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

SANS Atlanta 2017

May 30 - June 4

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

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Seven courses in:

CYBER DEFENSE
DETECTION & MONITORING
PENETRATION TESTING
INCIDENT RESPONSE
DIGITAL FORENSICS
ETHICAL HACKING
MANAGEMENT

"This training has been valuable both to me and my career – the course material and the instructor are an awesome match."
-Camille Crosby, The William Carter Company

GIAC CERTIFICATIONS
GIAC-Approved Training

SAVE $400
Register and pay by April 5th – Use code **EarlyBird17**

www.sans.org/atlanta

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 Atlanta 2017 lineup of instructors includes:

Chris Christianson
Instructor
@cchristianson

G. Mark Hardy
Certified Instructor
@g_mark

Seth Misenar
Senior Instructor
@sethmisenar

Michael Murr
Principal Instructor
@mikemurr

My-Ngoc Nguyen
Certified Instructor
@MenopN

Bryan Simon
Certified Instructor
@BryanOnSecurity

Peter Szczepankiewicz
Certified Instructor
@_s14

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 8.

KEYNOTE: ***Actionable Detects: Blue Team Cyber Defense Tactics***
Seth Misenar

The End of Banking as We Know It:
How Crypto Currencies and e-Payments Are Breaking Up a Centuries-Old Monopoly
G. Mark Hardy

Save $400 when you register and pay by April 5th using code EarlyBird17

Courses at a Glance

	TUE 5-30	WED 5-31	THU 6-1	FRI 6-2	SAT 6-3	SUN 6-4
SEC301 Intro to Information Security	Page 1					
SEC401 Security Essentials Bootcamp Style	Page 2					
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	Page 3					
SEC511 Continuous Monitoring and Security Operations	Page 4					
FOR578 Cyber Threat Intelligence	Page 5					
MGT414 SANS Training Program for CISSP® Certification	Page 6					
MGT512 SANS Security Leadership Essentials for Managers with Knowledge Compression™	Page 7					

SEC301:

Intro to Information Security

SANS

Five-Day Program
Tue, May 30 - Sat, June 3
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: My-Ngoc Nguyen

www.giac.org/gisf

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

"This course was the perfect blend of technical and practical information for someone new to the field, and I would recommend it!"
-Steve Mecco, Draper

"This training is very valuable as I start my position in IT security. There is so much to learn and many good concepts."
-Amy Swanson, Truven Health Analytics

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

- Do you have basic computer knowledge but are 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 (with some technical knowledge) 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 a basic knowledge of computers and technology but no prior knowledge of cybersecurity. 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.***

My-Ngoc Nguyen *SANS Certified Instructor*

My-Ngoc Nguyen (pronounced Mee-Nop Wynn) is the CEO/Principal Consultant for Secured IT Solutions. She has 15 years of experience in information systems and technology, with the past 12 years focused on cybersecurity and information assurance for both the government and commercial sectors. My-Ngoc is highly experienced in IT security and risk methodologies, and in legal and compliance programs. She led a cybersecurity program under a federal agency for a highly-regulated, first-of-a-kind project of national importance. With that experience, she has been helping client organizations in both the public and private sectors implement secure and compliant business processes and IT solutions using defense-in-depth and risk-based approaches. Along with a master's degree in management information systems, she carries top security certifications, including GPEN, GCIH, GSEC, and CISSP, and is a former QSA. She is an active member of the FBI's InfraGard, the Information Systems Security Association (ISSA), the Information Systems Audit and Control Association (ISACA), and the International Information Systems Security Certification Consortium (ISC). My-Ngoc co-founded the non-profit public service organization CyberSafeNV to raise security awareness among Nevada residents and is presently the organization's chairperson. @MenopN

SEC401:
Security Essentials Bootcamp Style

SANS

Six-Day Program
Tue, May 30 - Sun, June 4
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Chris Christianson

www.giac.org/gsec

www.sans.edu

www.sans.org/8140

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

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

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

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
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- 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.

Chris Christianson *SANS Instructor*
Chris Christianson is an Information Security Consultant based in Northern California with 20 years of experience and many technical certifications, including the CCSE, CCDP, CCNP, GSEC, CISSP, IAM, GCIH, CEH, IEM, GCIA, GREM, GPEN, GWAPT, GISF, and GCED. He holds a bachelor of science degree in management information systems and was the Assistant Vice President of the Information Technology Department at one of the nation's largest credit unions. Chris has also been an expert speaker at conferences and a contributor to numerous industry articles. @cchristianson

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Tue, May 30 - Sun, June 4
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Michael Murr

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 material and breadth is massive but it is so well constructed that anyone would learn something."
-Dan Trueman, Novae Group

This course enables you to turn the tables on computer attackers by helping you to 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, 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 introduces you to the various tools that are available to analysts and investigators that are used to perform tasks better and it really gives you a feel of how attacks occur. This has been a great hands-on experience!"
-Sheryll Anne Tiauzon, The Coca-Cola Company

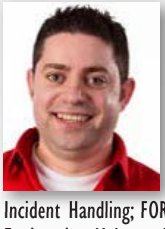
www.giac.org/gcih

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

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



Michael Murr *SANS Principal Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years. He has conducted numerous investigations and computer forensic examinations, and performed specialized research and development. Michael has taught SEC504: Hacker Tools, Techniques, Exploits and Incident Handling; FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting; and FOR610: Reverse-Engineering Malware. He has also led SANS Online Training courses, and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. He holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about digital forensics on his forensic computing blog (www.forensicblog.org). @mikemurr

SEC511:

Continuous Monitoring and Security Operations

New Extended Bootcamp Hours to Enhance Your Skills

SANS

Six-Day Program
Tue, May 30 - Sun, June 4
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Laptop Required
Instructor: Bryan Simon

www.giac.org/gmon

www.sans.edu

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

"This training provides excellent information for self assessment of current SEC practices. I picked up a lot of tricks and new perspectives."
-KYLE MONTGOMERY, NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying to prevent and combat cyber attacks, but despite this tremendous effort organizations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses.

Who Should Attend

- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center analysts, engineers, and managers
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)
- Computer Network Defense analysts

The underlying challenge for organizations victimized by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organizations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

"I'm looking forward to helping small businesses get 'cyber healthy' by applying the risk-relevant portions of this knowledge. AWESOME!" -ADAM AUSTIN, H-BAR CYBER SOLUTIONS

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach is early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

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 12 GIAC certifications including GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, GCUX, and GISF. 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

FOR578:
Cyber Threat Intelligence

SANS

Five-Day Program
Tue, May 30 - Sat, June 3
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Peter Szczepankiewicz

Make no mistake: current network defense, threat hunting, and incident response practices contain a strong element of intelligence and counterintelligence that cyber analysts must understand and leverage in order to defend their networks, proprietary data, and organizations.

FOR578: Cyber Threat Intelligence will help network defenders, threat hunting teams, and incident responders to:

- Understand and develop skills in tactical, operational, and strategic-level threat intelligence
- Generate threat intelligence to detect, respond to, and defeat advanced persistent threats (APTs)
- Validate information received from other organizations to minimize resource expenditures on bad intelligence
- Leverage open-source intelligence to complement a security team of any size
- Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX.

Who Should Attend

- Incident response team members
- Threat hunters
- Security Operations Center personnel and information security practitioners
- Experienced digital forensic analysts
- Federal agents and law enforcement officials
- SANS FOR408, FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that is used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture.

Cyber threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats. Malware is an adversary's tool but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders.

During a targeted attack, an organization needs a top-notch and cutting-edge threat hunting or incident response team armed with the threat intelligence necessary to understand how adversaries operate and to counter the threat. **FOR578: Cyber Threat Intelligence** will train you and your team in the tactical, operational, and strategic-level cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, and organizations more aware of the evolving threat landscape.

THERE IS NO TEACHER BUT THE ENEMY!

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

"Outstanding course material and instructor presentation! It truly drills into the analytic process, while remaining technical. I highly recommend this course to anyone performing any level of intelligence support to defensive cyber operations."
-Thomas L., U.S. Air Force

"I absolutely loved this class! The instructor provided a great framework for CTI that I will use to be more effective."
-Nate DeWitt, eBay, Inc.

Peter Szczepankiewicz *SANS Certified Instructor*

Formerly working 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. People lead technology, not the other way around, so Peter works daily to bring actionable intelligence out of disparate security devices for customers, making systems interoperable. "Putting together networks only to tear them apart is just plain fun," explains Peter, "and it allows students to take the information learned from books and this hands-on experience back to their particular work place." @_s14

MGT414:

SANS Training Program for CISSP® Certification

SANS

Six-Day Program
Tue, May 30 - Sun, June 4
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: Seth Misenar

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam.

MGT414 focuses solely on the eight domains of knowledge as determined by (ISC)² that form a critical part of the CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

Who Should Attend

- Security professionals who want to understand the concepts covered in 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 to apply the eight domains of knowledge to their current activities

You Will Be Able To:

- Understand the eight domains of knowledge that are covered on the CISSP® exam
- Analyze questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the eight domains of knowledge
- Apply the skills learned across the eight domains to solve security problems when you return to work

Note:
The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)².

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

Take advantage of the SANS CISSP® Get Certified Program currently being offered.
www.sans.org/cissp

www.giac.org/gisp

www.sans.org/8140

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

"This course is a great way to refresh and review my knowledge before sitting for the CISSP exam. Not only is the content presented in a clear and concise manner, it is prepared logically for ease of comprehension."
-Glenn Carr, Leidos

Seth Misenar *SANS Senior Instructor*

Seth Misenar is the founder of Jackson, Mississippi-based Context Security, where he provides information security thought leadership, independent research, and security training. Seth's background includes network and web application penetration testing, vulnerability assessment, regulatory compliance, security architecture design, and general security consulting. He has previously served as both physical and network security consultant for Fortune 100 companies and the Health Insurance Portability and Accountability Act, and as information security officer for a state government agency. Prior to becoming a security geek, Seth received a bachelor's of science degree in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is no stranger to certifications and thus far has achieved credentials that include CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. @sethmisenar

MGT512:

SANS Security Leadership Essentials for Managers with Knowledge Compression™

SANS

Five-Day Program
Tue, May 30 - Sat, June 3
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop Recommended
Instructor: G. Mark Hardy

www.giac.org/gslc

www.sans.edu

www.sans.org/8140

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

"This course is very comprehensive and provides excellent awareness of how web servers and interaction work. Worth your time!"
-Steve McGee, Curaspan Health Group

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

Who Should Attend

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

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

Knowledge Compression™

Maximize your learning potential!

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

G. Mark Hardy *SANS Certified Instructor*

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

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:

Actionable Detects: Blue Team Cyber Defense Tactics

Seth Misenar

Organizations relying on third parties to detect breaches can go almost a full year before finding out they have been compromised. Detect the breach yourself, and on average you will find it within about a month of the initial occurrence. Considering detection and defense against modern adversaries too costly to perform yourself can be a very expensive miscalculation considering the substantially increased price of response and recovery with breach duration.

Seth Misenar's ever-evolving Actionable Detects presentation provides you with the analysis, tactics, techniques, and procedures to once again take pride in your Blue Team Cyber capabilities. Not applying these lessons learned could prove costly in the face of adapting threat actors. Dig in and learn to hold your head high when talking about your defensive cyber operations capabilities.

The End of Banking as We Know It: How Crypto Currencies and e-Payments Are Breaking Up a Centuries-Old Monopoly

G. Mark Hardy

Are we finally ready to go mainstream with alt-currency? Bitcoin got off to a slow start but has attracted millions of VC dollars in the last two years. We'll look at this brave new world of electronic money to understand what it is, how it works, what it can (and cannot) do, and probabilities of success or failure. We'll examine spin-off technologies such as blockchains, and look into the mechanics behind electronic payment systems such as Apple Pay, CurrentC, and Softcard. We'll even talk about why crooks love Bitcoin for ransomware extortion, and dig into the mechanics of how credit card fraud works, and whether that might be going away as well.

Enhance Your Training Experience

Add an

OnDemand Bundle & GIAC Certification Attempt*

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

SPECIAL PRICING

Extend Your Training Experience with an OnDemand Bundle

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

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

-Robert Jones, Team Jones, Inc.

Get Certified with GIAC Certifications

GIAC CERTIFICATIONS

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

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

-Christina Ford, Department of Commerce

MORE INFORMATION

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

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

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events

Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers

sans.org/security-training/by-location/all

Community SANS

Live Training in Your Local Region with Smaller Class Sizes

sans.org/community

Private Training

Your Location! Your Schedule!

sans.org/private-training

Mentor

Live Multi-Week Training with a Mentor

sans.org/mentor

Summit

Live IT Security Summits and Training

sans.org/summit

ONLINE TRAINING

OnDemand

E-learning Available Anytime, Anywhere, at Your Own Pace

sans.org/ondemand

vLive

Online, Evening Courses with SANS' Top Instructors

sans.org/vlive

Simulcast

Attend a SANS Training Event without Leaving Home

sans.org/simulcast

OnDemand Bundles

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

Training Events

Tyssons Corner Spring	McLean, VA	Mar 20-25
Pen Test Austin	Austin, TX	Mar 27 - Apr 1

Baltimore Spring	Baltimore, MD	Apr 24-29

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

San Antonio – August	San Antonio, TX	Aug 6-11
Boston	Boston, MA	Aug 7-12
New York City	New York, NY	Aug 14-19
Salt Lake City	Salt Lake City, UT	Aug 14-19
Chicago	Chicago, IL	Aug 21-26

Summit Events

ICS Security	Orlando, FL	Mar 19-27
Threat Hunting and IR	New Orleans, LA	Apr 18-25
Automotive Cybersecurity	Detroit, MI	May 1-8
Security Operations Center	Washington, DC	Jun 5-12
Digital Forensics	Austin, TX	Jun 22-29
ICS & Energy	Houston, TX	Jul 10-14
Security Awareness	Nashville, TN	Jul 31 - Aug 9

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.

SANS ATLANTA 2017

Hotel Information

Training Campus

Grand Hyatt Atlanta in Buckhead

3300 Peachtree Road NE
Atlanta, GA 30305
888-421-1442
sans.org/event/atlanta-2017/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, this Buckhead, Atlanta hotel puts you in the heart of Atlanta's best shopping, dining, sports and live music.

Special Hotel Rates Available

A special discounted rate of $156.00 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 May 8, 2017. To book a room, please call 888-421-1442 and mention you are with SANS.

Top 5 reasons to stay at the Grand Hyatt Atlanta

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 Grand Hyatt Atlanta 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 Grand Hyatt Atlanta that you won't want to miss!
5. Everything is in one convenient location!

SANS ATLANTA 2017

Registration Information

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

Register online at www.sans.org/atlanta

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.

Use code **EarlyBird17** when registering early

Pay Early and Save*

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

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

SANS Voucher Program

Expand your training budget!

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

www.sans.org/vouchers

Cancellation

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 May 3, 2017 – 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/account