INFORMATION SECURITY TRAINING

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

See inside for courses offered in:
- Cyber Defense
- Penetration Testing
- CISSP® Preparation
- Digital Forensics
- Incident Response

“SANS training is relevant, concise and laser-focused on the exact topics relevant to my daily routine.”
-Alex Rifman, Anomali

SAVE $400
Register and pay by Feb 28th
Use code EarlyBird18

www.sans.org/seattle
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 Seattle Spring 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 9.

KEYNOTE: Convergence Forensics:
Leveraging Multiple Skills for Comprehensive Investigations
–Philip Hagen

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>SEC504</td>
<td>Hacker Tools, Techniques, Exploits &amp; Incident Handling</td>
<td>Page 4</td>
</tr>
<tr>
<td>SEC579</td>
<td>Virtualization and Software-Defined Security</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>FOR572</td>
<td>Advanced Network Forensics and Analysis</td>
<td>Page 7</td>
</tr>
<tr>
<td>MGT414</td>
<td>SANS Training Program for CISSP® Certification</td>
<td>Page 8</td>
</tr>
</tbody>
</table>

Save $400 when you register and pay by February 28th using code EarlyBird18

Register today for SANS Seattle Spring 2018!
www.sans.org/seattle
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.
Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

Is SEC401: Security Essentials Bootcamp Style the right course for you? 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.

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

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization’s critical information assets and business systems. 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.
Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. SEC501: Advanced Security Essentials – Enterprise Defender builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

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

“Nearly 100% of the material covered in SEC501 is immediately applicable to the daily role of an analyst, regardless of industry.”

-Terry Boedeker, FireEye

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

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

“SANS has done well putting this course together, I love every bit of the information. This is one of the best cybersecurity courses out there, and I’ve been sharing my stories and experiences already.”

-Lucky Onoriodhe, Tetra Pak

Bryan Simon  SANS Certified Instructor

Bryan Simon is an internationally recognized expert in cybersecurity and has been working in the information technology and security field since 1991. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. He has instructed individuals from organizations such as the FBI, NATO, and the UN in matters of cybersecurity on two continents.

Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in IT security, and was most recently profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 13 GIAC Certifications including GSEC, GCWN, GCIA, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, GCUX, GISF, and GMON. Bryan’s scholastic achievements have resulted in the honor of sitting as a current member of the Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program. Bryan is a SANS instructor for SEC401, SEC501, SEC505, and SEC511.

@BryanOnSecurity
SEC504
Hacker Tools, Techniques, Exploits, and Incident Handling

GCIH Certification
Incident Handler

Six-Day Program
Mon, Apr 23 – Sat, Apr 28
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
(If your laptop supports only wireless, please bring a USB Ethernet adapter.)
Instructor: Donald Williams

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

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.

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

“SEC504 is engaging, informative, and mind-blowing. I've always known about the topics, but the discussion and labs helped cement the understanding.”
- Jason Kinder, DRS Technologies

“Excellent, real-world examples and demos, with step-by-step examples of how to respond to an attack. SEC504 is a must for everyone on the team.”
- Mike Pyke, VyStar Credit Union

“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

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.

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
Virtualization and Software-Defined Security

SEC579

Five-Day Program
Mon, Apr 23 - Fri, Apr 27
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Dave Shackleford

Who Should Attend

- Security personnel who are tasked with securing virtualization and private cloud infrastructure
- Network and systems administrators who need to understand how to architect, secure and maintain virtualization and cloud technologies
- Technical auditors and consultants who need to gain a deeper understanding of VMware virtualization from a security and compliance perspective

One of today’s most rapidly evolving and widely deployed technologies is server virtualization. SEC579: Virtualization and Software-Defined Security is intended to help security, IT operations, and audit and compliance professionals build, defend, and properly assess both virtual and converged infrastructures, as well as understand software-defined networking and infrastructure security risks.

Many organizations are already realizing cost savings from implementing virtualized servers, and systems administrators love the ease of deployment and management of virtualized systems. More and more organizations are deploying desktop, application, and network virtualization as well. There are even security benefits of virtualization: easier business continuity and disaster recovery, single points of control over multiple systems, role-based access, and additional auditing and logging capabilities for large infrastructure.

With these benefits comes a dark side, however. Virtualization technology is the focus of many new potential threats and exploits, and it presents new vulnerabilities that must be managed. There are also a vast number of configuration options that security and system administrators need to understand, with an added layer of complexity that has to be managed by operations teams. Virtualization technologies also connect to network infrastructure and storage networks, and require careful planning with regard to access controls, user permissions, and traditional security controls.

In addition, many organizations are evolving virtualized infrastructure into private clouds using converged infrastructure that employs software-defined tools and programmable stack layers to control large, complex data centers. Security architecture, policies, and processes will need to be adapted to work within a converged infrastructure, and there are many changes that security and operations teams will need to accommodate to ensure that assets are protected.

This course will cover core operational functions such as secure network design and segmentation, building of secure systems, and secure virtualization implementation and controls. Cutting-edge topics like software-defined networking and container technology will also be covered in detail with an emphasis on security techniques and controls. Security-focused virtualization, integration, and monitoring will be covered at length. Attacks and threats to virtual environments will be discussed, and students will learn how to perform vulnerability assessments and penetration tests in their virtual environments. We’ll also look at how to implement network intrusion detection and access controls, implement log and event management, and perform forensics and incident handling in virtual and converged data centers. Finally, students will learn how to perform technical audits and assessments of their in-house and public cloud environments, creating reports and documenting technical controls. This course will emphasize automation and scripting techniques.

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/seattle-spring-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!
Six-Day Program
Mon, Apr 23 - Sat, Apr 28
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Philip Hagen

Who Should Attend
- Incident response team members and forensicators
- Hunt team members
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- Anyone interested in computer network intrusions and investigations
- Security Operations Center personnel and information security practitioners

It is exceedingly rare to work any forensic investigation that doesn’t have a network component. Endpoint forensics will always be a critical and foundational skill for this career, but overlooking network communications is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, uncover attackers that have been active for months or longer, or even prove useful in definitively proving a crime actually occurred.

FOR572 was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking – we’ll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence as well as how to place new collection platforms while an incident is already under way.

The hands-on labs in this class cover a wide range of tools and platforms, including the venerable tcpdump and Wireshark for packet capture and analysis; NetworkMiner for artifact extraction; and open-source tools including nfdump, tcpxtract, tcpflow, and more. Newly added tools in the course include the SOF-ELK platform—a VMware appliance pre-configured with the ELK stack. This “big data” platform includes the Elasticsearch storage and search database, the Logstash ingest and parse utility, and the Kibana graphical dashboard interface. Together with the custom SOF-ELK configuration files, the platform gives forensicators a ready-to-use platform for log and NetFlow analysis. For full-packet analysis and hunting at scale, the Moloch platform is also used. Through all of the in-class labs, your shell scripting abilities will also be used to make easy work of ripping through hundreds and thousands of data records.

"Phil continues to illustrate through examples and paint the big picture for examiners/responders. His approach and teaching style are second to none when it comes to network forensics.”
- Grad Garnett, Cisco

Philip Hagen  SANS Certified Instructor

Phil began his studies at the U.S. Air Force Academy’s Computer Science Department, where he focused on network security and was an inaugural member of the computer security extracurricular group. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. Today, Phil’s career has spanned the full attack life cycle – tool development, deployment, operations, and the investigative aftermath – giving him rare and deep insight into the artifacts left behind. Phil has covered deep technical tasks, managed an entire computer forensic services portfolio, and handled executive responsibilities. He’s supported systems that demanded 24x7x365 functionality, managed a team of 85 computer forensic professionals in the national security sector, and provided forensic consulting services for law enforcement, government, and commercial clients. These experiences led Phil to his role today as the DFIR strategist at Red Canary, where he supports the firm’s managed threat detection service. Phil also spends time developing and maintaining the SOF-ELK distribution, a virtual appliance free for the DFIR Community. #PhilHagen

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/seattle-spring-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 updated 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.

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

“David was awesome! He showed great depth of knowledge, and was able to convey that in easy-to-understand ways.”
- Kevin Spinnato, UPI

“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

“Awesome course and instructor! It was a long domain today and the amount of info was intense, but I loved the way things were broken down to better understand them. Simply awesome!”
- Glenn Rittereiser, Maersk Line

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

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
Bonus 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 for Comprehensive Investigations
Philip Hagen

One discipline is not enough to solve investigations relating to digital evidence. In this Keynote, Phil will expand on scenarios where 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.

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
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  |  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

Training Events

Our most recommended format, live SANS training events feature SANS’s 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 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

The same SANS courses, courseware, and labs are 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 certifications 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.

“I am thoroughly pleased with the OnDemand modality. From a learning standpoint, I lose nothing. In fact, the advantage of setting my own pace with respect to balancing work, family, and training is significant, not to mention the ability to review anything that I might have missed the first time.”

- Kevin E., U.S. Army

“The decision to take five days away from the office is never easy, but so rarely have I come to the end of a course and had no regret whatsoever. This was one of the most useful weeks of my professional life.”

-Dan Trueman, Novae PLC
Future Training Events

Scottsdale, AZ: Feb 5-10
Southern California, CA: Feb 12-17
Dallas, TX: Feb 19-24
New York City Winter, NY: Feb 26 - Mar 3
San Francisco, CA: Mar 12-17
Northern VA Spring – Tysons, VA: Mar 17-24
Pen Test Austin, TX: Mar 19-24
Boston Spring, MA: Mar 25-30

SANS 2018, Orlando, FL: Apr 3-10
RSA Conference, San Francisco, CA: Apr 11-16
Baltimore Spring, Baltimore, MD: Apr 21-28
Seattle Spring, Seattle, WA: Apr 23-28

Security West, San Diego, CA: May 11-18
Northern VA Reston Spring, Reston, VA: May 20-25
Atlanta, GA: May 29 - Jun 3
Rocky Mountain, Denver, CO: Jun 4-9
Crystal City, Arlington, VA: Jun 18-23
Minneapolis, Minneapolis, MN: Jun 25-30
Vancouver, Vancouver, BC: Jun 25-30
Charlotte, Charlotte, NC: Jul 9-14

SANSFIRE, Washington, DC: Jul 14-21
Boston Summer, Boston, MA: Aug 6-11
San Antonio, San Antonio, TX: Aug 6-11

Future Summit Events

Cloud Security, San Diego, CA: Feb 19-26
ICS Security, Orlando, FL: Mar 19-26
Blue Team, Louisville, KY: Apr 23-30
Automotive Cybersecurity, Chicago, IL: May 1-8
DFIR, Austin, TX: Jun 7-14

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.
Register online at www.sans.org/seattle-spring
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 April 4, 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.

Registration Information
Register online at www.sans.org/seattle-spring
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.

Top 5 reasons to stay at the Hyatt Regency Bellevue
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 Hyatt Regency Bellevue, 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 Hyatt Regency Bellevue that you won’t want to miss!
5. Everything is in one convenient location!

Special Hotel Rates Available
A special discounted rate of $219.00 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 5pm EST on April 2, 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.