THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS

Seattle 2013

Seattle, WA | October 7-14

Choose from seven popular courses:

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Intrusion Detection In-Depth

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Advanced Computer Forensic Analysis and Incident Response

Advanced Security Essentials - Enterprise Defender

High-Tech Crime Investigations/ Insider Threats

"I'm a repeat student at a SANS conference. Always great courses and knowledgeable instructors."

-Linh Sithihao, USTW

"I'm always blown away by the knowledge of the SANS instructors!"

-Caleb Queern, Cyveillance

GLOBAL INFORMATION ASSURANCE CERTIFICATION

GIAC

www.giac.org

GIAC Approved Training

Register at
www.sans.org/event/seattle-2013

Save $500
by registering early!
See page 13 for more details.

Dear Colleagues,

We are excited to invite you to attend **SANS Seattle 2013 on October 7-14** and experience SANS hands-on cybersecurity training in the grandeur of the Pacific Northwest. The courses in our lineup offer something for everyone. Choose one to supercharge your career!

A look through this brochure reveals that SANS Seattle 2013 offers top-rated courses brought to you by Dr. Eric Cole, Stephen Northcutt, Bryce Galbraith, Mike Poor, Alissa Torres, and Kevin Fiscus! Our instructor team is the best at ensuring that you can use what you learn the minute you get back to your office.

This brochure will tell you about the DoD 8570 Directive – find out which SANS courses align. See the GIAC page to learn about getting GIAC Certified! Another thing to look for is how to get your Master's Degree through SANS Technology Institute (STI). Take classes in Information Security Management (MSISM) or Engineering (MSISE). You can pick a course that will contribute to all of these that are important to you!

Join us at the **Renaissance Seattle Hotel** in the heart of downtown. The Renaissance Seattle Hotel is just minutes away from both CenturyLink and Safeco Fields. Pike Place Market with its upscale shopping is also close by. This hotel features views of the city skyline, Puget Sound, and the Cascade and Olympic mountains. It is convenient to the Sea-Tac airport and has easy access to major freeways. See the brochure page about the hotel for more information and how to ensure that you get the SANS discount rate for your stay.

Some of the things to see are the Wing Luke Museum dedicated to the Asian American experience or the Hiram M. Chittenden Locks (Ballard Locks), which go up and down regularly to let boats go through Seattle's Lake Washington Ship Canal. There is also a fish ladder that salmon use to migrate the waterways. Taking a dinner cruise or going whale watching in the Puget Sound could be lovely as the temperatures in October have a daily average high near 60 degrees. If indoors is your thing, try the Space Needle at the Seattle Center for views of the area. While at the Seattle Center, don't miss the EMP Museum (Experience Music Project) for the best in music education! Also housed at EMP is the Science Fiction Hall of Fame.

Register and pay by August 21 for a $500 tuition fee discount!
Let your colleagues and friends know about SANS Seattle 2013 and start making your training and travel plans now. We look forward to seeing you there.

Stephen Northcutt
SANS Faculty Fellow

Stephen Northcutt

Here is what past attendees had to say about their SANS training:

"SANS instructors are able to present complex technical info in easy to understand terms. All of the instructors seem to love teaching by sharing enthusiasm and spending time with individual students when needed."

-David Fava, Boeing

"This is by far the best class I have taken. The instructor is ridiculously knowledgeable and entertaining."

-Pierre Defoy,
The Jean Coutu Group -
RX Center

Courses-at-a-Glance

<table>
<tr><th></th><th></th><th>MON
10/7</th><th>TUE
10/8</th><th>WED
10/9</th><th>THU
10/10</th><th>FRI
10/11</th><th>SAT
10/12</th><th>SUN
10/13</th><th>MON
10/14</th></tr>
<tr><td>SEC401</td><td>Security Essentials Bootcamp Style</td><td colspan="6">PAGE 1</td><td></td><td></td></tr>
<tr><td>SEC501</td><td>Advanced Security Essentials - Enterprise Defender</td><td colspan="6">PAGE 2</td><td></td><td></td></tr>
<tr><td>SEC503</td><td>Intrusion Detection In-Depth</td><td colspan="6">PAGE 3</td><td></td><td></td></tr>
<tr><td>SEC504</td><td>Hacker Techniques, Exploits, and Incident Handling</td><td colspan="6">PAGE 4</td><td></td><td></td></tr>
<tr><td>FOR508</td><td>Advanced Computer Forensic Analysis & Incident Response</td><td colspan="6">PAGE 5</td><td></td><td></td></tr>
<tr><td>MGT512</td><td>SANS Security Leadership Essentials For Manager</td><td colspan="5">PAGE 6</td><td></td><td></td><td></td></tr>
<tr><td>HOSTED</td><td>High-Tech Crime Investigations/Insider Threats</td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">PG 7</td></tr>
</table>

SECURITY 401

Security Essentials Bootcamp Style

Six-Day Program • Mon, Oct 7 – Sat, Oct 12
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required
Instructor: Dr. Eric Cole

It seems wherever you turn organizations are being broken into and the fundamental question that everyone wants answered is: Why? Why is it that 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 have the 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.

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 foundation of security principles so they can be as effective as possible at their jobs**
- **Anyone new to information security with some background in information systems and networking**

With the 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 to 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 so that you will be prepared 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.

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

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.

SECURITY 501

Advanced Security Essentials – Enterprise Defender

Six-Day Program • Mon, Oct 7 – Sat, Oct 12
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Bryce Galbraith

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.

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:

- **Students who have taken Security Essentials and want a more advanced 500-level course similar to SEC401**
- **People who have foundational knowledge covered in SEC401, do not want to take a specialized 500-level course, and still want a broad, advanced coverage of the core areas to protect their systems**
- **Anyone looking for detailed technical knowledge on how to protect against, detect, and react to the new threats that will continue to cause harm to an organization**

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

> ***"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

You Will Be Able To

- Identify the threats against network infrastructures and build defensible networks that minimize the impact of attacks
- Learn the tools that can be used to analyze a network to both prevent and detect the adversary
- Decode and analyze packets using various tools to identify anomalies and improve network defenses
- Understand how the adversary compromises networks and how to respond to attacks
- Perform penetration testing against an organization to determine vulnerabilities and points of compromise
- Understand the 6 steps in the incident handling process and be able to create and run an incident handling capability
- Learn how to use various tools to identify and remediate malware across your organization
- Create a data classification program and be able to deploy data loss prevention solutions at both a host and network level

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

www.giac.org

Bryce Galbraith *SANS Certified 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 and his team provide 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 speaks at numerous conferences, and holds several security certifications and blogs about security issues at **http://blog.layeredsec.com**.

www.sans.edu

SECURITY 503

Intrusion Detection In-Depth

Six-Day Program • Mon, Oct 7 – Sat, Oct 12
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Mike Poor

Who Should Attend:

- Intrusion detection analysts (all levels)
- Network engineers
- System, security, and network administrators
- Hands-on security managers

If you have an inkling of awareness of security (even my elderly aunt knows about the perils of the Interweb!), you often hear the disconcerting news about another high-profile company getting compromised. The security landscape is continually changing from what was once only perimeter protection to a current exposure of always-connected and often-vulnerable. Along with this is a great demand for security savvy employees who can help to detect and prevent intrusions. That is our goal in the Intrusion Detection In-Depth course – to acquaint you with the core knowledge, tools, and techniques to prepare you to defend your networks.

This course spans a wide variety of topics from foundational material such as TCP/IP to detecting an intrusion, building in breadth and depth along the way. It's kind of like the "soup to nuts" or bits to bytes to packets to flow of traffic analysis.

"Mike Poor's ability to explain GCIA concepts is unmatched and will allow any junior analyst to hit the ground running."
-Erich Melcher, Sabre Systems, Inc.

"This course is valuable for anyone interested in IDS. Mike's knowledge and willingness to help you understand the material are unlike any other training I've been to. Great course and instructor."
-Dannie Arnold, U.S. Army

Hands-on exercises supplement the coursebook material, allowing you to transfer the knowledge in your head to your keyboard using the Packetrix VMware distribution created by industry practitioner and SANS instructor Mike Poor. As the Packetrix name implies, the distribution contains many of the tricks of the trade to perform packet and traffic analysis. All exercises have two different approaches – a more basic one that assists you by giving hints for answering the questions. Students who feel that they would like more guidance can use this approach. The second approach provides no hints, permitting a student who may already know the material or who has quickly mastered new material to have a more challenging experience. Additionally, there is an "extra credit" stumper question for each exercise intended to challenge the most advanced student.

By week's end, your head should be overflowing with newly gained knowledge and skills; and your luggage should be swollen with course book material that didn't quite get absorbed into your brain during this intense week of learning. This course will enable you to "hit the ground running" once returning to a live environment.

"This course provides a good basis of knowledge and presents important tools which will be at the core of any intrusion analysis."
-Thomas Kelly, DIA

Mike Poor *SANS Senior Instructor*

Mike is a founder and senior security analyst for the Washington D.C. firm InGuardians, Inc. In the past he has worked for Sourcefire as a research engineer and for SANS leading their intrusion analysis team. As a consultant Mike conducts incident response, breach analysis, penetration tests, vulnerability assessments, security audits, and architecture reviews. His primary job focus, however, is in intrusion detection, response, and mitigation. Mike currently holds the GCIA certification and is an expert in network engineering and systems and network and web administration. Mike is an author of the international best selling ***Snort*** series of books from Syngress, a member of the Honeynet Project, and a handler for the SANS Internet Storm Center.

"Course was designed around real-world intrusions and is highly needed for network security administrators and/or analysts."
-Hector Araiza, USAF

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

GIAC CERTIFIED INTRUSION ANALYST GCIA
www.giac.org

SANS TECHNOLOGY INSTITUTE
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program • Mon, Oct 7 – Sat, Oct 12
9:00am - 6:30pm (Day 1) • 9:00am - 5:00pm (Days 2-6)
Laptop Required • 37 CPE/CMU Credits
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.

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.

"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

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

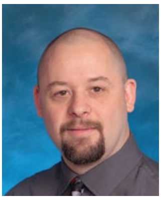
Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/event/seattle-2013.

"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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian



Kevin Fiscus *SANS 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

FORENSICS 508

Advanced Computer Forensic Analysis and Incident Response

Six-Day Program • Mon, Oct 7 – Sat, Oct 12
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.

DAY 0: A 3-letter government agency contacts you to say that critical information was stolen by 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.

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**

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?**

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 were 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.

> ***"Excellent course, invaluable hands-on experience taught by people who not only know the tools and techniques, but know their quirkiness through practical, real-world experience."***
>
> -John Alexander, US Army

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/seattle-2013.

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

www.giac.org

www.sans.edu

www.sans.org/cyber-guardian

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program • Mon, Oct 7 – Fri, Oct 11
9:00am - 6:00pm (Course Days 1-4) • 9:00am - 4:00pm (Course Day 5)
33 CPE/CMU Credits • Laptop NOT Required • Instructor: Stephen Northcutt

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 gain 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 your technical people are telling you**

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.

> *"Tremendously valuable experience!! Learned a lot and also validated a lot of our current pratices. Thank you!!"*
> -Chad Gray, Booz Allen Hamilton

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

Stephen Northcutt *SANS Faculty Fellow*

Stephen Northcutt founded the GIAC certification and served as president of the SANS Technology Institute (**www.sans.edu**). Stephen is author/coauthor of ***Incident Handling Step-by-Step***, ***Intrusion Signatures and Analysis***, ***Inside Network Perimeter Security 2nd Edition***, ***IT Ethics Handbook***, ***SANS Security Essentials***, ***SANS Security Leadership Essentials***, and ***Network Intrusion Detection 3rd Edition***. He was the original author of the Shadow Intrusion Detection system before accepting the position of chief for information warfare at the Ballistic Missile Defense Organization. Stephen is a graduate of Mary Washington College. Before entering the field of computer security, he worked as a Navy helicopter search and rescue crewman, white water raft guide, chef, martial arts instructor, cartographer, and network designer. Since 2007 Stephen has conducted over 40 in-depth interviews with leaders in the security industry, from CEOs of security product companies to the most well-known practitioners, in order to research the competencies required to be a successful leader in the security field. He maintains the SANS Leadership Laboratory, where research on these competencies is posted, as well as SANS Security Musings (**www.sans.edu/research/security-musings**). He leads the Management 512 Alumni Forum, where hundreds of security managers post questions. He is the lead author/instructor for Management 512: SANS Security Leadership Essentials for Managers, a prep course for the GSLC certification that meets all levels of requirements for DoD Security Managers per DoD 8570. He also is the lead author/instructor for Management 514: IT Security Strategic Planning, Policy, and Leadership. Stephen blogs at the SANS Security Laboratory.
www.sans.edu/research/security-laboratory

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

www.giac.org

www.sans.edu

HOSTED COURSE

SANS Hosted are a Series of Classes presented by other educational providers to complement your needs for training outside of our current course offerings.

HOSTED

High-Tech Crime Investigations/ Insider Threats

Two-Day Program • Sun, Oct 13 – Mon, Oct 14
9:00am - 5:00pm • 12 CPE/CMU Credits
Laptop Recommended • Instructor: Bobby Kuzma

Today's connected organizations find themselves at ever increasing risk of criminal victimization from both external, and of even more worry, internal threats. Through a combination of lecture, video reconstruction of incidents, interactive exercises, and role play based on real-world scenarios, participants will develop a best-practices framework for detecting, responding to, and mitigating risks surrounding high-tech crimes.

What's Your Next Career Move?

The information security field is growing and maturing rapidly. Are you positioned to grow with it? A Master's Degree in Information Security from the SANS Technology Institute (STI) will help you build knowledge and skills in management or technical engineering.

The SANS Technology Institute (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

SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

Apply today for the Fall 2013 cohort!
www.sans.edu

www.sans.edu
info@sans.edu
855-672-6733

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 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.

"So What?" The Most Important Question in Information Security *Kevin Fiscus*

The world of information security is filled with sophisticated technical concepts and 0-day "sploits". Penetration testers ride high as the elite of the security community. Unfortunately, the business aspect of security often gets lost. Penetration testers sit confused when their boss or their client doesn't seem to care about getting "root" or domain admin access. The communication gap widens when that boss or that client fails to fix identified problems or to follow sound recommendations. Fortunately, security professionals can solve these problems by just asking a simple question, "So what?"

Why Our Defenses Are Failing Us. One Click Is All It Takes... *Bryce Galbraith*

Organizations are spending unprecedented amounts of money in an attempt to defend their assets...yet all too often, one click is all it takes for everything to come toppling down around them. Every day we read in the news about national secrets, intellectual property, financial records, and personal details being exfiltrated from the largest organizations on earth. How is this being done? How are they bypassing our defenses (e.g. strong passwords, non-privileged accounts, anti-virus, firewalls/proxies, IDS/IPS, logging, etc.)? And most importantly, what can we do about it? A keen understanding of the true risks we face in today's threatscape is paramount to our success.

Sick Anti-analysis Mechanisms in the Wild *Alissa Torres*

For those in the trenches of enterprise defense, it appears malware authors are deriving sick pleasure of late in mechanizing their end products with sophisticated self-defense and evasion capabilities. From "environmentally-aware" binaries to malware that defeats image acquisition, attackers are becoming increasingly more adept at evading analysis. During this presentation, several of these anti-analysis techniques will be explored, preparing attendees for what they are likely to encounter with increasing frequency - malware that fights back.

GIAC Program Overview

SANS Technology Institute Open House

Vendor Showcase

Tuesday, October 8 | 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

- Data?
- Network?
- Systems?
- Critical Infrastructure?

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

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

Get Certified at
www.giac.org

Department of Defense Directive 8570 *(DoDD 8570)*

www.sans.org/8570

Department of Defense Directive 8570 (DoDD 8570) provides guidance and procedures for the training, certification, and management of all government employees who conduct information assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. GIAC provides the most options in the industry for meeting 8570 requirements.

SANS Training Courses for DoDD Approved Certifications

SANS TRAINING COURSE		DoDD APPROVED CERT
SEC401	Security Essentials Bootcamp Style	**GSEC**
SEC501	Advanced Security Essentials - Enterprise Defender	**GCED**
SEC503	Intrusion Detection In-Depth	**GCIA**
SEC504	Hacker Techniques, Exploits & Incident Handling	**GCIH**
AUD507	Auditing Networks, Perimeters, and Systems	**GSNA**
FOR508	Advanced Computer Forensic Analysis and Incident Response	**CCFA**
MGT414	SANS® +S™ Training Program for the CISSP® Certification Exam	**CISSP**
MGT512	SANS Security Essentials for Managers with Knowledge Compression™	**GSLC**

Compliance/Recertification:

To stay compliant with DoD 8570 requirements, you must maintain your certifications. GIAC certifications are renewable every four years. Go to www.giac.org to learn more about certification renewal.

DoDD 8570 certification requirements are subject to change, please visit http://iase.disa.mil/eta/iawip for the most updated version.

For more information, contact us at 8570@sans.org or visit www.sans.org/8570

SECURITY AWARENESS

FOR THE 21st CENTURY

SANS Securing The Human End User

SANS Securing The Human Utility

SANS Securing The Human Developer

SANS Securing The Human Phishing

- Go beyond compliance and focus on changing behaviors.
- Training is maptped against the 20 Critical Controls framework.
- Create your own program by choosing a variety of End User awareness modules.
- Enhance training by adding compliance topics, such as NERC-CIP, PCI DSS, HIPPA, FERPA, and Red Flags, to name a few.
- Test your employees and identify vulnerabilities through phishing emails.
- For a free trial visit us at www.securingthehuman.org

SANS Securing The Human

www.securingthehuman.org

Future SANS Training Events

SANS **Boston** 2013

Boston, MA | August 5-10

www.sans.org/event/boston-2013

SANS **Virginia Beach** 2013

Virginia Beach, VA | August 19-30

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

SANS **Capital City** 2013

Washington, DC | September 3-8

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

SANS **Network Security** 2013

Las Vegas, NV | September 14-23

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

SANS **Baltimore** 2013

Baltimore, MD | October 14-19

www.sans.org/event/baltimore-2013

SANS **Chicago** 2013

Chicago, IL | Oct 28 - Nov 2

www.sans.org/event/chicago-2013

SANS **South Florida** 2013

Fort Lauderdale, FL | November 4-9

www.sans.org/event/sans-south-florida-2013

SANS **Pen Test Hackfest**
TRAINING EVENT AND SUMMIT

Washington, DC | November 7-14

www.sans.org/event/pen-test-hack-fest-2013

SANS Training Formats

LIVE CLASSROOM TRAINING

Multi-Course Training Events

Live instruction from SANS' top faculty, vendor showcase, bonus evening sessions, and networking with your peers

http://www.sans.org/security-training/by-location/all

Community SANS

Live Training in Your Local Region with Smaller Class Sizes

www.sans.org/community

OnSite

Live Training at Your Office Location

www.sans.org/onsite

Mentor

Live Multi-Week Training with a Mentor

www.sans.org/mentor

Summit

Live IT Security Summits and Training

www.sans.org/summit

ONLINE TRAINING

OnDemand

E-learning available anytime, anywhere, at your own pace

www.sans.org/ondemand

vLive

Convenient online instruction from SANS' top instructors

www.sans.org/vlive

Simulcast

Attend a SANS training event without leaving home

www.sans.org/simulcast

CyberCon

Live online training event

www.sans.org/cybercon

SelfStudy

Self-paced online training for the motivated and disciplined infosec student **www.sans.org/selfstudy**

SANS Seattle 2013

Hotel Information

Training Campus
Renaissance Seattle Hotel

515 Madison Street
Seattle, WA 98104
www.sans.org/event/seattle-2013/location

Special Hotel Rates Available

A special discounted rate of $165.00 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 September 13, 2013. To make reservations please call 800-546-9184 and ask for the SANS group rate.

Escape to the Renaissance Seattle Hotel, a stylish hotel in Seattle conveniently located just minutes from Pike Place Market and upscale shopping. There is always something wonderfully new to discover while staying at this hotel. Unwind in spacious guest rooms with stunning views of Puget Sound, the mountains and city skyline. Enjoy casual dining coupled with spectacular city views at R View, a premier Seattle hotel restaurant. Come discover how this hotel seamlessly combines luxury, comfort and technology into an unforgettable urban retreat.

Top 5 reasons to stay at the Renaissance Seattle Hotel

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 Renaissance Seattle Hotel, 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 Renaissance Seattle Hotel that you won't want to miss!

5 Everything is in one convenient location!

SANS Seattle 2013

Registration Information

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

Register online at www.sans.org/event/seattle-2013

SANS
The Most Trusted Source for Information and Software Security Training

To register, go to

www.sans.org/event/seattle-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 September 11, 2013 – processing fees may apply.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	8/21/13	$500.00	9/4/13	$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 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