SANS

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

CHICAGO 2017

August 21-26

Protect Your Business and Advance Your Career

Nine hands-on, immersion-style information security courses taught by real-world practitioners

CYBER DEFENSE
DETECTION & MONITORING
PENETRATION TESTING
ETHICAL HACKING
DIGITAL FORENSICS
MANAGEMENT
ICS/SCADA SECURITY

GIAC CERTIFICATIONS

"Out of all the training I have taken, this has been the most informative. SANS can't be beat."

-Charles Chastain, Patagonia

SAVE $400

Register and pay by June 28th – Use code **EarlyBird17**

www.sans.org/chicago

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 Chicago 2017 lineup of instructors includes:

Chris Christianson
Certified Instructor
@cchristianson

Tim Conway
Instructor

Christopher Crowley
Principal Instructor
@CCrowMontance

Ted Demopoulos
Principal Instructor
@TedDemop

Mick Douglas
Instructor
@BetterSafetyNet

David Mashburn
Instructor
@d_mashburn

Cindy Murphy
Certified Instructor
@cindymurph

My-Ngoc Nguyen
Certified Instructor
@MenopN

Keith Palmgren
Senior Instructor
@kpalmgren

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 10.

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

Women's CONNECT Event
Hosted by the SANS COINS Program and the ISSA International Women in Security Special Interest Group

The 14 Absolute Truths of Security
Keith Palmgren

Save $400 when you register and pay by June 28th using code EarlyBird17

Courses at a Glance

	MON 8-21	TUE 8-22	WED 8-23	THU 8-24	FRI 8-25	SAT 8-26
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					
SEC566 Implementing and Auditing the Critical Security Controls – In-Depth	Page 5					
FOR585 Advanced Smartphone Forensics	Page 6					
MGT512 SANS Security Leadership Essentials for Managers with Knowledge Compression™	Page 7					
MGT517 Managing Security Operations: Detection, Response, and Intelligence	Page 8 *NEW!*					
ICS456 Essentials for NERC Critical Infrastructure Protection	Page 9					

SEC301

Intro to Information Security

GISF Certification

Information Security Fundamentals

www.giac.org/gisf

Five-Day Program
Mon, Aug 21 - Fri, Aug 25
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: My-Ngoc Nguyen

"Labs reinforced the security principles in a real-world scenario."
-Tyler Moore, Rockwell

"This is the perfect course for establishing a foundation for knowledge of aspects of information security, and the instructor is very knowledgeable and well-versed in the topics."
-Stephen Pridmore, Protective Life

▶II **Bundle OnDemand** with this course
www.sans.org/ondemand

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: Intro 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.

Written 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 Style**. 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 brings 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 has top security certifications that include GPEN, GCIH, GSEC, and CISSP, and is a former QSA. She is a 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 founded the non-profit organization CyberSafeNV to raise security awareness among Nevada residents and is currently the organization's chairperson. **@MenopN**

SEC401

Security Essentials Bootcamp Style

GSEC Certification
Security Essentials

www.giac.org/gsec

Six-Day Program
Mon, Aug 21 - Sat, Aug 26
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Keith Palmgren

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

"SEC401 has opened my eyes to just how important security is, and has given me a deeper understanding of how to protect our systems."
-Travis Sorensen, Xpress Solutions, Inc.

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

STOP and ask yourself the following questions:

- **Do you fully understand why some organizations get compromised and others do not?**
- **If there were compromised systems on your network, are you confident you would be able to find them?**
- **Do you know the effectiveness of each security device and are you certain they are all configured correctly?**
- **Are proper security metrics set up and communicated to your executives to drive security decisions?**

If you do not know the answers to these questions, SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

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

Prevention Is Ideal but Detection Is a Must

With the rise in advanced persistent threats, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organization's network depends on the effectiveness of the organization's defense. Defending against attacks is an ongoing challenge, with new threats emerging all of the time, including the next generation of threats. Organizations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

- **What is the risk?**
- **Is it the highest priority risk?**
- **What is the most cost-effective way to reduce the risk?**

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you will need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

SANS Technology Institute
www.sans.edu

www.sans.org/8140

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

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**

SEC504

GCIH Certification
Incident Handler

www.giac.org/gcih

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Aug 21 - Sat, Aug 26
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
(If your laptop supports only wireless, please bring a USB Ethernet adapter.)
Instructor: Mick Douglas

Who Should Attend

- Incident handlers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

"The training offered at SANS is the best in the industry and SEC504 is a must for any IT security professional – highly recommended."
-Michael Hoffman, Shell Oil Products U.S.

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.**

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

This course enables you to turn the tables on computer attackers by helping you understand their tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan. It addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare for, detect, and respond to those attacks. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning, exploiting, and defending systems. **This course will enable you to discover the holes in your system before the bad guys do!**

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. General security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

"SEC504 helped me put many pieces of the puzzle together."
-Ian Trimble, Blue Cross Blue Shield

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

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

Mick Douglas *SANS Instructor*

Even when his job title has indicated otherwise, Mick Douglas has been doing information security work for over 10 years. He earned a bachelor's degree in communications from Ohio State University and holds the CISSP, GCIH, GPEN, GCUX, GWEB, and GSNA certifications. He currently works at Binary Defense Systems as the DFIR Practice Lead. He is always excited for the opportunity to share with others so they do not have to learn the hard way! By studying with Mick, security professionals of all abilities will gain useful tools and skills that should make their jobs easier. When he's not "geeking out" you'll likely find Mick indulging in one of his numerous hobbies; photography, scuba diving, or hanging around in the great outdoors. **@ BetterSafetyNet**

SEC511

Continuous Monitoring and Security Operations

GMON Certification
Continuous Monitoring
www.giac.org/gmon

Six-Day Program
Mon, Aug 21 - Sat, Aug 26
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: David Mashburn

Who Should Attend

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

"This course has been awesome at teaching me how to use tools and existing architecture in ways I haven't thought of before!"
-John Hubbard, GlaxoSmithKline

We continue to underestimate the tenacity of our adversaries! Organizations are investing significant time and financial and human resources trying to combat cyber threats and prevent 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.

"Keep on giving real-life scenarios to spice up the class. This class was perfect."
-Genevieve Opaye-Tetteh, eProcess Int SA

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.

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 to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach will be 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.

SANS Technology Institute
www.sans.edu

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

David Mashburn *SANS Instructor*

David Mashburn is currently the IT security manager for a global non-profit organization in the Washington, D.C. area. He also has worked as an IT security professional for several civilian federal agencies, and has over 15 years of experience in IT. He holds a master's degree in computer science from John Hopkins University, and a B.S. from the University of Maryland at College Park. David holds multiple security-related certifications, including the CISSP, GPEN, GCIH, GCIA, and CEH. He is also a member of the SANS/GIAC Advisory Board, and has previously taught courses in the cybersecurity curriculum at the University of Maryland – University College. **@d_mashburn**

SEC566

Implementing and Auditing the Critical Security Controls – In-Depth

GCCC Certification
Critical Controls

www.giac.org/gccc

Five-Day Program
Mon, Aug 21 - Sat, Aug 25
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Chris Christianson

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Staff and clients of federal agencies
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MGT512

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

-Dan Trueman, Novae PLCSchool District

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle. The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

SANS' in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

The course shows security professionals how to implement the Controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

SANS Technology Institute
www.sans.edu

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

Chris Christianson *SANS Certified 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 in 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**

FOR585

Advanced Smartphone Forensics

GASF Certification
Advanced Smartphone Forensics

www.giac.org/gasf

Six-Day Program
Mon, Aug 21 - Sat, Aug 26
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Cindy Murphy

Who Should Attend

- Experienced digital forensic analysts who want to extend their knowledge and experience to forensic analysis of mobile devices, especially smartphones
- Media exploitation analysts who need to master Tactical Exploitation or Document and Media Exploitation (DOMEX) operations on smartphones and mobile devices by learning how individuals used their smartphones, who they communicated with, and what files they accessed
- Information security professionals who respond to data breach incidents and intrusions
- Incident response teams tasked with identifying the role that smartphones played in a breach
- Law enforcement officers, federal agents, and detectives who want to master smartphone forensics and expand their investigative skills beyond traditional host-based digital forensics
- IT auditors who want to learn how smartphones can expose sensitive information
- SANS SEC575, FOR500 (formerly FOR408), FOR508, FOR518, and FOR572 graduates looking to take their skills to the next level

"It's real-world practical info not just textbook!"

-Reza Salari, DRS Technologies

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

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

This in-depth smartphone forensics course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 17 hands-on labs that allow students to analyze different datasets from smart devices and leverage the best forensic tools and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools. Each lab is designed to teach you a lesson that can be applied to other smartphones. You will gain experience with the different data formats on multiple platforms and learn how the data are stored and encoded on each type of smart device. The labs will open your eyes to what you are missing by relying 100% on your forensic tools.

FOR585 is continuously updated to keep up with the latest malware, smartphone operating systems, third-party applications, and encryption. This intensive six-day course offers the most unique and current instruction available, and it will arm you with mobile device forensic knowledge you can apply immediately to cases you're working on the day you finish the course.

Smartphone technologies are constantly changing, and most forensic professionals are unfamiliar with the data formats for each technology. Take your skills to the next level: it's time for the good guys to get smarter and for the bad guys to know that their texts and apps can and will be used against them!

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

SANS Technology Institute
www.sans.edu

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

Cindy Murphy *SANS Certified Instructor*

Cindy Murphy served in law enforcement for more than 30 years, including 25 years with the Madison, WI Police Department, where she worked as a a detective and as a certified digital forensics examiner. During her time as an investigator, she saw firsthand the emergence of mobile devices as the primary source of evidence in investigations. This pushed her to grow into the mobile forensics expert she is today and enabled her to co-author the SANS **FOR585: Advanced Smartphone Forensics** course. Cindy has served as guest faculty for the National District Attorney's Association, testified as a computer forensics expert in state and federal court on numerous occasions, presented internationally on digital forensics topics, and written frequent articles and whitepapers. She has a Master of Science degree and a degree in forensic computing and cyber crime investigation from University College in Dublin. Cindy is also a military veteran, a mother, an activist in defense of First Amendment rights, and a musician. **@cindymurph**

MGT512

GSLC Certification
Security Leadership

www.giac.org/gslc

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program
Mon, Aug 21 - Fri, Aug 25
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop Recommended
Instructor: Ted Demopoulos

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

"MGT512 is one of the most valuable courses I've taken with SANS. It really did help bridge the gap from security practitioner to security orchestrator. Truly a gift!"
-John Madick, Epiq Systems, Inc.

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. Additionally, 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.

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!

SANS Technology Institute
www.sans.edu

www.sans.org/8140

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

Ted Demopoulos *SANS Principal 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 continuous 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 also a food and wine geek, goes flyfishing, and enjoys playing with his children. **@TedDemop**

MGT517

Managing Security Operations: Detection, Response, and Intelligence *NEW!*

Five-Day Program
Mon, Aug 21 - Fri, Aug 25
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Christopher Crowley

Who Should Attend

- Information security managers
- SOC Managers, Analysts & Engineers
- Information security architects
- IT managers
- Operations managers
- Risk management professionals
- IT/system administration/ network administration professionals
- IT auditors
- Business continuity and disaster recovery staff

"Chris is a fantastic instructor, has great pacing with engaging anecdotes, and he's very insightful."
-Rich Savacool, Nixon Peabody

Managing Security Operations covers the design, operation, and ongoing growth of all facets of the security operations capabilities in an organization. An effective Security Operations Center (SOC) has many moving parts and must be designed with the ability to adjust and work within the context and constraints of the organization. To run a successful SOC, managers need to provide tactical and strategic direction and inform staff of the changing threat environment as well as provide guidance and training for employees. This course covers design, deployment, and operation of the security program to empower leadership through technical excellence.

The course covers the functional areas of Communications, Network Security Monitoring, Threat Intelligence, Incident Response, Forensics, and Self-Assessment. We discuss establishing Security Operations governance for:

- **Business alignment and ongoing adjustment of capabilities and objectives**
- **Designing the SOC and the associated objectives of functional areas**
- **Software and hardware technology required for performance of functions**
- **Knowledge, skills, and abilities of staff as well as staff hiring and training**
- **Execution of ongoing operations**

You will walk out of this course armed with a roadmap to design and operate an effective SOC tailored to the needs of your organization.

Course Author Statement

"The inclusion of all functional areas of security operations is intended to develop a standardized program for an organization and express all necessary capabilities. Admittedly ambitious, the intention of the class is to provide a unified picture of coordination among teams with different skillsets to help the business prevent loss due to poor security practices. I have encountered detrimental compartmentalization in most organizations. There is a tendency for specialists to look only at their piece of the problem, without understanding the larger scope of information security within an organization. Organizations are likely to perceive a Security Operations Center as a tool, and not as the unification of people, processes, and technologies.

"This course provides a comprehensive picture of a Cyber Security Operations Center (CSOC). Discussion on the technology needed to run a SOC is handled in a vendor agnostic way. In addition, technology is addressed in a way that attempts to address both minimal budgets as well as budgets with global scope. The course outlines staff roles, addresses staff training through internal training and information-sharing, and examines the interaction between functional areas and data exchange.

"After attending this class, the participant will have a roadmap for what needs to be done in an organization seeking to implement security operations."

-Christopher Crowley

Christopher Crowley *SANS Principal Instructor*

Christopher has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. He is the course author for SANS MGT535: Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, FOR585, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the Year Award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. **@CCrowMontance**

ICS456

Essential for NERC Critical Infrastructure Protection

GIAC Certification Available Late 2017

Five-Day Program
Mon, Aug 21 - Fri, Aug 25
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Tim Conway

Who Should Attend

- IT and OT (ICS) cybersecurity
- Field support personnel
- Security operations personnel
- Incident response personnel
- Compliance staff
- Team leaders
- Governance officials
- Vendors/Integrators
- Auditors

This course empowers students with knowledge of the "what" and the "how" of the version 5/6 standards. The course addresses the role of the North American Electric Reliability Corporation (NERC), the Federal Energy Regulatory Commission (FERC), and the Regional entities. It provides multiple approaches for identifying and categorizing BES Cyber Systems and helps asset owners determine the requirements applicable to specific implementations. The course also covers implementation strategies for the version 5/6 requirements with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance. Our 25 hands-on labs range from securing workstations to digital forensics and lock picking.

Course Day Descriptions

456.1 HANDS ON: Asset Identification and Governance

A transition is under way from NERC CIP programs that are well defined and understood to a new CIP paradigm that expands its scope into additional environments and adds significantly more complexity. On day 1 students will develop an understanding of the electricity sector regulatory structure and history as well as an appreciation for how the CIP Standards fit into the overall framework of the reliability standards. Key NERC terms and definitions related to NERC CIP are reviewed using realistic concepts and examples that prepare students to better understand their meaning. We will explore multiple approaches to BES Cyber Asset identification and learn the critical role of strong management and governance controls. The day will examine a series of architectures, strategies, and difficult compliance questions in a way that highlights the reliability and cybersecurity strengths of particular approaches. Unique labs will include a scenario-based competition that helps bring the concepts to life and highlights the important role we play in defending the grid.

456.2 HANDS ON: Access Control and Monitoring

Strong physical and cyber access controls are at the heart of any good cybersecurity program. During day 2 we move beyond the "what" of CIP compliance to understanding the "why" and the "how." Firewalls, proxies, gateways, IDS and more – learn where and when they help and learn practical implementations to consider and designs to avoid. Physical protections include more than fences and you'll learn about the strengths and weaknesses of common physical controls and monitoring schemes. Labs will reinforce the learnings throughout the day and will introduce architecture review and analysis, firewall rules, IDS rules, compliance evidence demonstration, and physical security control reviews.

456.3 HANDS ON: System Management

CIP-007 has consistently been one of the most violated Standards going back to CIP version 1. With the CIP Standards moving to a systematic approach with varying requirement applicability based on system impact rating, the industry now has new ways to design and architect system management approaches. Throughout day 3, students will dive into CIP-007. We'll examine various Systems Security Management requirements with a focus on implementation examples and the associated compliance challenges. This day will also cover the CIP-010 requirements for configuration change management and vulnerability assessments that ensure systems are in a known state and under effective change control. We'll move through a series of labs that reinforce the topics covered from the perspective of the CIP practitioner responsible for implementation and testing.

456.4 HANDS ON: Information Protection and Response

Education is key to every organization's success with NERC CIP and the students in ICS 456 will be knowledgeable advocates for CIP when they return to their place of work. Regardless of their role, all students can be a valued resource to their organization's CIP-004 training program, the CIP-011 information protection program. Students will be ready with resources for building and running strong awareness programs that reinforce the need for information protection and cybersecurity training. On day 4 we'll examine CIP-008 and CIP-009 covering identification, classification, and communication of incidents as well as the various roles and responsibilities needed in an incident response or a disaster recovery event. Labs will introduce tools for ensuring file integrity and sanitization of files to be distributed, how to best utilize and communicate with the E-ISAC, and how to preserve incident data for future analysis.

456.5 HANDS ON: CIP Process

On the final day students will learn the key components for running an effective CIP Compliance program. We will review the NERC processes for standards development, violation penalty determination, Requests For Interpretation, and recent changes stemming from the Reliability Assurance Initiative. Additionally we'll identify recurring and audit related processes that keep a CIP compliance program on track: culture of compliance, annual assessments, gap analysis, TFEs, and self-reporting. We'll also look at the challenge of preparing for NERC audits and provide tips to be prepared to demonstrate the awesome work your team is doing. Finally, we'll look at some real-life CIP violations and discuss what happened and the lessons we can take away. At the end of day 5 students will have a strong call to action to participate in the ongoing development of CIP within their organization and in the industry overall as well as a sense that CIP is do-able! Labs will cover DOE C2M2, audit tools, and an audit-focused take on the "blue team – red team" exercise.

Tim Conway *SANS Instructor*

Tim is the Technical Director of ICS and SCADA programs at SANS. He is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. He previously served as the Director of CIP Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO), where he was responsible for Operations Technology, NERC CIP Compliance, and the NERC training environments for the operations departments within NIPSCO Electric. Tim was also an EMS Computer Systems Engineer at NIPSCO for eight years, with responsibility over the control system servers and the supporting network infrastructure. He was the chair of the RFC CIPC, and is the current chair of the NERC CIP Interpretation Drafting Team, a member of the NESCO advisory board, chair of the NERC CIPC GridEx Working Group, and chair of the NBISE Smart Grid Cyber Security panel.

Bonus Sessions

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

KEYNOTE: Infosec Rock Star: Geek Will Only Get You So Far

Ted Demopoulos

This presentation is based on the recently published book of the same title. Some of us are so effective and well known that the term "Rock Star" 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 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.

Presentation topics, which will feature input from real Rock Stars of Infosec, include:

- The Five Levels of Rock Stars
- Positioning - why "they" don't like us or security and what we can do about it
- The Science of Influence - ruthless social engineering or effective professional skills?
- Getting Things Done - brutal time management and the art of saying "no" without upsetting too many people
- How to let people know you rock. You might be the best in the world, but if no one knows it you're not going to do much good.

Women's CONNECT Event

Hosted by the SANS COINS Program and the ISSA International Women in Security Special Interest Group

Join SANS and the ISSA International Women in Security Special Interest Group (WIS SIG) as we partner with local association chapters and groups to foster an evening of connections. Group representatives will be on hand to discuss group activities and the benefits of membership. From Jean Jennings Bartik to Diane Greene, women have always been a driving force in the field of information technology. Their stories are not only about overcoming challenges but also about innovation and inspiration. Enjoy the networking and building camaraderie among your peers, all while discussing recent successes relating to local luminaries such as Joann Maguire, Sandra Rothenberg, Pam Shockley-Zalabak, and Judith Wagner, among MANY others.

The 14 Absolute Truths of Security

Keith Palmgren

Keith Palmgren has identified 14 absolute truths of security – things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these 14 absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the 14 absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

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

- 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.

Future Training Events

Rocky Mountain	Denver, CO	June 12-17
Charlotte	Charlotte, NC	June 12-17
Minneapolis	Minneapolis, MN	June 19-24
Columbia	Columbia, MD	June 26 - July 1
Los Angeles – Long Beach	Long Beach, CA	July 10-15

SANSFIRE Washington, DC July 22-29

San Antonio	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
Virginia Beach	Virginia Beach, VA	Aug 21 - Sep 1
Tampa – Clearwater	Clearwater, FL	Sep 5-10
San Francisco Fall	San Francisco, CA	Sep 5-10

Network Security Las Vegas, NV Sep 10-17

Baltimore	Baltimore, MD	Sep 25-30
Rocky Mountain Fall	Denver, CO	Sep 25-30
Phoenix-Mesa	Mesa, AZ	Oct 9-14
Tysons Corner Fall	McLean, VA	Oct 16-21
San Diego Fall	San Diego, CA	Oct 30 - Nov 4
Seattle	Seattle, WA	Oct 30 - Nov 4
Miami	Miami, FL	Nov 6-11
San Francisco Winter	San Francisco, CA	Nov 27 - Dec 2
Austin Winter	Austin, TX	Dec 4-9

Future Summit Events

Digital Forensics	Austin, TX	June 22-29
ICS & Energy	Houston, TX	July 10-15
Security Awareness	Nashville, TN	July 31 - Aug 9
Data Breach	Chicago, IL	Sep 25 - Oct 2
Secure DevOps	Denver, CO	Oct 10-17
SIEM & Tactical Analytics	Scottsdale, AZ	Nov 28 - Dec 5

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.

Hotel Information

The Palmer House Hilton
17 East Monroe Street
Chicago, IL 60603
Phone: 312-726-7500
www.sans.org/event/chicago-2017/location

One hundred forty years. Countless stories. The Palmer House didn't become a beloved downtown Chicago hotel by chance. It did so by design. Since 1871, the iconic Chicago hotel has been host to countless celebrated figures. Today, having undergone a meticulous $170 million renovation, the Palmer House awaits those stories yet to be written and forever to be retold. We invite you to share in the inspired story of this downtown Chicago hotel. Even more so, within the walls and halls of the Palmer House, we encourage you to compose your own.

Special Hotel Rates Available

A special discounted rate of $205.00 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. These rates include high-speed Internet in your room and are only available through **July 20, 2017**. To make reservations please call (800) HILTONS (800-445-8667) and ask for the SANS group rate.

Top 5 reasons to stay at the The Palmer House Hilton

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 The Palmer House Hilton 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 The Palmer House Hilton that you won't want to miss!
5. Everything is in one convenient location!

Registration Information

Register online at **www.sans.org/chicago**

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

Select your course and indicate whether you plan to test for GIAC certification. If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Pay Early and Save*

Use code **EarlyBird17** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code by	**6-28-17**	**$400.00**	**7-19-17**	**$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 & 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 **August 2, 2017**. 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.

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