SANS San Jose 2015

San Jose, CA July 20-25

"SANS course content is outstanding, and the instructor is very knowledgeable with great delivery."

-Michael Lonigro, USAA

THE MOST TRUSTED NAME
IN INFORMATION &
SOFTWARE SECURITY TRAINING

Save $400

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

Active Defense, Offensive Countermeasures, and Cyber Deception ***NEW!***

Security Essentials Bootcamp Style

Hacker Tools, Techniques, Exploits, and Incident Handling

Web App Penetration Testing and Ethical Hacking

SANS Security Leadership Essentials For Managers with Knowledge Compression™

SANS Training Program for CISSP Certification®

Advanced Network Forensics and Analysis

GIAC Approved Training

Register at sans.org/event/san-jose-2015

Welcome to San Jose 2015! SANS, the global leader in information security training, will host its inaugural training event in San Jose from July 20-25 with courses in IT security, incident handling, forensic analysis, CISSP certification, and IT management. The event will also feature SANS' new and popular course, **SEC550: Active Defense, Offensive Countermeasures and Cyber Deception**, a proactive approach to security that teaches you how to force attackers to make a first move in order to increase your ability to detect them.

At San Jose 2015 you will receive superior training from instructors who are industry leaders with the real-world experience to address the same challenges you face on a daily basis. SANS faculty are considered to be among the best cybersecurity instructors in the world, and their commitment is to ensure that you not only learn the material but that you can use it the day you return to the office.

Six of our courses offered at SANS San Jose 2015 have associated **GIAC** certifications, and three align with **DoD 8570**. To learn more, look at the GIAC page in this brochure or visit the website **www.giac.org** to register for your certification attempt.

Do you want to earn an advanced degree in information security? **SANS Technology Institute** offers a Master of Science in Information Security Engineering (MSISE) and Information Security Management (MSISM). New Graduate Certificates in Cyber Engineering, Penetration Testing, and Incident Response are also available. To learn more about SANS Cyber Degree programs go to **www.sans.edu** and apply today.

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 to your course, select the options when completing the online registration form.

San Jose 2015 will be held at **The Sainte Claire Hotel**, located minutes from San Jose's best attractions, including The Tech Museum, American Musical Theater of San Jose, San Jose Museum of Art, and Winchester Mystery House. A special discounted rate of $211.00 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 25. See our registration page for complete information and **save $400** when registering by entering the discount code "**EarlyBird15**" and paying for any 4-6 day course by May 27.

Come to San Jose to see for yourself why SANS is the top information security training provider in the world. We look forward to seeing you there!

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

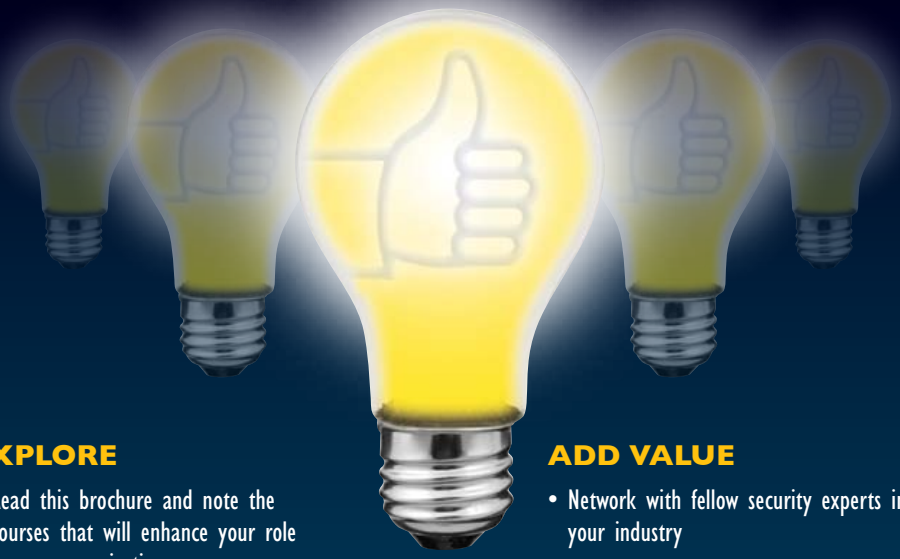
"I appreciated my instructor. He kept my attention, and the labs are reinforcement to my learning because of the hands-on training."
-Keiva Rhodes, SAIC

"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

		MON 7/20	TUE 7/21	WED 7/22	THU 7/23	FRI 7/24	SAT 7/25
SEC401	Security Essentials Bootcamp Style	Page 2					
SEC504	Hacker Tools, Techniques, Exploits & Incident Handling	Page 3					
SEC542	Web App Penetration Testing and Ethical Hacking	Page 4					
SEC550	Active Defense, Offensive Countermeasures and Cyber Deception *NEW!*	Page 5					
FOR572	Advanced Network Forensics and Analysis	Page 6					
MGT414	SANS Training Program for CISSP Certification®	Page 7					
MGT512	SANS Security Leadership Essentials For Managers with Knowledge Compression™	Page 8					

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, Jul 20 - Sat, Jul 25
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Bryan Simon

- 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

Bryan Simon *SANS Instructor*

With more than 20 years of experience in information technology and infosec, Bryan Simon is an internationally recognized expert in cybersecurity. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity, and has instructed individuals from organizations such as the FBI, NATO, and the UN in matters of cybersecurity, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. Bryan has received recognition for his work in I.T. Security, and was most recently profiled by McAfee (part of Intel Security) as an I.T. Hero. Bryan's scholastic achievements have resulted in the honour of sitting as a current member of the Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program.

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

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

- 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.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"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

Jonathan Ham *SANS Certified Instructor*

Jonathan is an independent consultant who specializes in large-scale enterprise security issues, from policy and procedure, through staffing and training, to scalable prevention, detection, and response technology and techniques. With a keen understanding of ROI and TCO (and an emphasis on process over products), he has helped his clients achieve greater success for over 12 years, advising in both the public and private sectors, from small upstarts to the Fortune 500. He's been commissioned to teach NCIS investigators how to use Snort, performed packet analysis from a facility more than 2000 feet underground, and chartered and trained the CIRT for one of the largest U.S. civilian Federal agencies. He has variously held the CISSP, GSEC, GCIA, and GCIH certifications, and is a member of the GIAC Advisory Board. A former combat medic, Jonathan still spends some of his time practicing a different kind of emergency response, volunteering and teaching for both the National Ski Patrol and the American Red Cross.

SECURITY 542

Web App Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, Jul 20 - Sat, Jul 25
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Micah Hoffman

- GIAC Cert: GWAPT
- Cyber Guardian
- STI Master's Program
- OnDemand Bundle

Web applications play a vital role in every modern organization. This becomes apparent when adversaries compromise these applications, damage business functionality and steal data.

Who Should Attend

- General security practitioners
- Penetration testers
- Ethical hackers
- Web application developers
- Website designers and architects

Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems. SEC542 helps students move beyond push-button penetration testing to professional web application penetration testing that finds flaws before the adversaries discover and abuse them.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, so, not surprisingly, every major industry study finds that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but web application penetration testing requires something deeper. SEC542 will enable students to capably assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations. Students will come to understand major web application flaws and their exploitation and, most importantly, learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations.

"The content is very relevant as it features recently discovered vulnerabilities. It also effectively, from my view, caters to various experience levels."
-Malcolm King, Morgan Stanley

"Everything was very well thought out and organized. The URLs used for the labs worked flawlessly. The course content and teaching skills were great!"
-Stephan Hofacker, InfoTrust AG

giac.org

sans.edu

sans.org/cyber-guardian

Bundle OnDemand
with this course
sans.org/ondemand

Micah Hoffman *SANS Instructor*

Micah Hoffman has been working in the information technology field since 1998 supporting federal government, commercial, and internal customers in their searches to discover and quantify information security weaknesses within their organizations. He leverages years of hands-on, real-world penetration testing and incident response experience to provide unique solutions to his customers. Micah holds GIAC's GAWN, GWAPT, and GPEN certifications as well as the CISSP. Micah is an active member in the NoVAHackers group, has written Recon-ng and Nmap testing tool modules and enjoys tackling issues with the Python scripting language. When not working, teaching, or learning, Micah can be found hiking or backpacking on Appalachian Trail or the many park trails in Maryland. T: @WebBreacher

SECURITY 550

Active Defense, Offensive Countermeasures and Cyber Deception

NEW

Five-Day Program
Mon, Jul 20 - Fri, Jul 24
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Bryce Galbraith

A *Washington Post* article on the rise of cyber attacks reported that "behind the scenes, talk among company officials increasingly turns to an idea once considered so reckless that few would admit to even considering it: Going on the offensive. Or, in the parlance of cybersecurity consultants, 'hacking back.'"

That's just one example of the considerable media coverage recently about using Active Defenses to combat cyber threats. There are those who thirst for vengeance and want to directly attack the attackers. Others believe that any sort of active response directed at an attacker is wrong or legally dicey. We believe the answer is somewhere in between.

The current threat landscape is shifting. Traditional defenses are failing us. We need to develop new strategies to defend ourselves. Even more importantly, we need to better understand who is attacking us and why. You may be able to immediately implement some of the measures we discuss in this course, while others may take a while. Either way, consider what we discuss as a collection of tools at your disposal when you need them to annoy attackers, determine who is attacking you, and, finally, attack the attackers.

SEC550: Active Defense, Offensive Countermeasures and Cyber Deception is based on the Active Defense Harbinger Distribution live Linux environment funded by the Defense Advanced Research Projects Agency (DARPA). This virtual machine is built from the ground up for defenders to quickly implement Active Defenses in their environments. The course is very heavy with hands-on activities – we won't just talk about Active Defenses, we will work through labs that will enable you to quickly and easily implement what you learn in your own working environment.

Who Should Attend

- Security professionals and systems administrators who are tired of playing catch-up with attackers
- Anyone who is in IT and/or security and wants defense to be fun again

You Will Learn:

- How to force an attacker to take more moves to attack your network – moves that in turn may increase your ability to detect that attacker
- How to gain better attribution as to who is attacking you and why
- How to gain access to a bad guy's system
- Most importantly, you will find out how to do the above legally

"For me the most value is the security perspective of technology. It has helped me think about my job differently."
-Afzaal Syed, Ernst and Young

"Bryce has an excellent knowledge and passion for security. This shows in his delivery of the material. He uses good real-life examples that bring the material to life."
-Ron Austin,
Sony Network Entertainment

Bryce Galbraith *SANS Principal Instructor*

As a contributing author of the internationally bestselling book *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, he was a member of Foundstone's renowned penetration testing team and served as a senior instructor and co-author of Foundstone's Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS Institute's most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, he holds several security certifications and speaks at conferences around the world. T: @brycegalbraith

FORENSICS 572

Advanced Network Forensics and Analysis

SANS

Six-Day Program
Mon, Jul 20 - Sat, Jul 25
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Philip Hagen

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

Take your system-based forensic knowledge onto the wire, incorporate network evidence into your investigations, provide better findings, and get the job done faster.

Who Should Attend

- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- IT lawyers and paralegals
- Anyone interested in computer network intrusions and investigations

Forensic casework that does not include a network component is a rarity in today's environment. Performing disk forensics will always be a critical and foundational skill, but overlooking the network component of today's computing architecture is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, a data theft case, or an employee misuse scenario, the network often has an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent or even definitively prove that a crime actually occurred.

digital-forensics.sans.org

"The instructor was very knowledgeable with relevant and interesting examples to illustrate key points."
-Everett Sherlock, Kapstone Paper

"SEC572 was an excellent course that kept my attention and it will be immediately useful when I get back to work."
-John Ives, UC Berkeley

FOR572: Advanced Network Forensics and Analysis was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. The course focuses on the knowledge necessary to expand the forensic mindset from residual data on the storage media of a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking – we'll teach you to listen.

giac.org

sans.edu

Bundle OnDemand
with this course
sans.org/ondemand

Philip Hagen *SANS Certified Instructor*

Philip Hagen has been working in the information security field since 1998, running the full spectrum including deep technical tasks, management of an entire computer forensic services portfolio, and executive responsibilities. Currently, Phil is an Evangelist at Red Canary, where he engages with current and future customers of Red Canary's managed threat detection service to ensure their use of the service is best aligned for success in the face of existing and future threats. Phil started his security career while attending the U.S. Air Force Academy, with research covering both the academic and practical sides of security. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. In 2003, Phil became a government contractor, providing technical services for various IT and information security projects. These included systems that demanded 24x7x365 functionality. He later managed a team of 85 computer forensic professionals in the national security sector. He has provided forensic consulting services for law enforcement, government, and commercial clients prior to joining the Red Canary team. Phil is the course lead and co-author of FOR572: Advanced Network Forensics and Analysis. T: @PhilHagen

MANAGEMENT 414

SANS Training Program for CISSP® Certification®

Content Updated for New Exam! Effective April 15th

SANS

Six-Day Program
Mon, Jul 20 - Sat, Jul 25
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: Paul A. Henry

- GIAC Cert: GISP
- DoDD 8570
- OnDemand Bundle

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that has been specifically updated to prepare you to pass the 2015 version of the CISSP® exam.

Course authors Eric Conrad and Seth Misenar, who are also authors of the best-selling Syngress CISSP® Study Guide, have revised MGT414 to take into account the 2015 updates to the CISSP® exam and prepare students to navigate all types of questions included in the new version.

Who Should Attend

- Security professionals who want to understand the concepts covered in the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of network security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® 8 domains
- Security professionals and managers looking for practical ways to apply the 8 domains of knowledge to their current activities

MGT414 focuses solely on the 8 domains of knowledge as determined by (ISC)² that form a critical part of CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

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

"I think Paul is an awesome instructor and his knowledge, experience, and energy really make the classes enjoyable."
-Jim Shields, Tiff Advisory Services

You Will Be Able To:

- Detailed coverage of the 8 domains of knowledge
- The analytical skills required to pass the CISSP® exam
- The technical skills required to understand each question
- The foundational information needed to become a Certified Information Systems Security Professional (CISSP®)

giac.org


sans.org/8570

"As a developing security professional, this course sufficiently covers the core concepts needed to obtain CISSP."
-Kurt Zimmerman, Protivity Inc.

Bundle OnDemand with this course
sans.org/ondemand

Take advantage of SANS CISSP® Get Certified Program currently being offered.
sans.org/special/cissp-get-certified-program

Paul A. Henry *SANS Senior Instructor*

Paul Henry is a Senior Instructor with the SANS Institute and one of the world's foremost global information security and computer forensic experts with more than 20 years' experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. Paul also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the Department of Defense's Satellite Data Project (USA), and both government as well as telecommunications projects throughout Southeast Asia. T: @phenrycissp

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program
Mon, Jul 20 - FRI, Jul 24
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop NOT Needed
Instructors: Ted Demopoulos

- 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.

"I've already learned much in this class and it will greatly assist in increasing my knowledge base and my interaction with my IT/CS departments."
-Jon Shadduck, Ameren Missouri

"This course (MGT512) gives me more oversight and in-depth understanding of networks and data."
-Dean Hardison, DOD BUPERS Millington, TN

giac.org

sans.edu

sans.org/8570

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!

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Ted Demopoulos *SANS Certified Instructor*

Ted Demopoulos' first significant exposure to computers was in 1977 when he had unlimited access to his high school's PDP-11 and hacked at it incessantly. He consequently almost flunked out but learned he liked playing with computers a lot. His business pursuits began in college and have been 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, and maintains Security Certs, a Web site on Security Certifications. 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. Ted lives in New Hampshire and more about him is available at Demopoulos Associates. In his spare time, he is also a food and wine geek, enjoys flyfishing, and playing with his children. T: @TedDemop

SANS@NIGHT EVENING TALKS

Enrich your SANS training experience!

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

KEYNOTE: **Evolving Threats** *Paul A. Henry*

For nearly two decades defenders have fallen into the "Crowd Mentality Trap" and have simply settled on doing the same thing everyone else was doing. While at the same time attackers have clearly evolved both in terms of malware delivery vectors and attack methodology. Today our defenses focus primarily on the gateway and upon attempting to outwit attackers' delivery methods. This leaves us woefully exposed and according to a recent Data Breach Report has resulted in 3,765 incidents, 806 million records exposed, and $157 billion (USD) in data breach costs in only the past 6 years.

Running Away from Security: Web App Vulnerabilities and OSINT Collide

Micah Hoffman

Lately it seems like more and more of our lives are being sucked into the computer world. There are wrist-sensors for tracking our steps, phone apps that plot our workouts on maps, and sites to share our healthy-eating and weight loss progress. When people sign up for these sites, they usually use pseudonyms or the sites give them a unique numbered ID to keep their information "private." How hard would it be to connect a person's step-counting, diet history and other info on these health sites to their real lives? Are businesses using these sites for non-fitness purposes? This talk will show weaknesses in several web applications used for health and exercise tracking and reveal [spoiler alert] how trivial it is to find the real people behind the "private" accounts.

Continuous Ownage: Why you Need Continuous Monitoring

Bryan Simon

Repeat after me, "I will be breached." Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous, and the monitoring must match. This talk will help you face this problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring. The talk will also give you a hint at the value you and your organization will gain from attending Seth Misenar and Eric Conrad's new course Continuous Monitoring and Security Operations.

Infosec Rock Star: Geek will only get you so far *Ted Demopoulos*

Some of us are so effective, and well known, that the term "Rock Stars" is entirely accurate. What kind of skills do Rock Stars have and wannabe Rock Stars need to develop? Although we personally may never be swamped by groupies, we can learn the skills be more effective, well respected, and well paid. Obviously it's not just about technology; in fact most of us are very good at the technology part. And although the myth of the Geek with zero social skills is just that, a myth, the fact is that increasing our skills more on 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.

The Tap House *Phil Hagen*

Packets move pretty fast. The field of Network Forensics needs to move fast, too. Whether you are investigating a known incident, hunting unidentified adversaries in your environment, or enriching forensic findings from disk- and memory-based examinations, it's critical to stay abreast of the latest developments in the discipline. In this @Night series, Phil Hagen will discuss some of the latest technologies, techniques, and tools that you will want to know in pursuit of forensication nirvana. Phil is also an avid craft beer fan, so there's a good chance you will learn something about a new notable national or interesting local beer in the process. This presentation will be helpful for those that wish to keep up-to-date on the most cutting-edge facets of Network Forensics.

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 Minneapolis 2015
Minneapolis, MN | July 20-25 | #SANSmpls

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 SAN JOSE 2015

Hotel Information

Training Campus
The Sainte Claire

302 South Market Street
San Jose, CA 95113
sans.org/event/san-jose-2015/location

The Sainte Claire is one of California's genuine grand hotels – a stately hotel with majestic, plush interiors situated in the heart of downtown San Jose. This landmark embraces the character of yesteryear and greets the innovators of tomorrow with luxurious modern amenities and timeless service. Relaxing and comfortable, yet inspiring and sophisticated – a Silicon Valley Hotel that truly offers the best of both worlds.

Special Hotel Rates Available

A special discounted rate of $211.00 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 25, 2015.

Top 5 reasons to stay at the The Sainte Claire

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

SANS SAN JOSE 2015

Registration Information

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

Register online at sans.org/event/san-jose-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