SANS Miami 2016

November 7-12

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

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

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Five courses on

CYBER DEFENSE
ETHICAL HACKING
DIGITAL FORENSICS
SECURITY MANAGEMENT

"This course is most applicable with a direct business value, and is exactly what the defenders need."
-David Grotenberg,
TECO Energy

SAVE $400
when you register and pay by September 14th using code **EarlyBird2016**

GIAC
GIAC-Approved Training

www.sans.org/miami

SANS Instructors

SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses. This guarantees that what you learn in class will be up to date and relevant to your job. The SANS Miami 2016 lineup of instructors includes:

Ted Demopoulos
Certified Instructor
@TedDemop

Ronald Hamann
SANS Instructor
@airforceteacher

Paul A. Henry
Senior Instructor
@phenrycissp

Keith Palmgren
Senior Instructor
@kpalmgren

Anuj Soni
Certified Instructor
@asoni

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 7.

KEYNOTE: ***Debunking the Complex Password Myth*** – Keith Palmgren

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

Evolving Threats – Paul A. Henry

Purple Teaming: Red and Blue, Not Red vs. Blue – Jorge Orchilles

Need for Speed: Malware Edition – Anuj Soni

Developers: Five Things I Want You to Keep Doing – Ron Hamann

The training campus for SANS Miami 2016 is in the contemporary, 22-story boutique-style Sonesta Coconut Grove Miami, just steps from the fashionable shopping, dining and nightlife of CocoWalk.

SEE PAGE 13

Save $400 when you register and pay by Sept 14th using code EarlyBird2016

Courses-at-a-Glance

		MON 11-7	TUE 11-8	WED 11-9	THU 1-10	FRI 1-11	SAT 11-12
SEC301	Intro to Information Security	Page 2					
SEC401	Security Essentials Bootcamp Style	Page 3					
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	Page 4					
FOR508	Advanced Digital Forensics and Incident Response	Page 5					
MGT514	IT Security Strategic Planning, Policy, and Leadership	Page 6					

The Value of SANS Training & YOU

EXPLORE

- Read this brochure and note the courses that will enhance your role in your organization
- Use the Career Roadmap (www.sans.org/media/security-training/roadmap.pdf) to plan your growth in your chosen career path

RELATE

- Consider how security needs in your workplace will be met with the knowledge you'll gain in a SANS course
- Know the education you receive will make you an expert resource for your team

VALIDATE

- Pursue a GIAC Certification after your training to validate your new expertise
- Add a NetWars challenge to your SANS experience to prove your hands-on skills

SAVE

- Register early to pay less using early-bird specials
- Consider the SANS Voucher Program or bundled course packages to make the most of your training budget

ADD VALUE

- Network with fellow security experts in your industry
- Prepare thoughts and questions before arriving to share with the group
- Attend SANS@Night talks and activities to gain even more knowledge and experience from instructors and peers alike

ALTERNATIVES

- If you cannot attend a live training event in person, attend the courses virtually via SANS Simulcast
- Use SANS OnDemand or vLive to complete the same training online from anywhere in the world, at any time

ACT

- Bring the value of SANS training to your career and organization by registering for a course today, or contact us at 301-654-SANS with further questions

Return on Investment

SANS live training is recognized as the best resource in the world for information security education. With SANS, you gain significant returns on your InfoSec investment. Through our intensive immersion classes, our training is designed to help your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited.

REMEMBER

the SANS promise:

You will be able to apply our information security training the day you get back to the office!

SEC301:

Intro to Information Security

SANS

Five-Day Program
Mon, Nov 7- Fri, Nov 11
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Keith Palmgren

To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

- Are you new to information security and in need of an introduction to the fundamentals?
- Are you bombarded with complex technical security terms that you don't understand?
- Are you a non-IT security manager who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o'clock news?
- Do you need to be conversant in basic security concepts, principles, and terms, even if you don't need "deep in the weeds" detail?
- Have you decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification?

If you answer yes to any of these questions, the **SEC301: Introduction to Information Security** training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised five-day comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

This course is designed for students who have no prior knowledge of security and limited knowledge of technology. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

Authored by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next course up the line, **SEC401: Security Essentials Bootcamp**. It also delivers on the SANS promise: ***You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.***

"The course is excellent as is! Great flow from topic to topic."
-Danielle Alexander, Bechtel

www.giac.org/gisf

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

"The instructor was excellent and the basis for my new knowledge of computer cyber-crimes for law enforcement. This course will help with our investigation and detection of cyber-fraud in the field."
-Justine Killeen, NYPD

Keith Palmgren *SANS Senior Instructor*

Keith Palmgren is an IT security professional with 26 years of experience in the field. He began his career with the U.S. Air Force working with cryptographic keys and codes management. He also worked in what was at the time the newly-formed computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a senior security architect working on engagements with the DoD and the National Security Agency. As security practice manager for both Sprint and Netigy, Keith built and ran the security consulting practice, responsible for all security consulting world-wide and for leading dozens of security professionals on many consulting engagements across all business spectrums. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. As a trainer, Keith has satisfied the needs of nearly 5,000 IT professionals and authored 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications. @kpalmgren

SEC401:
Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Nov 7 - Sat, Nov 12
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Paul A. Henry

www.giac.org/gsec

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"This course will give me valuable insight to support my job as a cybersecurity engineer."
-Erik Miller, Exelon

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

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

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization's critical information assets and business systems. This course will show you how to prevent your organization's security problems from being headline news in the *Wall Street Journal*!

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
- Forensic analysts, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

With the rise of 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'll need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

Paul A. Henry *SANS Senior Instructor*

Paul is one of the world's foremost global information security and computer forensic experts, with more than 20 years' experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. He also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the U.S. Department of Defense's Satellite Data Project, and both government and telecommunications projects throughout Southeast Asia. Paul is frequently cited by major publications as an expert on perimeter security, incident response, computer forensics, and general security trends, and serves as an expert commentator for network broadcast outlets such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications such as the *Information Security Management Handbook*, to which he is a consistent contributor. Paul is a featured speaker at seminars and conferences worldwide, delivering presentations on diverse topics such as anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, perimeter security, and incident response. @phenrycissp

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Nov 7 - Sat, Nov 12
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Ronald Hamann

www.giac.org/gcih

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

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

"The information provided in this course is targeted and relevant to defend against exploits."
-Bernard Hafey, Ingram Micro

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. **As defenders, it is essential we understand these hacking tools and techniques.**

Who Should Attend

- Incident handlers
- 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 teaches you methods for testing your defenses and how to identify weaknesses in your network and systems."
-Rene Graf, Federal Home Loan Bank

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 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 for, exploiting, and defending systems. This 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.**

"This course really puts the state of things in perspective. We need to be proactive to combat the threats of the Internet, and this is a great place to start."
-Jonathan Manafi, McIlhenny Company

Ronald Hamann *SANS Instructor*

Ron is a retired U.S. Air Force officer with almost 20 years experience in various areas of IT, from software development to system administration, security, and Cyber Command and Control. Ron analyzed and developed security orders for the Air Force network, and is adept at breaking down technical security issues for senior leaders and lay people. Ron also was an accomplished security instructor for the Air Force, teaching over 30 security classes to Air Force officers, enlisted personnel, and civilians. @airforceteacher

FOR508:

Advanced Digital Forensics and Incident Response

SANS

Six-Day Program
Mon, Nov 7 - Sat, Nov 12
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Anuj Soni

www.giac.org/gcfa

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"Great material and instructor, the lab scenarios were very well done and fun to investigate." -Bryan Thiry, Lockheed Martin

FOR508: Advanced Digital Forensics and Incident Response will help you determine:

- How the breach occurred
- How systems were affected and compromised
- What attackers took or changed
- How to contain and mitigate the incident

DAY 0: A 3-letter government agency contacts you to say critical information was stolen through a targeted attack on your organization. They won't tell how they know, but they identify several breached systems within your enterprise. An advanced persistent threat adversary, aka an APT, is likely involved – the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Who Should Attend

- Incident response team leaders and members
- Security Operations Center personnel and information security practitioners
- Experienced digital forensic analysts
- System administrators
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 graduates

Over 80% of all breach victims learn of a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years.

"I liked the focus on doing the things that matter most in an incident response, and I learned a lot during time-line labs about the importance of knowing how the timesharing is modified." -Niklas Andersson, Coresec Systems

Incident response tactics and procedures have evolved rapidly over the past several years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in your enterprise; they are compromising hundreds. Your team can no longer afford antiquated incident response techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident.

This in-depth incident response course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks, including APT adversaries, organized crime syndicates, and hactivism. Constantly updated, FOR508 addresses today's incidents by providing hands-on incident response tactics and techniques that elite responders are successfully using in real-world breach cases.

GATHER YOUR INCIDENT RESPONSE TEAM – IT'S TIME TO GO HUNTING!

Anuj Soni *SANS Certified Instructor*

Anuj Soni is a Senior Threat Researcher at Cylance, where he performs malware research and reverse engineering activities. Since entering the information security field in 2005, Anuj has performed numerous intrusion investigations to help government and commercial clients mitigate attacks against the enterprise. His malware hunt skills and technical analysis abilities have resulted in the successful identification, containment, and remediation of multiple threat actor groups. Anuj has analyzed hundreds of malware samples to assess function, purpose, and impact, and his recommendations have improved the security posture of the organizations he supports. @asoni

MGT514:

IT Security Strategic Planning, Policy, and Leadership

SANS

Five-Day Program
Mon, Nov 7- Fri, Nov 11
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: Ted Demopoulos

SANS Technology Institute
www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"This was excellent training with encyclopedic coverage of the topic, and the instructor was fantastic with lots of wisdom and real-life examples."
-Alexander Kotkov, Ernst and Young

"The balance is great and the full policy in the appendix helped to round out the analysis. The policy discussions and slides were quite helpful."
-Jason Popp, Nordstrom Inc.

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

This course teaches security professionals how to do three things:

Who Should Attend

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

Develop Strategic Plans

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

Create Effective Information Security Policy

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

Develop Management and Leadership Skills

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

Ted Demopoulos *SANS Certified Instructor*

Ted Demopoulos' first significant exposure to computers was in 1977 when he had unlimited access to his high school's PDP-11 and hacked at it incessantly. He consequently almost flunked out but learned he liked playing with computers a lot. His business pursuits began in college and have been ongoing ever since. His background includes over 25 years of experience in information security and business, including 20+ years as an independent consultant. Ted helped start a successful information security company, was the CTO at a "textbook failure" of a software startup, and has advised several other businesses. Ted is a frequent speaker at conferences and other events, quoted often by the press. He also has written two books on social media, has an ongoing software concern in Austin, Texas in the virtualization space, and is the recipient of a Department of Defense Award of Excellence. In his spare time, he is a food and wine geek, enjoys flyfishing, and plays with his children. @TedDemop

SANS@NIGHT EVENING TALKS

Enrich your SANS training experience!

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

KEYNOTE: **Debunking the Complex Password Myth** — *Keith Palmgren*

Perhaps the worst advice you can give a user is "choose a complex password." The result is the impossible-to-remember password requiring the infamous sticky note on the monitor. In addition, that password gets used at a dozen sites at home, AND the very same password gets used at work. The final result ends up being the devastating password compromise. In this one-hour talk, we will look at the technical and non-technical (human nature) issues behind passwords. Attendees will gain a more complete understanding of passwords and receive solid advice on creating more easily remembered AND significantly stronger passwords at work and at home, for their users, for themselves and even for their children.

Infosec Rock Star: Geek Will Only Get You So Far

Ted Demopoulos

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

Evolving Threats — *Paul A. Henry*

For nearly two decades, defenders have fallen into the "Crowd Mentality Trap" and have simply settled on doing the same thing everyone else was doing. While at the same time, attackers have clearly evolved both in terms of malware delivery vectors and attack methodology. Today our defenses focus primarily on the gateway and upon attempting to outwit attackers' delivery methods. This leaves us woefully exposed and according to a recent Data Breach Report, it has resulted in 3,765 incidents, 806 million records exposed, and $157 billion in data breach costs in only the past six years. The Evolving Threats presentation is updated monthly and provides insight into mitigations of our most current threats.

Purple Teaming: Red and Blue, Not Red vs. Blue — *Jorge Orchilles*

We have all heard that defense should inform offense and that offense should inform defense. How does this work from a practical perspective? In this talk, we will cover the evolution of Red Teaming to bring more value to the Blue Teams and vice-versa by introducing a new perspective, the Purple Team. We will present a test case of how Red Teams can bring value to incident responders and how incident responders bring value to Red Teams.

Need for Speed: Malware Edition — *Anuj Soni*

Performing malware analysis can be a thrilling activity, but it can also be time-consuming and tedious. During this talk, I'll use real malware samples to propose strategies to accelerate the malicious code analysis process. Whether you're new to this topic area or familiar with its challenges, this discussion will give you an appreciation for reverse engineering and equip you with tips and tricks to speed up your investigation.

Developers: Five Things I Want You to Keep Doing — *Ron Hamann*

I want a new boat. If you guys will keep making these mistakes, I'll keep getting billable hours and can buy an even bigger boat! Tongue in cheek title for overview of development errors in web and desktop applications that cause major security flaws and loss of customer data.

Enhance Your Training Experience

WITH:

Even More Training Value

Add an

OnDemand Bundle & GIAC Certification Attempt*

to your course within seven days of this event for just $689 each.

SPECIAL PRICING

Extend Your Training Experience with OnDemand Bundle

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

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

-Robert Jones, Team Jones, Inc.

Get Certified with GIAC Certification

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

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

-Christina Ford, Department of Commerce

MORE INFORMATION

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

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

Employers need good talent. Veterans need good jobs. SANS VetSuccess Immersion Academy delivers both.

Introducing the SANS VetSuccess Immersion Academy, an intensive, accelerated program that provides the real-world training and certifications needed to fill critical jobs in cybersecurity.

For employers, the academy is a faster, more reliable, and less expensive way to find, train, certify, and employ highly qualified cybersecurity talent.

For transitioning veterans, the academy provides free accelerated training and certifications to quickly and effectively launch careers in cybersecurity.

Find out how your organization can benefit from hiring graduates or sponsoring an academy to meet your specific talent needs.

Read the Pilot Program Results Report
Visit sans.org/vetsuccess

SANS | CyberTalent IMMERSION ACADEMY

Read the Pilot Program Results Report
Visit sans.org/vetsuccess

Women's Academy Pilot
1st cohort graduation
Summer 2016

SANS VOUCHER PROGRAM

The SANS Voucher Program allows an organization to manage their training budget from a single SANS Account, potentially receive bonus funds based on their investment level, and centrally administer its training.

Training Investment & Bonus Funds

To open a Voucher Account, an organization pays an agreed-upon training investment. Based on the amount of the training investment, an organization could be eligible to receive bonus funds.

The investment and bonus funds:

- Can be applied to **any live or online SANS training course, SANS Summit, GIAC certification, or certification renewal***
- Can be increased at any time by making additional investments
- Need to be utilized within 12 months, however, the term can be extended by investing additional funds before the end of the 12-month term

*Current exceptions are the Partnership Program, Security Awareness Training, and SANS workshops hosted at events and conferences run by other companies.

Flexibility & Control

The online SANS Admin Tool allows the organization's Program Administrator to manage the account at anytime from anywhere.

With the SANS Admin Tool, the Administrator can:

- Approve student enrollment and manage fund usage
- View fund usage in real time
- View students' certification status and test results
- Obtain OnDemand course progress by student per course

By creating a Voucher Account, your organization can:

- Simplify the procurement process with a single invoice and payment
- Easily change course attendees if previous plans change
- Lock-in your hard fought training budget and utilize it over time
- Control how, where, and for whom funds are spent
- Allow employees to register for training while managing approvals centrally

Getting Started

Complete and submit the form online at **www.sans.org/vouchers** and a SANS representative in your region will contact you within 24 business hours.

Get started today and within as little as one week, we can create your Account and your employees can begin their training.

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events www.sans.org/security-training/by-location/all
Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers

Community SANS www.sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

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

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

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

ONLINE TRAINING

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

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

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

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

FUTURE SANS TRAINING EVENTS

Chicago 2016
Chicago, IL | Aug 22-27

Alaska 2016
Anchorage, AK | Aug 22-27

Virginia Beach 2016
Virginia Beach, VA | Aug 22 - Sep 2

NORTHERN VIRGINIA
Crystal City 2016
Crystal City, VA | Sep 6-11

Network Security 2016
Las Vegas, NV | Sep 10-19

Security Leadership
SUMMIT & TRAINING 2016
Dallas, TX | Sep 27 - Oct 4

Seattle 2016
Seattle, WA | Oct 3-8

Baltimore 2016
Baltimore, MD | Oct 10-15

Tysons Corner 2016
Tysons Corner, VA | Oct 22-29

San Diego 2016
San Diego, CA | Oct 23-28

Pen Test Hackfest
SUMMIT & TRAINING 2016
Crystal City, VA | Nov 2-9

Healthcare Cybersecurity
SUMMIT & TRAINING 2016
Houston, TX | Nov 14-21

San Francisco 2016
San Francisco, CA | Nov 27 - Dec 2

Cyber Defense Initiative 2016
Washington, DC | Dec 10-17

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

SANS MIAMI 2016

Hotel Information

Training Campus
Sonesta Coconut Grove Miami

2889 McFarlane Road
Coconut Grove, FL 33133 | 305.529.2828
www.sans.org/event/miami-2016/location

A contemporary, 22-story boutique-style hotel in the heart of Coconut Grove, just steps from the fashionable shopping, dining and nightlife of CocoWalk. You are minutes from downtown Miami's Business District (Brickell Avenue), Port of Miami, South Beach, Coral Gables, University of Miami and the beaches of Key Biscayne.

Special Hotel Rates Available

A special discounted rate of $199.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. This rate is only available through Friday, October 21, 2016. A $3.00 service fee may apply.

Top 5 reasons to stay at the Sonesta Coconut Grove Miami

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 Sonesta Coconut Grove Miami 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 Sonesta Coconut Grove Miami that you won't want to miss!
5. Everything is in one convenient location!

SANS MIAMI 2016

Registration Information

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

Register online at www.sans.org/miami

Select your course or courses and indicate whether you plan to test for GIAC certification.

If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Use code **EarlyBird16** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**9-14-16**	**$400.00**	**10-5-16**	**$200.00**

Some restrictions apply.

SANS Voucher Program

Expand your training budget!

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

www.sans.org/vouchers

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by October 19, 2016 – processing fees may apply.

Open a **SANS Account** today to enjoy these FREE resources:

WEBCASTS

Ask The Expert Webcasts – SANS experts bring current and timely information on relevant topics in IT Security.

Analyst Webcasts – A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

WhatWorks Webcasts – The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.

Tool Talks – Tool Talks are designed to give you a solid understanding of a problem, and to show how a vendor's commercial tool can be used to solve or mitigate that problem.

NEWSLETTERS

NewsBites – Twice-weekly high-level executive summary of the most important news relevant to cybersecurity professionals

OUCH! – The world's leading monthly free security-awareness newsletter designed for the common computer user

@RISK: The Consensus Security Alert – A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data

OTHER FREE RESOURCES

- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQs
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

www.sans.org/security-resources