The Most Trusted Source for Information Security Training, Certification, and Research

INFORMATION SECURITY TRAINING

Atlanta 2019
May 28 – June 2

Protect Your Business | Advance Your Career

Seven hands-on, immersion-style courses taught by real-world practitioners

See inside for courses and GIAC certifications in:
- Cyber Defense
- Penetration Testing
- Ethical Hacking
- Digital Forensics
- ICS/SCADA Security

FEATUREING A NEW COURSE
SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis

“The SANS training offered practical techniques for security in an easy-to-digest way. I feel better equipped to approach the concepts in a real-world setting.”
-Nate Roosien, Meijer, Inc.

SAVE $350
Register and pay by April 3rd
Use code EarlyBird19

www.sans.org/atlanta
Join us at SANS Atlanta 2019 and take a first-hand look at why SANS is the most trusted source for information security training, certification, and research. Learn the skills needed to protect your organization and advance your career! Take advantage of these opportunities to get the most out of your training:

- Distinguish yourself as an information security leader by preparing for your GIAC Certification.
- Network with like-minded security professionals facing similar challenges.
- Attend evening bonus sessions led by SANS instructors and gain insight into the latest cybersecurity topics.
- Extend your SANS course by four months with an OnDemand Bundle.

Register now and get immersion-style training with our top-rated instructors who are dedicated to helping you meet your goals. Don’t miss this opportunity to strengthen your information security skillset with hands-on training.

Courses at a Glance

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
</tr>
<tr>
<td>SEC487</td>
<td>Open-Source Intelligence (OSINT) Gathering and Analysis</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
</tr>
<tr>
<td>ICS456</td>
<td>Essentials for NERC Critical Infrastructure Protection</td>
</tr>
</tbody>
</table>

Evening Bonus Sessions

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

General Session – Welcome to SANS
– Bryan Simon

Moving Past Just Googling It: Harvesting and Using OSINT
– Micah Hoffman

Automating NIST Risk Management Framework (RMF)/800-53
– Peter Szczepankiewicz

Save $350 when you register and pay by April 3rd using code EarlyBird19
At SANS, our course authors and instructors are renowned cybersecurity experts who share their knowledge through their own real-world examples and top-shelf curriculum. Industry professionals choose SANS training again and again, year after year, for access to these highly regarded experts.

There are only about 100 individuals in the world currently qualified as SANS Certified Instructors. Each is selected after proving his or her technical and teaching expertise through years of work and success. The instructors are the founders of international cybersecurity organizations, authors of best-selling books, and developers of the world’s most advanced cyber ranges and Capture-the-Flag challenges. Many are regularly called upon to share their expertise with government and commercial organizations around the world.

In addition to their impressive résumés, every member of the SANS faculty is fully committed to providing the most comprehensive training possible. Our instructors do more than just stand in front of a classroom—they’re present for their students every step of the way, with follow-ups, webcasts, mentoring, and more. Their goal is your success, and that dedication is what truly sets SANS training apart from all the rest.

Whether you train with SANS online or at one of our live events, we promise you’ll be able to apply what you learn from these top-tier instructors as soon as you return to work.

“I have attended several SANS classes over the years and I am always impressed with the level of knowledge and professionalism of the instructors.”

-Ron Foupht, Sirius Computer Solutions
Write a formal request

- All organizations are different, but because training requires a significant investment of both time and money, most successful training requests justify the need and benefit in writing (via a short memo and/or a few PowerPoint slides).
- Provide all the necessary information in one place, including copies of the Training Roadmap, instructor bio, Why SANS? summary pages, and a list of additional benefits offered 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.
- Highlight the specifics of what you’ll be able to do after training. Each SANS course description includes a section titled “You Will Be Able To.” Be sure to include this in your request to 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.
Extend and Validate Your Training

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 – $769

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 – $769

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

-ROBERT JONES, TEAM JONES, INC.

“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.
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

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, then the SEC401 course 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.

Bryan Simon is an internationally recognized expert in cybersecurity who 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 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 the GSEC, GCWNN, GSHH, GCFA, GOPEN, GWAPT, GAWN, GISP, OCA, GCED, GCUX, GISF, and GMON. Bryan’s scholastic achievements have resulted in the honor of sitting as a current member of the SANS Institute Advisory Board and in his acceptance into the prestigious SANS Cyber Guardian program. In addition to teaching SEC401, Bryan teaches SEC501: Advanced Security Essentials – Enterprise Defender; SEC505: Securing Windows and Powershell Automation; and SEC511: Continuous Monitoring and Security Operations.
Immeasurable amounts of personal and potentially incriminating data are currently stored in the websites, apps, and social media platforms that people access and update daily via their devices. Those data can become evidence for citizens, governments, and businesses to use in solving real financial, employment, and criminal issues with the help of a professional information gatherer.

Many people think using their favorite Internet search engine is sufficient to find the data they need and do not realize that most of the Internet is not indexed by search engines. SEC487 teaches students legitimate and effective ways to find, gather, and analyze these data from the Internet. You’ll learn about reliable places to harvest data using manual and automated methods and tools. Once you have the information, we’ll show you how to ensure that it is sound, how to analyze what you’ve gathered, and how to make sure it is useful to your investigations.

This is a foundational course in open-source intelligence (OSINT) gathering and, as such, will move quickly through many areas of the field. You will learn current, real-world skills, techniques, and tools that law enforcement, private investigators, cyber attackers, and defenders use to scour the massive amount of information across the Internet, analyze the results, and pivot on interesting pieces of data to find other areas for investigation. Our goal is to provide the OSINT knowledge base for students to be successful in their fields whether they are cyber defenders, threat intelligence analysts, private investigators, insurance claims investigators, intelligence analysts, law enforcement personnel, or just someone curious about OSINT.

Throughout the course week, students will participate in numerous hands-on labs using the tools and techniques that are the basis for gathering free data from the Internet. More than 20 labs in this course use the live Internet and dark web to help students gain real-world confidence. You’ll leave the course knowing not just how to use search features on a website, but all of the scenario-based requirements and OSINT techniques needed to gather truly important OSINT data.

Author Statement

“I recognized that the barrier to performing excellent OSINT was not that there was no free data on the Internet. It was that there was too much data on the Internet. The challenge transitioned from ‘how do I find something’ to ‘how do I find only what I need?’ This course was born from this need to help others learn the tools and techniques to effectively gather and analyze OSINT data from the Internet.”

-Micah Hoffman

Micah Hoffman has been working in the information technology field since 1998 supporting federal government, commercial, and internal customers in their efforts to discover and quantify information security weaknesses in their organizations. He leverages years of hands-on, real-world OSINT, penetration testing, and incident response experience to provide excellent solutions to his customers. Micah is the author of SEC487: Open-Source Intelligence Gathering and Analysis, and holds GIAC’s GMON, GAWN, GWAPT, and GPEN certifications as well as the CISSP®. Micah is a highly active member in the cybersecurity and OSINT communities. When not working, teaching, or learning, Micah can be found hiking on the Appalachian Trail or the many park trails in Maryland.
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 them.

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

"SEC504 is foundational and core strength-building in the most critical areas of incident handling. It reinforces and develops understanding around roles and TTPs of both the adversary and defender."

-Araceli Ari Gomes, Dell Secureworks

In his past work with the military, Peter responded to network attacks and worked with both defensive and offensive red teams. Currently, Peter is a senior security engineer with IBM. Peter believes that people lead technology, not the other way around. He works daily to bring actionable intelligence out of disparate security devices for customers, making systems interoperable. As Peter explains, "Putting together networks only to tear them apart is just plain fun, and allows students to take the information learned from books and this hands-on experience back to their particular work place."
Web applications play a vital role in every modern organization. However, if your organization doesn’t properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

SEC542 helps students move beyond push-button scanning to professional, thorough, and high-value web application penetration testing.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no “patch Tuesday” for custom web applications, and major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

SEC542 enables students to assess a web application’s security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations.

In this course, students will come to understand major web application flaws and their exploitation. Most importantly, they’ll learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations. Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. This course will help you demonstrate the true impact of web application flaws through exploitation.

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn. The course features more than 30 formal hands-on labs and culminates in a web application pen test tournament powered by the SANS NetWars Cyber Range. This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way that hammers home lessons learned.

“SEC542 shows a hands-on way of doing web app penetration testing – not just how to use this tool or that tool.”

-Christopher J. Stover, Infogressive Inc.

Bundle OnDemand with this course

Timothy McKenzie has over 20 years of IT and Information Security experience working in financial, government, defense contractor, and service-related markets. Timothy has been trained in malware research and exploit development, expert penetration, and forensics work. He currently works for Secureworks as a red team penetration tester, focused primarily on network and web-based attacks. Timothy loves sharing the vast knowledge he has acquired to give back to the Information Security community.
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.

You’ll 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.

After taking SEC560, 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.

"SEC560 provides practical, how-to material that I can use daily in my penetration testing activities – not only technically, but also from a business perspective."

-Steve Nolan, General Dynamics

Jason is the Director of Technical Services at Pulsar Security, where he manages security and enterprise software efforts. With a range of technical experience including support, presales engineer, developer, network administrator, and penetration tester, Jason can frequently be found working with clients to develop creative solutions to red team (and increasingly blue team) challenges. Passionate about both technology and the lifelong learning process, Jason enjoys enabling others via teaching and aiding in career development. Jason holds GXPN, GREM, GPEN, GAWN, GWAPT, GCH, GCIA, GMON, GMOB, GPPY, GCUX, GSNA, GSEC, GCCC, GNSA, OSCP, CEH, Security+, Network+, and CSM certifications.
FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting

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.

Threat hunting and Incident response tactics and procedures have evolved rapidly over the past several years. Your team can no longer afford to use antiquated incident response and threat hunting techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident. Incident response and threat hunting teams are the keys to identifying and observing malware indicators and patterns of activity in order to generate accurate threat intelligence that can be used to detect current and future intrusions.

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!

Eric Zimmerman
SANS Certified Instructor
@EricZimmerman

As a special agent with the FBI, Eric Zimmerman had responsibilities that included managing on-scene triage. He identified several gaps in an existing process and started creating solutions to address them. What began as building and expanding a few live response tools took Eric down a path that eventually led to him writing more than 50 programs that are now used by nearly 8,800 law enforcement officers in over 80 countries. Much of Eric’s work involved designing and building software related to investigations of sexual abuse of children. In a single year, Eric’s programs led to the rescue of hundreds of these children. As a result, in May 2012, Eric was given a National Center for Missing and Exploited Children’s Award, which honors outstanding law enforcement professionals who have performed above and beyond the call of duty. Eric was also presented with the U.S. Attorney Award for Excellence in Law Enforcement in 2013. Today, Eric serves as a senior director at Kroll in the company’s cybersecurity and investigations practice. As an instructor, Eric’s focus on understanding the big picture of digital forensics prepares students to perform better analysis, do new research of their own, and identify the best tools or techniques to perform successful investigations – all skills that will have a lifelong impact.
This five-day course empowers students with knowledge of the “what” and the “how” of the version 5/6 standards. The course addresses the role of FERC, NERC and the Regional Entities, provides multiple approaches for identifying and categorizing BES Cyber Systems, and helps asset owners determine the requirements applicable to specific implementations. Additionally, the course covers implementation strategies for the version 5/6 requirements with a balanced practitioner approach to both cybersecurity benefits as well as regulatory compliance. The course features 25 hands-on labs ranging from securing workstations to digital forensics and lock picking.

The ICS456 course was developed by SANS ICS team members with extensive electric industry experience, including former Registered Entity Primary Contacts, a former NERC officer, and a Co-Chair of the NERC CIP Interpretation Drafting Team. Together the authors bring real-world, practitioner experience gained from developing and maintaining NERC CIP and NERC 693 compliance programs and actively participating in the standards development process.

You Will Learn:

- BES Cyber System identification and strategies for lowering their impact rating
- Nuances of the applicability of NERC-defined terms and CIP standards, and how subtle changes in definitions can have a big impact on your program
- The significance of properly determining Cyber System impact ratings and strategies for minimizing compliance exposure
- Strategic implementation approaches for supporting technologies
- How to manage recurring tasks and strategies for CIP program maintenance
- Effective implementations for cyber and physical access controls
- How to break down the complexity of NERC CIP in order to communicate with your leadership
- What to expect in your next CIP audit, how to prepare supporting evidence, and how to avoid common pitfalls
- How to understand the most recent Standards Development Team’s efforts and how they may impact your current CIP program

Jason Christopher is the Chief Technology Officer for Axio. His responsibilities include providing technical leadership on security and resilience issues relevant to Axio and its partners and clients, and on the development of all Axio technology platforms for security metrics and benchmarking. Prior to Axio, Jason led the research for cybersecurity metrics and information assurance at the Electric Power Research Institute. Previously, he was the technical lead for cybersecurity capability and risk management at the U.S. Department of Energy. Jason also served as the program lead for both Critical Infrastructure Protection Standards and Smart Grid Security at the Federal Energy Regulatory Commission. Jason has worked on a variety of infrastructure projects, particularly in the field of industrial control system design and implementation. He has also researched and designed technology systems across multiple industries, including energy, water, transportation, and communications. Jason holds a bachelor of science and master of engineering from the State University of New York at Binghamton, and a master’s of engineering degree in electrical engineering from Cornell University.
Enrich your SANS training experience! Evening talks by our instructors and selected subject-matter experts help you broaden your knowledge. You’ll hear from the voices that matter in information security and get the most for your training dollar.

General Session – Welcome to SANS
Bryan Simon
Join us for a 30-minute overview to help you get the most out of your SANS training experience. You will receive event information and learn about programs and resources offered by SANS. This brief session will answer many questions and get your training off to a great start. This session will be valuable to all attendees but is highly recommended for first-time attendees.

Moving Past Just Googling It: Harvesting and Using OSINT
Micah Hoffman
Every single day we search for things on the Internet. Defenders research a domain or IP that contains malware. Attackers look for email addresses for an upcoming phishing campaign. DFIR people examine locations and usernames that they acquired from a subject’s computer. Policy and compliance people examine the risk that employees in their organizations might bring to work. Recruiters scour the Internet looking for candidates. And normal people shop, date, geolocate, post, tweet, and otherwise send a huge amount of data to the public Internet. Come join Micah Hoffman as we examine how OSINT (Open-Source Intelligence) can reveal interesting content about your work and personal lives.

Automating NIST Risk Management Framework (RMF)/800-53
Peter Szczepankiewicz
Doing good cybersecurity is so much more than inspection compliance. We’ve all seen it. You’re 100% compliant and can still get hacked! But after decades of gathering security information from your global enterprise, measured in gross tonnage, the converse is also true. Weighed down with tons of data, very interesting things start to happen when you view portions of your data through the lens of the NIST Risk Management Framework. You realize that there are phantom scripts running around in your network, written by your own staff. People on vacation have accounts that are somehow still actively logging in and out, from many VPNs! Your vulnerabilities, coupled with your outbound packets, reveal file-less malware that doesn’t use command and control. As a standard course of action, one should be detecting violations in real time, as well as searching with this lens. Come learn about specific real-time correlation rules that your peers are using for NIST RMF and join in this discussion about what is working in the field. While not all of NIST RMF can be automated, what can be automated should be automated.
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.

Future Training Events

See www.sans.org for more information.

Future Summit Events

ICS Security
Orlando, FL
Mar 18-25

Blue Team
Louisville, KY
Apr 11-18

Cloud Security
San Jose, CA
Apr 29 - May 6

Security Operations
New Orleans, LA
Jun 24 - Jul 1

DFIR
Austin, TX
Jul 25 - Aug 1

Security Awareness
San Diego, CA
Aug 5-14

Future Training Events

Future Summit Events

Future Community SANS Events
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 May 8, 2019. 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.

Pay Early and Save*

<table>
<thead>
<tr>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-3-19</td>
<td>$350</td>
<td>4-24-19</td>
<td>$200</td>
</tr>
</tbody>
</table>

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

SANS Voucher Program

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

www.sans.org/vouchers

SANS Voucher Program

Registration Information

Register online at www.sans.org/atlanta

We recommend registering early to 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 server will accept your registration. Sold-out courses will be removed from the online registration. Everyone must complete the online registration form. We do not take registrations by phone.

Grand Hyatt Atlanta in Buckhead

3300 Peachtree Road NE
Atlanta, GA 30305
404-237-1234
www.sans.org/atlanta/location

Recently named one of USA Today’s 10 Best Atlanta hotels, Grand Hyatt Atlanta is the perfect combination of sophistication, state-of-the-art amenities, and southern charm. Conveniently located on Peachtree Street, the Grand Hyatt Atlanta puts you in the heart of the city’s best shopping, dining, sports and live music.

Special Hotel Rates Available

A special discounted rate of $159 plus applicable taxes will be honored based on space availability.

Government per diem rooms at the prevailing rate are available with proper ID. These rates include high-speed Internet in your room and are only available through May 6, 2019.

Top 3 reasons to stay at the Grand Hyatt Atlanta in Buckhead

1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Grand Hyatt Atlanta in Buckhead, you can further network with your industry peers and remain in the center of the activity surrounding the training event.
3. SANS schedules morning and evening events at the Grand Hyatt Atlanta in Buckhead that you won’t want to miss!

Hotel Information

Pay Early and Save*  Use code EarlyBird19 when registering early

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 May 8, 2019. 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.
Newsletters

NewsBites
Twice-weekly, high-level executive summaries of the news most 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 newly discovered attack vectors, vulnerabilities with active new exploits, how recent attacks worked, and other valuable data.

Webcasts

Ask the Experts Webcasts
SANS experts bring current and timely information on relevant topics in IT security.

Analyst Webcasts
Analyst Webcasts share highlights and key results from our Analyst Program whitepapers and surveys.

WhatWorks Webcasts
The SANS WhatWorks webcasts share 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 (SANS.org account not required)

- 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 September 19th. Register today at www.sans.org/san-diego-fall

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.

To be removed from future mailings, please contact unsubscribe@sans.org or (301) 654-SANS (7267). Please include name and complete address. NALT-BRO-SAN-DIEGO-FALL-2018