SANS

THE MOST TRUSTED SOURCE FOR INFORMATION AND SOFTWARE SECURITY TRAINING

San Francisco 2013

July 29 - August 3, 2013

Offering SANS most technically-advanced courses.

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

SANS +S Training Program for the CISSP Certification Exam

Advanced Computer Forensic Analysis and Incident Response

Advanced Security Essentials – Enterprise Defender

Mobile Device Security and Ethical Hacking

IT Security Strategic Planning, Policy, and Leadership

"Great overall experience, excellent content. The instructor was amazing."

-RICHARD TAFOYA, REDFLEX TRAFFIC SYSTEMS

GIAC Approved Training

Register at www.sans.org/event/san-francisco-2013

Dear Colleagues,

Stephen Northcutt

We are inviting you to join us in the Bay Area for **SANS San Francisco 2013**. SANS is bringing seven 5- or 6-day courses to San Francisco, **July 29 - August 3**. Along with offering our two most popular security courses (SEC401 and SEC504), you will be able to choose an advanced security essentials course, a mobile device security course, our advanced computer forensic analysis course, an IT security strategic planning course, or take our training program for the CISSP® certification exam. **Register by June 12 and save up to $500 on tuition fees.**

Looking to get more value out of your San Francisco experience? Enhance your training with our evening events, which are included as part of your registration fee. Our *SANS@Night* talks include **Offensive Digital Forensics** presented by Alissa Torres, and **Base64 Can Get You Pwned!** presented by Kevin Fiscus along with a Keynote, **APT: It is Not Time to Pray, It is Time to Act**, from Dr. Eric Cole. Our *Vendor Showcase* activities will be held on July 30.

SANS training is well-known for being relevant and pragmatic. Our faculty for this event are Dr. Eric Cole, Paul A. Henry, Kevin Fiscus, Alissa Torres, Chris Christianson, Mark Williams, and Christopher Crowley. These expert instructors understand the challenges you face on a daily basis as their real-world experience increases the practical value of the course material.

Our campus for this event, the **Hyatt Fisherman's Wharf**, has a special discounted SANS rate of $209 Single/Double, which will be honored based on space availability. Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through July 3, 2013. See our hotel page for all the information you need. With all that there is to do at Fisherman's Wharf, you will have many enjoyable options to keep you busy when you are not in class! Picture yourself on a bench at Fisherman's Wharf enjoying some Ghirardelli chocolate or clam chowder in a bread bowl while watching the seals or the picturesque bay. The cable car stop is across the street from the hotel, and that can take you to all the San Francisco destinations. For those of you who are night owls, there are countless options within the many San Francisco area districts from amazing restaurants to clubbing and one of a kind bars and boutique shops. See our website: **www.sans.org/event/san-francisco-2013/welcome** for a long list of ideas.

Come see for yourself why SANS is the most trusted source in computer security training, certification, and research. Register today for SANS San Francisco 2013.

Stephen Northcutt
President
The SANS Technology Institute, a postgraduate computer security college

Here's what past Rocky Mountain attendees had to say:

"Best training I have attended in 20 years in the field."
-Wing Chan, Allette, Inc.

"I just recently graduated from college (May 2011) and I thought this class was just going to be a refresher. It was that and so much more! This was my first SANS course, and it won't be the last."
-Michael Stanley, Capital One

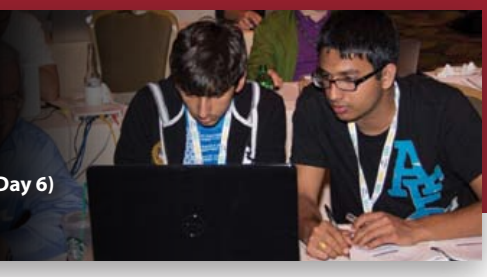
"SANS is always professional organized, flexible, friendly, and personable. I will definitely do business again with you and recommend you to peers."
-Sarah McVey,
Lane County Government

Courses-at-a-Glance

	MON 7/29	TUE 7/30	WED 7/31	THU 8/1	FRI 8/2	SAT 8/3
SEC401 Security Essentials Bootcamp Style	PAGE 1					
SEC501 Advanced Security Essentials - Enterprise Defender	PAGE 2					
SEC504 Hacker Techniques, Exploits, and Incident Handling	PAGE 3					
SEC575 Mobile Device Security and Ethical Hacking	PAGE 4					
FOR508 Advanced Computer Forensic Analysis & Incident Response	PAGE 5					
MGT414 SANS +S Training Program for the CISSP Cert Exam	PAGE 6					
MGT514 IT Security Strategic Planning, Policy and Leadership	PAGE 7					

SECURITY 401

Security Essentials Bootcamp Style



Six-Day Program • Mon, July 29 - Sat, August 3
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required
Instructor: Chris Christianson

It seems wherever you turn organizations are being broken into and the fundamental question that everyone wants answered is: Why? Why do some organizations get broken into and others not? SEC401 Security Essentials is focused on teaching you the right things that need to be done to keep an organization secure. Organizations are spending millions of dollars on security and are still compromised. The problem is they are doing good things but not the right things. Good things will lay a solid foundation but the right things will stop your organization from being headline news in the *Wall Street Journal*. SEC401's focus is to teach individuals the essential skills and techniques needed to protect and secure an organization's critical information assets and business systems. We also understand that security is a journey and not a destination. Therefore, we will teach you how to build a security roadmap that can scale today and into the future. When you leave our training we promise that you will be given techniques that you can implement today and tomorrow to keep your organization at the cutting edge of cyber security. Most importantly, your organization will be secure.

With the APT (advanced persistent threat), organizations are going to be targeted. Whether the attacker is successful penetrating an organization's network depends on the organization's defense. While 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 works in cyber security. 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 on anything in the name of cyber security, three questions must be answered:

1. **What is the risk?**
2. **Is it the highest priority risk?**
3. **Is it the most cost-effective way of reducing the risk?**

Security is all about making sure you are focusing on the right areas of defense. By attending SEC401 you will learn the language and underlying theory of computer security. Since all jobs today require an understanding of security, this course will help you understand why security is important and how it applies to your job. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security 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 gain cutting-edge knowledge you can put into practice immediately upon returning to work; and, (2) You will be taught by the best security instructors in the industry.

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

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/san-francisco-2013.

"I'm a newbie to security. This course presented a ton of information on this subject in a fast-paced, easy-to-understand manner."
-Michael Horkan, Rockwell Automation

Chris Christianson *SANS Instructor*

Chris Christianson is an Information Security Analyst and Network Engineer who lives and works in Northern California. He currently works in the financial industry and is the Assistant Vice President of Network Services for one of the nation's largest credit unions. With more than fifteen years of experience, Chris has spoken at conferences, contributed articles for magazines, and obtained many technical certifications including: CCSE, CCDP, CCNP, GSEC, CISSP, IAM, GCIH, CEH, IEM, GCIA, GREM, GPEN, and GWAPT. He has also earned a Bachelor of Science in Management Information Systems.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

SECURITY 501

Advanced Security Essentials – Enterprise Defender

Six-Day Program • Mon, July 29 - Sat, August 3
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Dr. Eric Cole

Cybersecurity continues to be a critical area for organizations and will continue to increase in importance as attacks become stealthier, have a greater financial impact on an organization, and cause reputational damage. Security Essentials lays a solid foundation for the security practitioner to engage the battle.

"Great course! I'm disturbed/ impressed at how much the instructors know. Top-notch instructors are what makes SANS!"
-Chris Robinson, Sempra Energy

A key theme is that prevention is ideal, but detection is a must. We need to be able to ensure that we constantly improve our security to prevent as many attacks as possible. This prevention/protection occurs on two fronts - externally and internally. Attacks will continue to pose a threat to an organization as data become more portable and networks continue to be porous. Therefore a key focus needs to be on data protection, securing our critical information no matter whether it resides on a server, in a robust network architecture, or on a portable device.

Despite an organization's best effort at preventing attacks and protecting its critical data, some attacks will still be successful. Therefore we need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks and looking for indication of an attack. It also includes performing penetration testing and vulnerability analysis against an organization to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react to it in a timely fashion and perform forensics. Understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

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

"The information taught is valuable and applicable. It does not matter what your job functions are at your company, you will definitely find value in this course."
-Leslie Morales, Southwest Research Institute

Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole has experience in information technology with a focus on helping customers focus on the right areas of security by building out a dynamic defense. Dr. Cole has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. He served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is the author of several books, including ***Advanced Persistent Threat***, ***Hackers Beware***, ***Hiding in Plain Site***, ***Network Security Bible*** 2nd Edition, and ***Insider Threat***. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is the founder and an executive leader at Secure Anchor Consulting where he provides leading-edge cyber security consulting services, expert witness work, and leads research and development initiatives to advance the state-of-the-art in information systems security. Dr. Cole is actively involved with the SANS Technology Institute (STI) and is a SANS faculty fellow and course author who works with students, teaches, and develops and maintains courseware.

"Great course. Best training I have attended. This is my first SANS course and I can't wait to attend more."
-Leonard Crull, MI ANG

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/san-francisco-2013.

www.giac.org

www.sans.edu

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program • Mon, July 29 - Sat, August 3
9:00am - 6:30pm (Day 1) • 9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits • Laptop Required
Instructor: Kevin Fiscus

If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), 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.

"When I get back to the office, I will use the knowledge I gained here to better defend my organization's network."
-Joshua Anthony, West Virginia Army National Guard

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, the in-depth information in this course helps you turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them; and a hands-on workshop for discovering holes before the bad guys do. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

This challenging course is particularly well-suited to individuals who lead or are a part of an incident handling team. Furthermore, 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.

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

"The course covers almost every corner of attack and defense areas. It's a very helpful handbook for a network security analysis job. It upgrades my knowledge in IT security and keeps pace with the trend."
-Anthony Liu, Scotia Bank

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/san-francisco-2013.

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 taught many of SANS most popular classes including SEC401, SEC504, SEC575, FOR508, and MGT414. In addition to his security work, he is a proud husband and father of two children.

"Fantastic class! Fantastic Instructor! I have taken six SANS classes, I have not had a bad experience yet, they are just so professionally done!"
-Rafael Cabrera, Air Force

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

SECURITY 575

Mobile Device Security and Ethical Hacking

Six-Day Program • Mon, July 29 - Sat, August 3
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Christopher Crowley

Mobile phones and tablets have become essential to enterprise and government networks, from small organizations to Fortune 500 companies and large-scale agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient email access as well as managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from enterprise resource planning to project management. With increased reliance on these devices, organizations are quickly recognizing that mobile phones and tablets need greater security implementations than a simple screen protector and clever password.

Who Should Attend:

- **Security personnel whose job involves assessing, deploying, or securing mobile phones and tablets**
- **Network and system administrators supporting mobile phones and tablets**
- **Penetration testers**
- **Ethical hackers**
- **Auditors who need to build deeper technical skills**

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/san-francisco-2013.

The security risks of mobile phone and tablet device use in the workplace

Whether the device is an Apple iPhone or iPad, a Windows Phone, an Android or BlackBerry phone or tablet, the ubiquitous mobile device has become a hugely attractive and vulnerable target for nefarious attackers. The use of mobile devices introduces a vast array of new risks to organizations, including:

- **distributed sensitive data storage and access mechanisms**
- **lack of consistent patch management and firmware updates**
- **the high probability of device loss or theft, and more.**

Mobile code and apps are also introducing new avenues for malware and data leakage, exposing critical enterprise secrets, intellectual property, and personally identifiable information assets to attackers. To further complicate matters, today there simply are not enough people with the security skills needed to manage mobile phone and tablet deployments.

"Wow! This course is everything you need to know about mobile device deployment, risks and more. Don't deploy your mobile devices without taking this course first."
-Bryan Simon, INTEGRIS Credit Union

From mobile device security policy development, to design and deployment, and more

This course was designed to help organizations struggling with mobile device security by equipping personnel with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and mobile code analysis to penetration testing and ethical hacking, this course will help you build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in your organization.

"Don't walk, run to this course if your life has anything to do with mobility. Don't go anywhere else, all other courses are pretenders, this is the best."
-Aamir Lakhani, World Wide Technology

You will gain hands-on experience in designing a secure mobile phone network for local and remote users and learn how to make critical decisions to support devices effectively and securely. You will also be able to analyze and evaluate mobile software threats, and learn how attackers exploit mobile phone weaknesses so you can test the security of your own deployment. With these skills, you will be a valued mobile device security analyst, fully able to guide your organization through the challenges of securely deploying mobile devices.

Christopher Crowley *SANS Certified Instructor*

Mr. Crowley has 10 years of industry experience managing and securing networks. He has GSEC, GCIA, GCIH (gold), GCFA, and CISSP certifications. His teaching experience includes GSEC, GCIA, and GCIH Mentor; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the year award. "The Mentor of the Year Award is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities."

FORENSICS 508

Advanced Computer Forensic Analysis and Incident Response

Six-Day Program • Mon, July 29 - Sat, August 3
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Alissa Torres

This course focuses on providing incident responders with the necessary skills to hunt down and counter a wide range of threats within enterprise networks, including economic espionage, hactivism, and financial crime syndicates. The completely updated FOR508 addresses today's incidents by providing real-life, hands-on response tactics. Don't miss the NEW FOR508!

Who Should Attend:

- Information security professionals
- Incident response team members
- Experienced digital forensic analysts
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 Graduates

DAY 0: A 3-letter government agency contacts you to say that critical information was stolen from a targeted attack on your organization. Don't ask how they know, but they tell you that there are several breached systems within your enterprise. You are compromised by an Advanced Persistent Threat, aka an APT – the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Over 90% of all breach victims learn of a compromise from third party notification, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years. Gather your team—it's time to go hunting.

FOR508: Advanced Computer Forensic Analysis and Incident Response will help you determine:

- **How did the breach occur?**
- **What systems were compromised?**
- **What did they take? What did they change?**
- **How do we remediate the incident?**

"Everything you need to learn for the basics of forensics in just six days; any more knowledge and your head would explode!"
-Matthew Harvey, U.S. Department of Justice

The updated FOR508 trains digital forensic analysts and incident response teams to identify, contain, and remediate sophisticated threats—including APT groups and financial crime syndicates. A hands-on lab—developed from a real-world targeted attack on an enterprise network—leads you through the challenges and solutions. You will identify where the initial targeted attack occurred and which systems an APT group compromised. The course will prepare you to find out which data was stolen and by whom, contain the threat, and provide your organization the capabilities to manage and counter the attack.

During a targeted attack, an organization needs the best incident responders and forensic analysts in the field. FOR508 will train you and your team to be ready to do this work.

"This course doesn't just train you on tools, it teaches you about the system as a whole where important information is saved then how to extract that information."
-Kevin Lees, USNA

Alissa Torres *SANS Certified Instructor*

Alissa Torres is a certified SANS Instructor and Incident Handler at Mandiant, finding evil on a daily basis. She previously worked as a security researcher at KEYW Corporation, leading research and development initiatives in forensic and offensive methodologies and is co-founder of Torrora, LLC, a forensics consulting company. Prior to KEYW, Alissa performed digital forensic investigations and incident response for a large contractor in the Defense Industrial Base. Alissa began her career in information security as a Communications Officer in the United States Marine Corps and is a graduate of University of Virginia and University of Maryland. As an accomplished instructor, Alissa has taught for various government agencies on topics to include digital forensics, incident response, and offensive methodologies, and is a frequent speaker at industry conferences. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/san-francisco-2013.

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

Digital Forensics and Incident Response
http://computer-forensics.sans.org

MANAGEMENT 414

SANS® +S™ Training Program for the CISSP® Certification Exam

Six-Day Program • Mon, July 29 - Sat, August 3
9:00am - 7:00pm (Day 1) • 8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6) • 46 CPE/CMU Credits
Laptop NOT Required • Instructor: Paul A. Henry

The SANS® +S™ Training Program for the CISSP® Certification Exam will cover the security concepts needed to pass the CISSP® exam. This is an accelerated review course that assumes the student has a basic understanding of networks and operating systems and focuses solely on the 10 domains of knowledge of the CISSP®:

Domain 1: Access Controls
Domain 2: Telecommunications and Network Security
Domain 3: Information Security Governance & Risk Management
Domain 4: Software Development Security
Domain 5: Cryptography
Domain 6: Security Architecture and Design
Domain 7: Security Operations
Domain 8: Business Continuity and Disaster Recovery Planning
Domain 9: Legal, Regulations, Investigations and Compliance
Domain 10: Physical (Environmental) Security

Each domain of knowledge is dissected into its critical components. Every component is discussed in terms of its relationship to other components and other areas of network security. After completion of the course, the student will have a good working knowledge of the 10 domains of knowledge and, with proper preparation, be ready to take and pass the CISSP® exam.

"This class focuses like a laser on the key concepts you'll need to understand the CISSP exam. Don't struggle with thousand page textbooks – let this course be your guide!"
-Carl Williams, Harris Corporation

Who Should Attend:

- Security professionals who are interested in understanding 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® 10 Domains
- Security professionals and managers looking for practical ways the 10 domains of knowledge can be applied to the current job

Obtaining your CISSP® certification consists of:

- Fulfilling minimum requirements for professional work experience
- Completing the Candidate Agreement
- Review of résumé
- Passing the CISSP® 250 multiple-choice question exam with a scaled score of 700 points or greater
- Submitting a properly completed and executed Endorsement Form
- Period Audit of CPEs to maintain the credential

External Product Notice: CISSP® exams are not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam.

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

Paul A. Henry *SANS Senior Instructor*

Paul Henry is one of the world's foremost global information security and computer forensic experts with more than 20 years' experience managing security initiatives for Global 2000 enterprises and government organizations worldwide.

Paul is a principle 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.

Paul is frequently cited by major and trade print publications as an expert in computer forensics, technical security topics, and general security trends and serves as an expert commentator for network broadcast outlets, such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications, such as the Information Security Management Handbook, where he is a consistent contributor. Paul serves as a featured and keynote speaker at seminars and conferences worldwide, delivering presentations on diverse topics including anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, firewall architectures, security architectures, and managed security services.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/san-francisco-2013.

"This course breaks the huge CISSP study books down into manageable chunks, and helped me focus and identify weaknesses. The instructor's knowledge and teaching skills are excellent." -Jeff Jones, Constellation Energy Group

GIAC INFORMATION SECURITY PROFESSIONAL GISP
www.giac.org

MANAGEMENT 514

IT Security Strategic Planning, Policy and Leadership

Five-Day Program • Mon, July 29 - Fri, August 2
9:00am - 5:00pm • 30 CPE/CMU Credits
Laptop Recommended • Instructor: Mark Williams

Mastering the Strategic Planning Process

Strategic planning is hard for people in IT and IT Security because we spend so much time responding and reacting. Some of us have been exposed to a SWOT or something similar in an MBA course, but we almost never get to practice until we get promoted to a senior position, and then we are not equipped with the skills we need to run with the pack.

In this course you will learn the entire strategic planning process: what it is and how to do it; what lends itself to virtual teams, and what needs to be done face to face. We will practice building those skills in class. Topics covered in depth include how to "plan the plan," horizon analysis, visioning, environmental scans (SWOT, PEST, Porter's etc.), historical analysis, mission, vision, and value statements. We will also discuss the planning process core, candidate initiatives, the prioritization process, resource and IT change management in planning, how to build the roadmap, setting up assessments, and revising the plan.

Who Should Attend:

•This course is designed and taught for existing, recently appointed, and aspiring IT and IT Security managers and supervisors who desire to enhance their leadership and governance skills to develop their staff into a more productive and cohesive team.

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/san-francisco-2013.

Creating Effective Information Security Policy

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

Developing Management and Leadership Skills

The third focus of the course is on management and leadership competencies. Leadership is a capability that must be learned, exercised and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. However, leaders and followers influence each other toward the goal; it is a two-way street where all parties perform their functions to reach a common objective.

Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organization's mission. Grooming effective leaders is critical to all types of organizations, as the most effective teams are cohesive units that work together toward common goals with camaraderie and a can-do spirit!

Leadership tends to be a bit "squishy" and courses covering the topic are often based upon the opinions of people who were successful in the marketplace. However, success can be as much a factor of luck as skill, so we base this part of the course on five decades of the research of social scientists and their experiments going as far back as Maslow and on research as current as Sunstein and Thaler. We discuss leadership skills that apply to commercial business, non-profit, not-for-profit, or other organizations. This course is designed to develop existing and new supervisors and managers who aspire to go beyond being the boss. It will help you build leadership skills to enhance the organization's climate and team-building skills to support the organization's mission, its growth in productivity, workplace attitude/satisfaction, and staff and customer relationships.

Mark Williams *SANS Instructor*

Mark Williams currently holds the position of Principal Systems Security Officer at BlueCross BlueShield of Tennessee. Mark holds multiple certifications in security and privacy including CISSP, CISA, CRISC, and CIPP/IT. He has authored and taught courses at undergraduate and graduate levels, as well as public seminars around the world. He has worked in public and private sectors in the Americas, Canada, and Europe in the fields of security, compliance, and management. Mark has more than 20 years of international high-tech business experience working with major multinational organizations, governments, and private firms. During this career Mark has consulted on issues of privacy and security, lead seminars, and developed information security, privacy, and compliance related programs.

www.sans.edu

Bonus Sessions

SANS@Night Evening Talks

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

Keynote: APT: It is Time to Act

Dr. Eric Cole

Albert Einstein said "We cannot solve our problems with the same thinking we used when we created them." With the new advanced and emerging threat vectors that are breaking into networks with relative ease, a new approach to security is required. The myth that these attacks are so stealthy they cannot be stopped is just not true. There is no such thing as an unstoppable adversary. It is time to act. In this engaging talk one of the experts on APT, Dr. Cole, will outline an action plan for building a defensible network that focuses on the key motto that "Prevention is Ideal but Detection is a Must". Better understand what the APT really is and what organizations can do to be better prepared. The threat is not going away, so the more organizations can realign their thinking with solutions that actually work, the safer the world will become.

Base64 Can Get You Pwned! *Kevin Fiscus*

There are many different types of numbering systems and related encoding including binary (base2), decimal (base10) and hexadecimal (base16). One commonly used numbering system is base64. Learn how you can use this simple encoding to bypass DLP and WAF controls, write malware to victim systems, and even execute self-contained cross site scripting attacks. Then understand how it is possible to detect this type of threat using freely available tools and techniques.

Offensive Digital Forensics *Alissa Torres*

Network intruders are utilizing sophisticated offensive forensic techniques to parse remote systems, obtain credentials, and locate and steal "target data". Incident responders and forensic examiners must be able to unravel the actions and intent of the adversary on their own networks in order to halt their progress, and anticipate future campaigns. From this session, attendees will gain a deeper understanding of today's offensive forensic strategies, how adversaries determine where key sensitive data and individuals reside and, most importantly, how to detect these techniques utilizing Windows and file system artifacts.

GIAC Program Overview

SANS Technology Institute Open House

For dates, times, and complete information, visit www.sans.org/event/san-francisco-2013/bonus-sessions

Vendor Showcase

Tuesday, July 30
10:30am-10:50am
12:30pm-1:15pm
3:00pm-3:20pm

Our events incorporate external vendor partners showcasing some of the best security solutions available. Take advantage of the opportunity to interact with the people behind the products and learn what they have to offer you and your organization.

How Are You Protecting Your

Risk management is a top priority. The security of these assets depends on the skills and knowledge of your security team. Don't take chances with a one-size fits all security certification. **Get GIAC certified!**

GIAC offers over 20 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

"GIAC is the only certification that proves you have hands-on technical skills."
-Christina Ford, Department of Commerce

"GIAC Certification demonstrates an applied knowledge versus studying a book."
-Alan C, USMC

Learn more about GIAC and how to *Get Certified* at **www.giac.org**

What's Your Next Career Move?

The information security field is growing and maturing rapidly; are you positioned to win? A Master's Degree in Information Security from the SANS Technology Institute will help you build knowledge and skills in management or technical engineering.

STI offers two unique master's degree programs:

Master of Science in Information Security Engineering

Master of Science in Information Security Management

"The STI program prepares me in both technical aptitude and leadership skills. The instructors have extensive real-world experience - you walk out of every class with skills you can use immediately."
-Courtney Imbert, MSISE Student

If you are interested in an STI master's degree, but have not completed your bachelor's degree, we now offer a bachelor's degree completion program through our partnership with Excelsior College.
www.sans.edu

SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

www.sans.edu
info@sans.edu

Three of the courses being offered at SANS San Francisco 2013 may be applied towards an STI master's degree.

Future SANS Training Events

SANS Mobile Device Security SUMMIT

Southern California | May 30 - June 6, 2013

www.sans.org/event/mobile-device-security-summit-2013

SANSFIRE 2013

Washington, DC
June 14-22, 2013

www.sans.org/event/sansfire-2013

SANS Digital Forensics & Incident Response SUMMIT

Austin, TX | July 9-16, 2013

www.sans.org/event/dfir-summit-2013

SANS Rocky Mountain 2013

Denver, CO
July 14-20, 2013

www.sans.org/event/rocky-mountain-2013

SANS Boston 2013

Boston, MA
August 5-10, 2013

www.sans.org/event/boston-2013

SANS Virginia Beach 2013

Virginia Beach, VA
August 19-30, 2013

www.sans.org/event/virginia-beach-2013

SANS Capital City 2013

Washington, DC
September 3-8, 2013

www.sans.org/event/sans-capital-city-2013

SANS Network Security 2013

Las Vegas, NV
September 14-23, 2013

www.sans.org/event/network-security-2013

SANS Seattle 2013

Seattle, WA
October 7-12, 2013

www.sans.org/event/seattle-2013

SANS Chicago 2013

Chicago, IL
Oct 26 - Nov 4, 2013

www.sans.org/event/chicago-2013

Dates may change. Get the complete list of events at www.sans.org

SANS San Francisco 2013

Hotel Information

Conference Location
Hyatt at Fisherman's Wharf

555 North Point Street | San Francisco, CA 94133
Phone: 415-486-4410
fishermanswharf.hyatt.com

Fall in love with "The City by the Bay" from your ideal location at Hyatt at Fisherman's Wharf, a premiere San Francisco luxury hotel. Nob Hill, Chinatown, Alcatraz, and the Golden Gate Bridge are just minutes away. Stroll along Fisherman's Wharf, explore Pier 39, sample delicious fare at Ghirardelli Square, or hop on a picturesque cable car across from the hotel and see famous Lombard Street or Union Square. Experience all San Francisco has to offer from this Fisherman's Wharf hotel landmark.

Special Hotel Rates Available

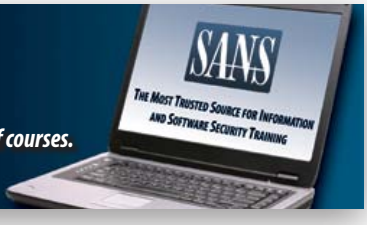
A special discounted rate of $209.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID. These rates include high speed Internet in your room and are only available through July 3, 2013.

Top 5 reasons to stay at the Hyatt at Fisherman's Wharf

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 Hyatt at Fisherman's Wharf, 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 Hyatt at Fisherman's Wharf that you won't want to miss!
5. Everything is in one convenient location!

SANS San Francisco 2013

Registration Information



We recommend you register early to ensure you get your first choice of courses.
Register online at www.sans.org/event/san-francisco-2013

To register, go to www.sans.org/event/san-francisco-2013

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

How to tell if there is room available in a course:

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.

Look for E-mail Confirmation – It Will Arrive Soon After You Register

We recommend you register and pay early to ensure you get your first choice of courses. An immediate e-mail confirmation is sent to you when the registration is submitted properly. If you have not received e-mail confirmation within two business days of registering, please call the SANS Registration office at 301-654-7267 9am - 8pm ET.

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 3, 2013 – processing fees may apply.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**6/12/13**	**$500.00**	**6/26/13**	**$250.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

15% discount if 12 or more people from the same organization register at the same time
10% discount if 8 - 11 people from the same organization register at the same time
5% discount if 4 - 7 people from the same organization register at the same time

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

SANS Voucher Credit Program

Expand your Training Budget! Extend your Fiscal Year. The SANS Voucher Discount Program pays you credits and delivers flexibility.

www.sans.org/vouchers