assessment. SEC503 imparts the philosophy that the analyst must have access to alerts and the ability to examine them in order to give them meaning and context. You will learn to investigate and reconstruct activity to determine if it is noteworthy or a false indication.

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 DNS and HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to master different open-source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK. 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.

The concepts learned in SEC503 helped me bridge a gap in knowledge of what we need to better protect our organization.”
- Greg Thys, Mary Greeley Medical Center

Donald Williams  SANS Certified Instructor

Donald retired from active duty in 2014 after over 20 years of service in the U.S. Army. He has extensive experience in incident handling, intrusion analysis, and network auditing. During his Army career, Donald served as the Defensive Cyber Operations Chief for the Army’s Regional Computer Emergency Response Team in South West Asia (RCERT-SWA), directly overseeing the intrusion analysis and incident response teams for one of the Army’s largest networks spanning over 10 countries. Donald holds several GIAC certifications, including the GIAC Security Expert (GSE), GCIH, GCIA, and GSNA certifications, as well as numerous other industry certifications. @donaldjwilliam5
The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection and 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.

“As someone who works in information security but has never had to do a full incident report, SEC504 taught me all the proper processes and steps.”
- Todd Choryan, Motorola Solutions

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 those attacks. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning, exploiting, and defending systems. This course 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.

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

“I can’t wait to bring new information from SEC504 back to my organization.”
- Josh Hoss, Netspend

“A real eye opener on the Web attack section. Windows command-line bootcamp section was excellent.”
- Terrence Randell, JPMorgan Chase

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, GPEP, 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
Network Penetration Testing and Ethical Hacking

SEC560

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

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

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.

“I like that the labs in SEC560 provided clear, step-by-step guidance. The instructor’s level of knowledge and ability to relay information is fantastic.”
- Bryan Barnhart,
Infiltration Labs

Moses Hernandez  SANS Certified Instructor

Moses Hernandez is a seasoned security professional with over 15 years in the IT industry. He has held positions as a network engineer, network architect, security architect, platform engineer, site reliability engineer, and consulting sales engineer. He has a background in complex network systems, systems administration, forensics, penetration testing, and development. He has worked with some of the largest companies in the nation as well as fast-growing, bootstrap startups. Moses has developed information security regimens safeguarding some of the most sensitive personal data in the nation. He creates custom security software to find and mitigate unknown threats, and works on continually evolving his penetration testing skills. He enjoys building software, networks, systems, and working with business-minded individuals. Moses’s current passions include offensive forensics, building secure systems, finance, economics, history, and music. @mosesrenegade

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/dallas-2018/courses
FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting will help you to:

- Detect how and when a breach occurred
- Identify compromised and affected systems
- Determine what attackers took or changed
- Contain and remediate incidents
- Develop key sources of threat intelligence
- Hunt down additional breaches using knowledge of the adversary

DAY 0: A 3-letter government agency contacts you to say an advanced threat group is targeting organizations like yours, and that your organization is likely a target. They won’t tell how they know, but they suspect that there are already several breached systems within your enterprise. An advanced persistent threat, aka an APT, is likely involved. This is the most sophisticated threat that you are likely to face in your efforts to defend your systems and data, and these adversaries may have been actively rummaging through your network undetected for months or even years.

This is a hypothetical situation, but the chances are very high that hidden threats already exist inside your organization’s networks. Organizations can’t afford to believe that their security measures are perfect and impenetrable, no matter how thorough their security precautions might be. Prevention systems alone are insufficient to counter focused, human adversaries who know how to get around most security and monitoring tools.

This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and hactivism. Constantly updated, FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting addresses today’s incidents by providing hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to detect, counter, and respond to real-world breach cases.

GATHER YOUR INCIDENT RESPONSE TEAM – IT’S TIME TO GO HUNTING!
FOR585: Advanced Smartphone Forensics

Six-Day Program
Mon, Feb 19 - Sat, Feb 24
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructors: Heather Mahalik, Domenica Crognale

Who Should Attend
- Experienced digital forensic analysts
- Media exploitation analysts
- Information security professionals
- Incident response teams
- Law enforcement officers, federal agents, and detectives
- Accident reconstruction investigators
- IT auditors
- Graduates of SANS SEC575, SEC563, FOR500, FOR508, FOR526, FOR518, or FOR518 who want to take their skills to the next level

“Is this the most advanced mobile device training that I know of and is greatly needed. It is currently the only course being taught at this level!”
- Scott McNamee, D0s/CACI

Heather Mahalik  SANS Senior Instructor
Heather has worked on high-stress and high-profile cases, investigating everything from child exploitation to Osama Bin Laden’s media. She has helped law enforcement, eDiscovery firms, and the federal government extract and manually decode artifacts used in solving investigations around the world. All told she has more than 14 years of experience in digital forensics, including eight years focused on mobile forensics—there’s hardly a device or platform she hasn’t researched or examined or a commercial tool she hasn’t used. These days Heather is the Director of Forensic Engineering at ManTech CARD. Heather previously led the mobile device team for Basis Technology, where she focused on mobile device exploitation in support of the federal government. She also worked as a forensic examiner at Stroz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she handled a number of high-profile cases. She has also developed and implemented forensic training programs and standard operating procedures. @HeatherMahalik

Domenica Crognale  SANS Instructor
Domenica is one of the course co-authors of SANS FOR585: Advanced Smartphone Forensics. She has been working in digital forensics for more than 10 years and specializing in mobile devices since 2009. In previous jobs she has provided training to military and government agencies, worked on high-profile cases, tested and validated various mobile forensics utilities, and provided security assessments for many mobile applications. In her day job, she spends time dissecting third-party mobile applications, where there is no shortage of interesting data left behind. She maintains multiple certifications including the GASF, EnCE, CCE, and CISSP. @domenicacrognal

SMARTPHONES HAVE MINDS OF THEIR OWN. DON’T MAKE THE MISTAKE OF REPORTING SYSTEM EVIDENCE AS USER ACTIVITY. IT’S TIME TO GET SMARTER!

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, accident reconstruction, and more. Understanding how to leverage the data from the device in a correct manner can make or break your case and your future as an expert. FOR585: Advanced Smartphone Forensics will teach you those skills.

Every time the smartphone thinks or makes a suggestion, the data are saved. It’s easy to get mixed up in what the forensic tools are reporting. Smartphone forensics is more than pressing the find evidence button and getting answers. Your team cannot afford to rely solely on the tools in your lab. You have to understand how to use them correctly to guide your investigation, instead of just letting the tool report what it believes happened on the device. It is impossible for commercial tools to parse everything from smartphones and understand how the data were put on the device. Examination and interpretation of the data is your job and this course will provide you and your organization with the capability to find and extract the correct evidence from smartphones with confidence.

This in-depth smartphone forensic course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 20 hands-on labs that allow students to analyze different datasets from smart devices and leverage the best forensic tools, methods, and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools. Each lab is designed to teach you a lesson that can be applied to other smartphones. You will gain experience with the different data formats on multiple platforms and learn how the data are stored and encoded on each type of smart device. The labs will open your eyes to what you are missing by relying 100% on your forensic tools.

SMARTPHONE DATA CAN’T HIDE FOREVER – IT’S TIME TO OUTSMART THE MOBILE DEVICE!

FOR585: Advanced Smartphone Forensics will teach you those skills.

“It’s time to outsmart the mobile device!”
- Scott McNamee, DoS/CACI

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/dallas-2018/courses
SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam. MGT414 focuses solely on the eight domains of knowledge, as determined by (ISC)², that form a critical part of the CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

Who Should Attend

> Security professionals who are interested in understanding the concepts covered on the CISSP® exam as determined by (ISC)²
> Managers who want to understand the critical areas of information security
> System, security, and network administrators who want to understand the pragmatic applications of the CISSP® eight domains
> Security professionals and managers looking for practical ways the eight domains of knowledge can be applied to their current job

Obtaining Your CISSP® Certification Consists of:

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

“I have taken several CISSP® prep courses in the last several years and this by far is the best. Finally I feel that I have the confidence to take the test.”
- JERRY CARE, SARUM, LLC

“This training was a comprehensive overview of all topics covered on the CISSP® exam. All in attendance were there for a common goal, including the instructor. It was easy to follow, and the real-world examples given were priceless.”
- RON PINNOCK, NAVY EXCHANGE SERVICE COMMAND

“I think the course material and the instructor are very relevant for the task of getting a CISSP®. The overall academic exercise is solid.”
- AARON LEWTER, AVAILITY

David R. Miller  SANS Certified Instructor

David has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on information system security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security program, including through policy writing, network architecture design (including security zones), development of incident response teams and programs, design and implementation of public key infrastructures, security awareness training programs, specific security solution designs such as secure remote access and strong authentication architectures, disaster recovery planning and business continuity planning, and pre-audit compliance gap analysis and remediation. He serves as a security lead and forensic investigator on numerous enterprise-wide IT design and implementation projects for Fortune 500 companies, providing compliance, security, technology, and architectural recommendations and guidance. His current projects include work on Microsoft Windows Active Directory enterprise designs, security information and event management systems, intrusion detection and protection systems, endpoint protection systems, patch management systems, configuration monitoring systems, and enterprise data encryption for data at rest, in transit, in use, and within email systems. David is an author, lecturer and technical editor of books, curriculum, certification exams, and computer-based training videos. 

@DRM_CyberDude
LEG523
Law of Data Security and Investigations

Five-Day Program
Mon, Feb 19 - Fri, Feb 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
> Cyber incident and emergency responders around the world (including private sector, law enforcement, national guard, civil defense and the like)

NEW!
> Form contract for inviting outside incident responders – including police, contractors National Guard, or civil defense agency anywhere in the world – to help with a cyber crisis
> 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
> How to improve the assessment and interpretation of digital evidence, such as evidence of a breach or other cyber event

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 three or four years ago.’”
- Tom S., Case Western Reserve University

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
Enhance Your Training Experience

Add an **OnDemand Bundle** OR **GIAC Certification Attempt**
to your course within seven days of this event to get bundle 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

*OnDemand Bundle price – $729*

“*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 bundle price – $729*

“*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](http://www.sans.org/ondemand/bundles) | [www.giac.org](http://www.giac.org)

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

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

**KEYNOTE: Convergence Forensics: Leveraging Multiple Skills to Analyze Evidence**

Heather Mahalik

One discipline is not enough to solve investigations relating to digital evidence. In this keynote talk, Heather Mahalik will expand on scenarios in which multiple skills are needed to hunt and uncover evidence. Network forensics, memory forensics, malware detection, malware analysis, and data synchronization between smartphones, Mac and Windows computers may change the way you need to look at your evidence. Simply having tunnel vision in your field will limit your success! A change in your approach may change your success rate when examining digital media.

---

**You’ve Got Ransomware! 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. In this presentation, Benjamin 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.

---

**SECURITY AWARENESS**

Security Awareness Training by the Most Trusted Source

Protect Your Employees

Keep your organization safe with flexible, computer-based training.

- Train employees on their own schedule
- Modify modules to address specific audiences
- Increase comprehension – courses translated into many languages
- Test learner comprehension through module quizzes
- Track training completion for compliance reporting purposes

Learn more about SANS Security Awareness at: securingthehuman.sans.org

Change Human Behavior
Manage Risk
Maintain Compliance
Protect Your Brand
## Future Training Events

### Security East

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Northern VA Winter</td>
<td>Reston, VA</td>
<td>Jan 15-20</td>
</tr>
<tr>
<td>Las Vegas</td>
<td>Las Vegas, NV</td>
<td>Jan 28 - Feb 2</td>
</tr>
<tr>
<td>Miami</td>
<td>Miami, FL</td>
<td>Jan 29 - Feb 3</td>
</tr>
<tr>
<td>Scottsdale</td>
<td>Scottsdale, AZ</td>
<td>Feb 5-10</td>
</tr>
<tr>
<td>Southern California</td>
<td>Anaheim, CA</td>
<td>Feb 12-17</td>
</tr>
<tr>
<td>Dallas</td>
<td>Dallas, TX</td>
<td>Feb 19-24</td>
</tr>
<tr>
<td>New York City Winter</td>
<td>New York, NY</td>
<td>Feb 26 - Mar 3</td>
</tr>
<tr>
<td>San Francisco Spring</td>
<td>San Francisco, CA</td>
<td>Mar 12-17</td>
</tr>
<tr>
<td>Northern VA Spring – Tysons</td>
<td>McLean, VA</td>
<td>Mar 17-24</td>
</tr>
<tr>
<td>Pen Test Austin</td>
<td>Austin, TX</td>
<td>Mar 19-24</td>
</tr>
<tr>
<td>Boston Spring</td>
<td>Boston, MA</td>
<td>Mar 25-30</td>
</tr>
</tbody>
</table>

### SANS 2018

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baltimore Spring</td>
<td>Baltimore, MD</td>
<td>Apr 21-28</td>
</tr>
<tr>
<td>Seattle Spring</td>
<td>Seattle, WA</td>
<td>Apr 23-28</td>
</tr>
</tbody>
</table>

### Security West

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Northern VA Reston Spring</td>
<td>Reston, VA</td>
<td>May 20-25</td>
</tr>
<tr>
<td>Atlanta</td>
<td>Atlanta, GA</td>
<td>May 29 - Jun 3</td>
</tr>
<tr>
<td>Rocky Mountain</td>
<td>Denver, CO</td>
<td>Jun 4-9</td>
</tr>
<tr>
<td>Crystal City</td>
<td>Arlington, VA</td>
<td>Jun 18-23</td>
</tr>
<tr>
<td>Minneapolis</td>
<td>Minneapolis, MN</td>
<td>Jun 25-30</td>
</tr>
<tr>
<td>Vancouver</td>
<td>Vancouver, BC</td>
<td>Jun 25-30</td>
</tr>
</tbody>
</table>

## Future Summit Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Threat Intelligence</td>
<td>Bethesda, MD</td>
<td>Jan 29 - Feb 5</td>
</tr>
<tr>
<td>Cloud Security</td>
<td>San Diego, CA</td>
<td>Feb 19-26</td>
</tr>
<tr>
<td>ICS Security</td>
<td>Orlando, FL</td>
<td>Mar 19-26</td>
</tr>
<tr>
<td>Blue Team</td>
<td>Louisville, KY</td>
<td>Apr 23-30</td>
</tr>
<tr>
<td>Automotive Cybersecurity</td>
<td>Chicago, IL</td>
<td>May 1-8</td>
</tr>
<tr>
<td>DFIR</td>
<td>Austin, TX</td>
<td>Jun 7-14</td>
</tr>
</tbody>
</table>

## Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit [www.sans.org/community](http://www.sans.org/community) for up-to-date Community course information.
Register online at www.sans.org/dallas
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.

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. Processing fees will apply. 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 January 31, 2018. 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.

Top 5 reasons to stay at the Dallas/Addison Marriott Quorum by the Galleria
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 Dallas/Addison Marriott Quorum by the Galleria, 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 Dallas/Addison Marriott Quorum by the Galleria that you won’t want to miss!
5. Everything is in one convenient location!

Special Hotel Rates Available
A special discounted rate of $182.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through January 29, 2018.

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

Dallas/Addison Marriott Quorum by the Galleria
14901 Dallas Parkway
Dallas, TX  75254
972-661-2800
www.sans.org/event/dallas-2018/location

Slumber in style at Dallas/Addison Marriott Quorum by the Galleria. Centrally located in the heart of Addison, this hotel features easy access to premier restaurants, entertainment and shopping. The hotel also offers complimentary shuttle service to the Galleria every hour.

Registration Information
Register online at www.sans.org/dallas
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 EarlyBird18 when registering early

<table>
<thead>
<tr>
<th>Pay &amp; enter code by</th>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12-27-17</td>
<td>$400.00</td>
<td>1-17-18</td>
<td>$200.00</td>
</tr>
</tbody>
</table>

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

Dallas/Addison Marriott Quorum by the Galleria
14901 Dallas Parkway
Dallas, TX  75254
972-661-2800
www.sans.org/event/dallas-2018/location

Top 5 reasons to stay at the Dallas/Addison Marriott Quorum by the Galleria
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 Dallas/Addison Marriott Quorum by the Galleria, 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 Dallas/Addison Marriott Quorum by the Galleria that you won’t want to miss!
5. Everything is in one convenient location!

Special Hotel Rates Available
A special discounted rate of $182.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through January 29, 2018.

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

Dallas/Addison Marriott Quorum by the Galleria
14901 Dallas Parkway
Dallas, TX  75254
972-661-2800
www.sans.org/event/dallas-2018/location

Slumber in style at Dallas/Addison Marriott Quorum by the Galleria. Centrally located in the heart of Addison, this hotel features easy access to premier restaurants, entertainment and shopping. The hotel also offers complimentary shuttle service to the Galleria every hour.

Registration Information
Register online at www.sans.org/dallas
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 EarlyBird18 when registering early

<table>
<thead>
<tr>
<th>Pay &amp; enter code by</th>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12-27-17</td>
<td>$400.00</td>
<td>1-17-18</td>
<td>$200.00</td>
</tr>
</tbody>
</table>

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

Dallas/Addison Marriott Quorum by the Galleria
14901 Dallas Parkway
Dallas, TX  75254
972-661-2800
www.sans.org/event/dallas-2018/location

Top 5 reasons to stay at the Dallas/Addison Marriott Quorum by the Galleria
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 Dallas/Addison Marriott Quorum by the Galleria, 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 Dallas/Addison Marriott Quorum by the Galleria that you won’t want to miss!
5. Everything is in one convenient location!

Special Hotel Rates Available
A special discounted rate of $182.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through January 29, 2018.

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
Newsletters

**NewsBites**
Twice-weekly, high-level executive summaries 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.

Webcasts

**Ask the Experts 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 how a vendor’s commercial tool can be used to solve or mitigate that problem.

Other Free Resources (No portal account is necessary)

- 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)

Save $400 when you pay for any 4-, 5-, or 6-day course and enter the code “EarlyBird18” by December 27th. www.sans.org/dallas

As the leading provider of information defense, security, and intelligence training to military, government, and industry groups, the SANS Institute is proud to be a Corporate Member of the AFCEA community.