SANS Minneapolis 2015

Minneapolis, MN July 20-25

THE MOST TRUSTED NAME IN INFORMATION & SOFTWARE SECURITY TRAINING

"The entire course has been fantastic and it exceeded my expectations. SANS training is far superior to other training programs."

-Paul Petrasko, Bemis Company

Protect your company and advance your career with these crucial courses:

- Security Essentials Bootcamp Style
- Hacker Tools, Techniques, Exploits, and Incident Handling
- Network Penetration Testing and Ethical Hacking
- Windows Forensic Analysis
- SANS Security Leadership Essentials For Managers with Knowledge Compression™
- Advanced Web App Penetration Testing and Ethical Hacking
- Advanced Security Essentials - Enterprise Defender
- ICS/SCADA Security Essentials

GIAC Approved Training

Register at
sans.org/event/minneapolis-2015

Save $400
Register & pay early!
See page 13 for more details.

SANS is bringing its top-rated cybersecurity training to Minneapolis for the first time! We are pleased to invite you to **SANS Minneapolis 2015** from July 20-25. The event will feature eight of our most popular courses, all specifically designed to provide you with the practical skills and tools you need to quickly identify attacks on your company's critical systems and networks.

SANS is the leading information security training provider in the world. Our courses are taught by industry experts whose goal is to intensively and rapidly scale up your cybersecurity knowledge so that you can use what you learn as soon as you get back to the office. SANS instructors apply the concepts and techniques they teach on a daily basis and are considered to be among the best cybersecurity instructors in the world. Our instructor line-up for SANS Minneapolis 2015 includes Adrien de Beaupre, Kevin Fiscus, G. Mark Hardy, Keith Palmgren, Justin Searle, Eric Cornelius, David Cowen, and Russell Eubanks.

Seven of the courses offered at this event are associated with a **GIAC Certification**, and four are aligned with the **DoD 8570 Directive**. You can also supplement your SANS training with an **OnDemand Bundle** option when purchasing a course and receive four months of online access to the course's custom e-learning program, including lecture video or audio files, quizzes, and labs – all accessible through your SANS account after your live training ends. To add OnDemand or a GIAC certification to your course, select the options when completing the online registration form.

You can build on your training experience and advance your career by enrolling in a master's degree or a graduate certificate program with the **SANS Technology Institute**, which is regionally accredited and eligible for tuition reimbursement plans. Choose from a Master's in Information Security Engineering or a Graduate Certificate in Penetration Testing or Incident Response. Go to **www.sans.edu** and apply today!

Our campus location for this event is the Hilton Minneapolis. This 25-story, Victorian-style brick high-rise is right in the city's financial center and conveniently connected to the Convention Center. Attractions within minutes of the hotel include the Minneapolis Institute of Arts, featuring 80,000 works; Orchestra Hall, where classical and pop music stars perform year-round; and Nicollet Mall, with shops stretching along a 12-block radius. A special discounted rate of $189.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through June 26.

What are you waiting for? **Save $400** by entering discount code "**EarlyBird15**" on the registration page and paying for any 4-6 day course by May 27! For more details see the registration page in this brochure.

Start making your training and travel plans now and tell your colleagues and friends about SANS Minneapolis 2015. Come prepared to learn from the best and leave with the skills and tools you'll need to protect your critical infrastructure.

We look forward to seeing you in Minneapolis!

Here's what SANS alumni have said about the value of SANS training:

"The course covers all areas of basic security. Not only were the text books great, doing the labs helped apply what I've learned."
-Michael Hagen, VSACISAP Korea

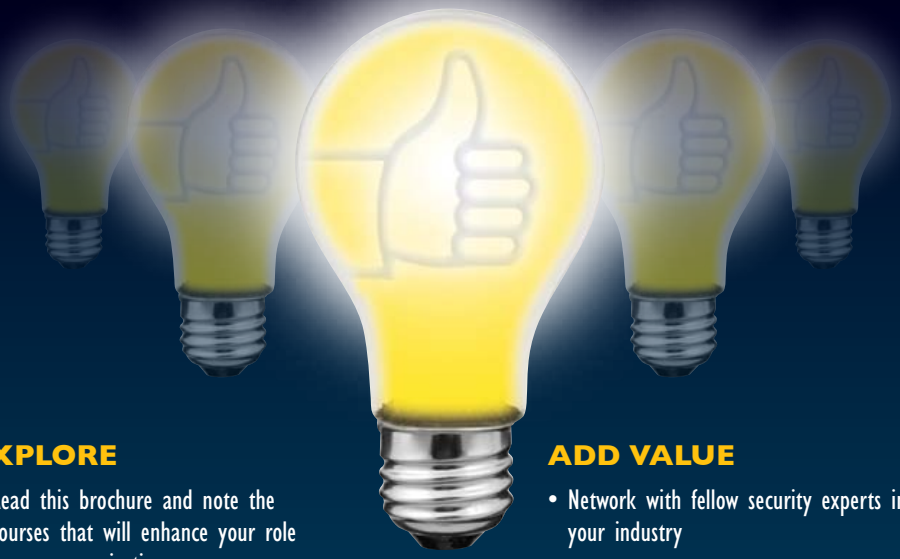
"I appreciated my instructor. He kept my attention, and the labs are reinforcement to my learning because of the hands-on training."
-Keiva Rhodes, SAIC

"The course helped me get a better sense of knowing if I am doing things correctly, and it also provided some useful tools and applications."
-Daniel Samuel, United Nations Development Programme

Courses-at-a-Glance

@SANSInstitute *Join the conversation:* #SANSmpls

The Value of SANS Training & YOU



EXPLORE

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

RELATE

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

VALIDATE

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

SAVE

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

ADD VALUE

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

ALTERNATIVES

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

ACT

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

Return on Investment

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

REMEMBER

the SANS promise:

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

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, July 20 - Sat, July 25
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Russell Eubanks

- GIAC Cert: GSEC
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

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

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

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

With the advanced persistent threat, 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.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

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

"There's a ton of excellent information in this course which has opened my eyes to the importance of cybersecurity and all the threats I never knew existed." -Ben Penaflor, General Atomics

Russell Eubanks *SANS Instructor*

Russell Eubanks has been a security leader in several financial and health care organizations. He has developed information security programs from the ground up and actively seeks opportunities to measurably increase their overall security posture. Russell is enrolled in the SANS Technology Institute and has a Bachelor of Science in Computer Science. He holds several security certifications including the CISSP, CISM, GCIA, GCIH, GPEN, GISP, GSEC and GWAPT. He is a leader of the Atlanta OWASP chapter and is instrumental in helping it grow. www.securityeverafter.com

SECURITY 501

Advanced Security Essentials – Enterprise Defender

SANS

Six-Day Program
Mon, July 20 - Sat, July 25
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Keith Palmgren

- GIAC Cert: GCED
- STI Master's Program
- OnDemand Bundle

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. **SEC501: Advanced Security Essentials - Enterprise Defender** builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

Who Should Attend

- Incident response and penetration testers
- Security Operations Center engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

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

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

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

"Good introduction and hands-on experience with a variety of tools!"
-Carrie Crot, DOJ

"A very good thoughtful and practical understanding of security, something everyone in IT should get."
-Paul Godard, OPC

"I learned how to manage the risks, how to protect data, and how to prevent the loss of data that my institution owns."
-Puiu Lucian Chitu, ANCOM

GCED
giac.org

SANS INSTITUTE
sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

Keith Palmgren *SANS Certified 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 & 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 a total of 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications. T: @kpalmgren

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, July 20 - Sat, July 25
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Kevin Fiscus

- GIAC Cert: GCIH
- STI Master's Program
- Cyber Guardian
- DoDD 8570
- OnDemand Bundle

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
- Penetration testers
- Ethical hackers
- 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

By helping you understand attackers' 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, this course helps you turn the tables on computer attackers. 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, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning for, exploiting, and defending systems. It 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.

"Incident handling is the baseline for cybersecurity, so having a course like SEC504 is great for the beginner and the expert alike. A good solid foundation leads to a great cybersecurity setup."
-Robert Fredricks, Parkell Inc.

"The instructor did a great job showing us hacker tools and perspectives. I can't wait to take the techniques back to my job."
-Emily Gladstone Cole, HP

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

Bundle OnDemand
with this course
sans.org/ondemand

Kevin Fiscus *SANS Certified Instructor*

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively on information security for the past 12. Kevin currently holds the CISA, GPEN, GREM, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GCWN, GCSC-Gold, GSEC, SCSA, RCSE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. Kevin has taught many of SANS most popular classes including SEC401, SEC464, SEC504, SEC542, SEC560, SEC575, FOR508, and MGT414. In addition to his security work, he is a proud husband and father of two children. T: @kevinbfiscus

SECURITY 560

Network Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, July 20 - Sat, July 25
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Adrien de Beaupre

- GIAC Cert: GPEN
- Cyber Guardian
- STI Master's Program

As a cybersecurity professional, you have a unique responsibility to find and understand your organization's vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this duty head-on.

SEC560 is the must-have course for every well-rounded security professional.

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Red team members
- Blue team members

This course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks and wireless and web apps, with over 30 detailed hands-on labs throughout.

Learn the best ways to test your own systems before the bad guys attack.

Chock full of practical, real-world tips from some of the world's best penetration testers, SEC560 prepares you to perform detailed reconnaissance by examining a target's infrastructure and mining blogs, search engines, social networking sites and other Internet and intranet infrastructure. You will be equipped to scan target networks using best-of-breed tools. We will not just cover run-of-the-mill options and configurations, we will also go over the less-known but highly useful capabilities of the best pen test toolsets available today. After scanning, you will learn dozens of methods for exploiting target systems to gain access and measure real business risk, then examine post-exploitation, password attacks, wireless and web apps, pivoting through the target environment to model the attacks of real-world bad guys.

giac.org

sans.edu

sans.org/
cyber-guardian

You will bring comprehensive penetration testing and ethical hacking know-how back to your organization.

After building your skills in challenging labs over five days, the course culminates with a full-day, real-world network penetration test scenario. You will conduct an end-to-end penetration test, applying the knowledge, tools and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization.

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"This course has a direct correlation to my job duties. The insight, real-world references, and the use of various tools will make my job a lot easier. You will learn skills and ways your systems are vulnerable."
-Roland Thomas, USAF

"SEC560 really tests your skills and abilities and the Netcat backdoor exercises have really opened my eyes on the endless possibilities & capabilities."
-David Poulin, 7th Cyber Protection Brigade

Adrien de Beaupre *SANS Certified Instructor*

Adrien de Beaupre is a certified SANS instructor and works as an independent consultant in beautiful Ottawa, Ontario. His work experience includes technical instruction, vulnerability assessment, penetration testing, intrusion detection, incident response and forensic analysis. He is a member of the SANS Internet Storm Center (isc.sans.edu). He is actively involved with the information security community, and has been working with SANS since 2000. Adrien holds a variety of certifications including the GXPN, GPEN, GWAPT, GCIH, GCIA, GSEC, CISSP, OPST, and OPSA. When not geeking out he can be found with his family, or at the dojo. T: @adriendb

SECURITY 642

Advanced Web App Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, July 20 - Sat, July 25
9:00am - 5:00pm
36 CPEs
Instructor: Justin Searle
- OnDemand Bundle

This course is designed to teach you the advanced skills and techniques required to test web applications today. This advanced pen testing course uses a combination of lecture, real-world experiences, and hands-on exercises to educate you in the techniques used to test the security of enterprise applications.

Who Should Attend

- Web penetration testers
- Security consultants
- Developers
- QA testers
- System administrators
- IT managers
- System architects

We will begin by exploring specific techniques and attacks to which applications are vulnerable. These techniques and attacks use advanced ideas and skills to exploit the system through various controls and protections. This learning will be accomplished through lectures and exercises using real-world applications.

We will then explore encryption as it relates to web applications. You will learn how encryption works as well as techniques to identify the type of encryption in use within the application. Additionally, you will learn methods for exploiting or abusing this encryption, again through lecture and labs.

The next day of class will focus on how to identify web application firewalls, filtering, and other protection techniques. You will then learn methods to bypass these controls in order to exploit the system. You'll also gain skills in exploiting the control itself to further the evaluation of the security within the application.

Following these general exploits, you will learn techniques that target specific enterprise applications. You will attack systems such as content management and ticketing systems. We will explore the risks and flaws found within these systems and how to better exploit them. This part of the course will also include web services and mobile applications due to their prevalence within modern organizations.

This information-packed advanced pen testing course will wrap up with a full day Capture the Flag (CtF) event. This CtF will target an imaginary organization's web applications and will include both Internet and intranet applications of various technologies. This event is designed to allow you to put the pieces together from the previous five days reinforcing the information and learning you will have gained.

"SEC642 is the perfect course for someone who has a background in web app pen testing, but wants to really gain advanced skills."
-Matthew Sullivan, Webfilings

"The Capture-the-Flag event was excellent! It was very clear and easy to understand, well structured, and a lot of relevant content."
-Geoffrey Davidson, QA Ltd.

Justin Searle *SANS Certified Instructor*

Justin Searle is a Managing Partner of UtiliSec, specializing in Smart Grid security architecture design and penetration testing. Justin led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and played key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG). He currently leads the testing group at the National Electric Sector Cybersecurity Organization Resources (NESCOR). Justin has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences. Mr. Searle is currently a certified instructor for the SANS Institute. In addition to electric power industry conferences, Justin frequently presents at top international security conferences such as Black Hat, DEFCON, OWASP, Nullcon, and AusCERT. Justin co-leads prominent open source projects including the Samurai Web Testing Framework (SamuraiWTF), the Samurai Security Testing Framework for Utilities (SamuraiSTFU), Middler, Yokoso!, and Laudanum. Justin has an MBA in International Technology and is a CISSP and SANS GIAC certified Incident Handler (GCIH), Intrusion Analyst (GCIA), and Web Application Penetration Tester (GWAPT). T: @meeas

FORENSICS 408

Windows Forensic Analysis

SANS

Six-Day Program
Mon, July 20 - Sat, July 25
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: David Cowen

- GIAC Cert: GCFE
- STI Master's Program
- OnDemand Bundle

Master Windows Forensics – You can't protect what you don't know about.

Every organization must prepare for cyber-crime occurring on their computer systems and within their networks. Demand has never been higher for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

Who Should Attend

- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

DFIR
digital-forensics.sans.org

FOR408: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and artifacts is a core component of information security. Learn to recover, analyze, and authenticate forensic data on Windows systems. Understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. Use your new skills for validating security tools, enhancing vulnerability assessments, identifying insider threats, tracking hackers, and improving security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR408 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7, Windows 8/8.1, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook,). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out - attendees learn to analyze everything from legacy Windows XP systems to just discovered Windows 8.1 artifacts.

FIGHT CRIME. UNRAVEL INCIDENTS... ONE BYTE AT A TIME

GCFE
giac.org

SANS INSTITUTE
sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"After the course, I am able to have a good picture of the whole process from the basic hands-on to the organizations of findings. Excellent!"
-Jenny Blaine, University of Minnesota

"FOR408 provides in-depth knowledge of the best forensic practices that can be applied directly to investigations."
-Nathan Lewis, KPMG

David Cowen *SANS Instructor*

Mr. Cowen has more than sixteen years of experience in the areas of integration, architecture, assessment, programming, forensic analysis and investigation. He currently holds the Certified Information Systems Security Professional certification from (ISC)2. He has been trained in proper forensics practices by the High Tech Crime Investigators Association, ASR Data and Guidance Software, and SANS, amongst others. He is an active contributor within the computer forensics community where he frequently presents and trains on various forensic topics. He has managed, created, and worked with multiple forensics/litigation support teams and associated procedures. His experience spans a variety of environments ranging from high security military installations to large/small private sector companies. He is the author of *Infosec Pro Guide to Computer Forensics*, *Hacking Exposed: Computer Forensics* (1st and 2nd edition) and the *Anti Hacker Toolkit* 3rd edition all by McGraw Hill. T: @hecfblog

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program
Mon, July 20 - Fri, July 24
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop NOT Needed
Instructors: G. Mark Hardy

- GIAC Cert: GSLC
- STI Master's Program
- DoDD 8570
- OnDemand Bundle

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.

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.

"Every IT security professional should attend – no matter what their position. This information is important to everyone."
-John Flood, NASA

"MGT512 gives a good understanding of what knowledge our employees need to have to be successful."
-Teddie Steele, State Department of FCU

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!

giac.org

sans.edu

sans.org/8570

Bundle OnDemand
with this course
sans.org/ondemand

G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and President of National Security Corporation. He has been providing cyber security expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events worldwide. G. Mark 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 US 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 holds a BS in Computer Science, a BA in Mathematics, a Masters in Business Administration, a Masters in Strategic Studies, and holds the GSLC, CISSP, CISM and CISA certifications. T: @g_mark

INDUSTRIAL CONTROL SYSTEMS 410

ICS/SCADA Security Essentials

SANS

Five-Day Program
Mon, July 20 - Fri, July 24
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Eric Cornelius
- GIAC Cert: GICSP
- OnDemand Bundle

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. **ICS410: ICS/SCADA Security Essentials** provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

Who Should Attend

- The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:
- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

The course will provide you with:

- **An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints.**
- **Hands-on lab learning experiences to control system attack surfaces, methods, and tools**
- **Control system approaches to system and network defense architectures and techniques**
- **Incident-response skills in a control system environment**
- **Governance models and resources for industrial cybersecurity professionals.**

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as industrial control system penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

When students complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their industrial control system environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

GICSP
giac.org

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"This training really opens you up to possibilities and issues that otherwise you wouldn't really think about."
-Alfonso Barreiro, Panama Canal

"Today was information packed, and a lot of invaluable instruction and knowledge to consume."
-Rob Ruel, Edison

"Very satisfied with ICS410, and the instructor was very knowledgeable and great at balancing group backgrounds (IT vs. SCADA)."
-Chad Slater, The Dow Chemical Company

Eric Cornelius *SANS Instructor*

Eric Cornelius is currently a Technical Director at Cylance, Inc. and has recently served as the Chief Technical Analyst for DHS CSSP. As an active researcher in the field of cybersecurity since 2002, Mr. Cornelius supported many "boots-on-the-ground" engagements involving penetration testing, forensics, and malware analysis. Through these engagements, Mr. Cornelius aided multiple government, military, and private-sector organizations in protecting their networks and industrial control systems.

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: The 14 Absolute Truths of Security *Keith Palmgren*

Keith Palmgren has identified fourteen absolute truths of security - things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these fourteen 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 fourteen 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.

Complete Application Pw0nage Via Multi-Post Cross Site Request Forgery (XSRF) *Adrien de Beaupre*

This talk will discuss the risk posed by Cross Site Request Forgery (CSRF or XSRF) which is also known as session riding, or transaction injection. Many applications are vulnerable to XSRF, mitigation is difficult as it often requires re-engineering the entire application, and the threat they pose is often misunderstood. A live demo of identifying the vulnerability, and exploiting it by performing multiple unauthorized transactions in a single POST will be demonstrated.

Filesystem Journal Forensics *David Cowen*

Journaled file systems have been a part of modern file systems for years, but the science of computer forensics has only been approaching them mainly as a method of recovering deleted files. In this talk we will outline the three major file systems in use today that utilize journaling (NTFS, EXT3/4, HFS+) and explain what is stored and its impact on your investigations. We will discuss NTFS and new analysis techniques:

- Recover data hidden or destroyed by anti-forensics
- Determine exact deletion times
- Determine what was being accessed and how often

Card Fraud 101 *G. Mark Hardy*

Ever get a call from your bank saying your credit card was stolen, but it was still in your wallet? What's going on here? Card fraud costs $16 billion annually, and it's not getting better. Target, PF Changs, Michaels, Home Depot, who's next? Find out how these big card heists are pulled off, why chip-and-pin won't solve the fraud problem, and why Apple Pay is trivial to compromise. See if your bank even bothers to use the security protections it could – we'll have a mag stripe card reader so you can really see what's in your wallet. Certified SANS Instructor G. Mark Hardy is the CEO and founder of CardKill Inc., a start-up that helps banks preemptively kill stolen cards BEFORE they are used in fraud.

Debunking the Complex Password Myth *Keith Palmgren*

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

FUTURE SANS TRAINING EVENTS

SANS Security West 2015
San Diego, CA | May 3-12 | #SecurityWest

SANS/NH-ISAC Healthcare Cybersecurity SUMMIT & TRAINING
Atlanta, GA | May 12-19

SANS Pen Test Austin 2015
Austin, TX | May 18-23 | #PenTestAustin

SANS Houston ICS Security Training
Houston, TX | June 1-5 | #SANSICS

SANSFIRE 2015
Baltimore, MD | June 13-20 | #SANSFIRE

SANS Rocky Mountain 2015
Denver, CO | June 22-27 | #SANSRockyMtn

SANS Capital City 2015
Washington, DC | July 6-11 | #SANSDC

SANS Digital Forensics & Incident Response SUMMIT & TRAINING
Austin, TX | July 7-14 | #DFIRSummit

SANS San Jose 2015
San Jose, CA | July 20-25 | #SANSSJ

SANS Boston 2015
Boston, MA | August 3-8 | #SANSBoston

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

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

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

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

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

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

ONLINE TRAINING

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

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

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

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

SANS MINNEAPOLIS 2015

Hotel Information

Training Campus
Hilton Minneapolis

1001 Marquette Avenue South
Minneapolis, MN
sans.org/event/minneapolis-2015/location

This 25-story, Victorian-style brick high-rise boasts a fantastic location in the center of Minneapolis' financial center and is within minutes of many Minneapolis attractions. Conveniently connected to the Minneapolis Convention Center, the hotel is a world-class convention and leisure destination located near theaters, shops, restaurants and other cultural attractions. They are just steps from Target Center and Target Field. The Mall of America, Minnesota Zoo, and TCF Bank Stadium are just a short drive away.

Special Hotel Rates Available

A special discounted rate of $189.00 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 June 26, 2015.

Top 5 reasons to stay at the Hilton Minneapolis

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 Hilton Minneapolis, 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 Hilton Minneapolis that you won't want to miss!
5. Everything is in one convenient location!

SANS MINNEAPOLIS 2015

Registration Information

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

Register online at sans.org/event/minneapolis-2015/courses

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

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

Use code **EarlyBird15** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**5/27/15**	**$400.00**	**6/17/15**	**$200.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

10% discount if 10 or more people from the same organization register at the same time
5% discount if 5-9 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

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 July 1, 2015 – processing fees may apply.

SANS Voucher Credit Program

Expand your training budget! Extend your Fiscal Year. The SANS Voucher Discount Program pays you credits and delivers flexibility.
sans.org/vouchers


Open a
SANS
Account
Sign up for a
SANS Account
and receive free
webcasts, newsletters,
the latest news and
updates, and many other
free resources.
sans.org/account