SANS Houston 2015

THE MOST TRUSTED NAME IN INFORMATION & SOFTWARE SECURITY TRAINING COMES TO HOUSTON MAR 23-28

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

-Michael Lonigro, USAA

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

- Security Essentials Bootcamp Style
- Hacker Tools, Techniques, Exploits, and Incident Handling
- Intrusion Detection In-Depth
- Advanced Digital Forensics and Incident Response
- Advanced Security Essentials – Enterprise Defender
- Mobile Device Security and Ethical Hacking

GIAC Approved Training

Save $400
by registering early!
See page 13 for more details.

REGISTER AT sans.org/event/houston-2015

Dear Colleague,

As I am typing this, we are dealing with another SSL crisis, reports of failed patches in the press, yet again, blaming companies for breaches as they didn't patch fast enough. For a security professional, it is more important than ever to have the fundamental skills to quickly understand new threats and communicate the associated risk appropriately. The classes SANS offers have always been about communicating skills that can be directly applied. Just a couple days ago a student tweeted, "The class was extremely topical. I am able to put some anomaly detection skills to use first thing this am." This is my third time teaching in Houston, and I am excited to come back. Houston offers a rich technology scene and I found that the more regionally focused event leads to many interesting conversations among students, fostering information sharing and learning well beyond the event.

This SANS Houston 2015 brochure provides a complete course schedule, course descriptions, instructor bios, and information on keynote evening talks and cutting-edge security issues. The six courses offered at the event are all associated with the highly regarded GIAC certification, and five certifications align with DoD Directive 8570. GIAC holders are sought after by many industries because they have proven they have the hands-on skills to protect their cyber environment. Put your new knowledge to practical use and build your career by registering for a GIAC certification attempt at www.giac.org. Join more than 63,000 GIAC certified professionals who make the InfoSec industry safe!

Selected courses offered at SANS Houston 2015 can be applied toward an accredited Master of Science in Information Security at the SANS Technology Institute. Corporations are desperate for technically advanced security professionals with effective communications and management skills. Visit www.sans.edu to learn more about how to get started on your master's degree or on one of SANS Technology Institute's graduate certificates, including Penetration Testing and Incident Response.

Our host hotel for SANS Houston 2015, the Royal Sonesta Hotel Houston, is located near shopping, dining, and the city's Uptown entertainment hub. Key destinations include the tree-lined Museum District, with 18 cultural institutions; the Theater District features cutting-edge and classic performing arts facilities; and the 445 acre Hermann Park, which encompasses the Houston Zoo, Houston Garden Center, Miller Outdoor Theatre, and Houston Museum of Natural Science. The Royal Sonesta Hotel will honor a special discounted room rate of $189.00 S/D and will be honored based on space availability. Government per diem rooms are available with proper ID. This rate includes high speed Internet in your room and is only available through March 8, 2015.

Register and pay for any of the 6-day courses by January 28 to save $400 on tuition fees. Don't miss this opportunity to get the training you need while enjoying this great city! Come see for yourself why SANS is the leading organization in computer security training. Make plans to attend and I look forward to seeing you at SANS Houston 2015.

Johannes Ullrich

Johannes Ullrich, PhD
Dean of Research, SANS Technology Institute

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

"One of the best SANS courses I've taken. Extremely knowledgeable instructor with a great way of relating topics to students so they understand!"
-Ryan Gurr, NuScale Power

"This training definitely empowered me with knowledge above standards. If I apply my learnings here, I will be able to perform with more expertise."
-Robin U. Familara, CGI

"The current security landscape is rapidly changing, and the course content is still relevant and important to software security and compliance."
-Scott Hoof, Tripwire, Inc.

SC MAGAZINE AWARDS 2014 WINNER
Honored in the U.S.

COURSES-AT-A-GLANCE

		MON 3/23	TUE 3/24	WED 3/25	THU 3/26	FRI 3/27	SAT 3/28
SEC401	Security Essentials Bootcamp Style	Page 3					
SEC501	Advanced Security Essentials – Enterprise Defender	Page 4					
SEC503	Intrusion Detection In-Depth	Page 5					
SEC504	Hacker Tools, Techniques, Exploits & Incident Handling	Page 6					
SEC575	Mobile Device Security and Ethical Hacking	Page 7					
FOR508	Advanced Digital Forensics and Incident Response	Page 8					

Department of Defense Directive 8570

(DoDD 8570)

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.

DoD Baseline IA Certifications

IAT Level I	IAT Level II	IAT Level III	IAM Level I	IAM Level II	IAM Level III
A+CE Network+CE SSCP	**GSEC** (SEC401) Security+CE SSCP	**GCED** (SEC501) **GCIH** (SEC504) **CISSP** (MGT414) (or Associate) CISA	**GSLC** (MGT512) CAP Security+CE	**GSLC** (MGT512) **CISSP** (MGT414) (or Associate) CAP, CASP CISM	**GSLC** (MGT512) **CISSP** (MGT414) (or Associate) CISM

Computer Network Defense (CND) Certifications

CND Analyst	CND Infrastructure Support	CND Incident Responder	CND Auditor	CND Service Provider Manager
GCIA (SEC503) **GCIH** (SEC504) CEH	SSCP CEH	**GCIH** (SEC504) **GCFA** (FOR508) CSIH, CEH	**GSNA** (AUD507) CISA CEH	CISSP - ISSMP CISM

Information Assurance System Architecture & Engineering (IASAE) Certifications

IASAE I	IASAE II	IASAE III
CISSP (MGT414) (or Associate)	**CISSP** (MGT414) (or Associate) CASP	CISSP - ISSEP CISSP - ISSAP

Computer Environment (CE) Certifications

GCWN (SEC505) **GCUX** (SEC506)

Compliance/Recertification:

To stay compliant with DoDD 8570 requirements, you must maintain your certifications. GIAC certifications are renewable every four years.

Go to 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 sans.org/8570

The Value of SANS Training is Easy to Prove

EXPLORE

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

RELATE

- Consider how recent problems in your own workplace will be solved with the knowledge you'll gain in a SANS course
- Know that the education you receive will make you an expert resource for your team

VALIDATE

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

SAVE

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

ADD VALUE

- Take advantage of the time you'll spend with fellow network security experts at your live training event to compare notes
- Prepare thoughts and questions before arriving to pose to the group
- Attend SANS@Night talks and activities to glean even more knowledge and experience from instructors and peers alike

ALTERNATIVES

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

ACT

- The value of SANS training is apparent, we hope that you will register for a course now or contact us at 301-654-SANS (7267) if you have any further questions

Return on Investment

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

REMEMBER:

SANS is your first and best choice for information and software security training. The SANS Promise is "You will be able to apply our information security training the day you get back to the office!"

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Mar 23 - Sat, Mar 28
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Bryan Simon

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

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

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

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

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

"This is the third time I've taken SEC401. Each time I've taken something new away, and have been able to use it in my day to day job."
-Jennifer Bakowski, John Hancock Financial Services

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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

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

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

"The course SEC401 appears to have a great progressive movement from lower level to more in-depth security practices, and is a great way to refresh topics learned while covering new technology."
-Angela Stewart, Regions Financial Corp.

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

Bryan Simon *SANS Instructor*

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

SECURITY 501

Advanced Security Essentials – Enterprise Defender

SANS

Six-Day Program
Mon, Mar 23 - Sat, Mar 28
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Keith Palmgren

- GIAC Cert: GCED
- STI Master's Program
- DoDD 8570

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

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

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

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

Who Should Attend

- Students who have taken Security Essentials and want a more advanced 500-level course similar to SEC401
- Students who have foundational knowledge covered in SEC401, do not want to take a specialized 500-level course, and still want 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

"I liked the hands-on with tools to understand how they can be used on both sides of the fence."
-John Watts,
Micron Technology, Inc

"In this course [SEC501], I learned how to correctly recognize a security incident, and how to preserve and analyze data in a professional way."
-Puiu Lucian, CHITU ANCOM

giac.org

sans.edu

sans.org/8570

Keith Palmgren *SANS Certified Instructor*

Keith Palmgren is an IT Security professional with 26 years of experience in the field. He began his career with the U.S. Air Force working with cryptographic keys & codes management. He also worked in, what was at the time, the newly-formed computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a senior security architect working on engagements with the DoD and the National Security Agency. As security practice manager for both Sprint and Netigy, Keith built and ran the security consulting practice – responsible for all security consulting world-wide and for leading dozens of security professionals on many consulting engagements across all business spectrums. Currently, Keith is a certified instructor for the SANS Institute. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. As a trainer, Keith has satisfied the needs of nearly 5,000 IT professionals and authored a total of 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications. @kpalmgren

SECURITY 503

Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, Mar 23 - Sat, Mar 28
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor:
Johannes Ullrich, Ph.D.

- GIAC Cert: GCIA
- STI Master's Program
- Cyber Guardian
- DoDD 8570

Reports of prominent organizations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?

Who Should Attend

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

SEC503: Intrusion Detection In-Depth delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You'll get plenty of practice learning to configure and master different open-source tools like tcpdump, Wireshark, Snort, Bro, and many more. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material. In addition, most exercises include an "extra credit" stumper question intended to challenge even the most advanced student.

"Ullrich is very familiar with this material, passionate about the subject, and is a great resource on the topic."
-Brian Rodriguez, San Francisco Police Dept.

"Great combo of theory and hands-on skills, and the labs really help enforce the content."
-Victor Westbrook, Offensive Logic LLC

Industry expert Mike Poor has created a VMware distribution, Packetrix, specifically for this course. As the name implies, Packetrix contains many of the tricks of the trade to perform packet and traffic analysis. It is supplemented with demonstration "pcaps," which are files that contain network traffic. This allows students to follow along on their laptops with the class material and demonstrations. The pcaps also provide a good library of network traffic to use when reviewing the material, especially for certification.

giac.org

Preserving the security of your site in today's threat environment is more challenging than ever before. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and often vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in **SEC503: Intrusion Detection In-Depth** is to acquaint you with the core knowledge, tools, and techniques to defend your networks. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

sans.edu

sans.org/cyber-guardian

sans.org/8570

Johannes Ullrich, Ph.D. *SANS Senior Instructor*

As Dean of Research for the SANS Technology Institute, Johannes is currently responsible for the SANS Internet Storm Center (ISC) and the GIAC Gold program. He founded DShield.org in 2000, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. Prior to working for SANS, Johannes worked as a lead support engineer for a web development company and as a research physicist. Johannes holds a PhD in Physics from SUNY Albany and is located in Jacksonville, Florida. His daily podcast summarizes current security news in a concise format. @johullrich

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Mar 23 - Sat, Mar 28
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Kevin Fiscus

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

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose 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. As defenders, it is essential we understand these hacking tools and techniques.

Who Should Attend

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

"This course provides a dual-perspective when it comes to threats: offensive and defensive. The mentality of one lends itself to the other, and demonstrates the need for the knowledge."
-Michael Jedrey, Commonwealth of Virginia

"SEC504 was very structured and well-presented course, interesting and engaging for people new to the field as well as experienced professionals."
-Ewa Konkolska, Prudential, PGDS

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

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

Kevin Fiscus *SANS Certified Instructor*

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

SECURITY 575

Mobile Device Security and Ethical Hacking

SANS

Six-Day Program
Mon, Mar 23 - Sat, Mar 28
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor:
Christopher Crowley

- GIAC Cert: GMOB
- STI Master's Program

giac.org

sans.edu

"Once again, SANS has exceeded my expectations and successfully refocused my view of threats and risks. I recommend this course because it is very enlightening."
-Charles Allen, EM Solutions

"This course was everything I've been looking for over the last few years. Job well done on putting the course together."
-Troy Wojewoda, Huntington Ingalls Industries

Who Should Attend

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing target networks and systems to find security vulnerabilities

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 e-mail access as well by 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 ERP 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.

Whether the device is an Apple iPhone or iPad, a Windows Phone, or 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.

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 evaluating the network activity generated by mobile applications to mobile code analysis, from exploiting the weaknesses in common mobile applications to conducting a full-scale mobile penetration test, 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.

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*

Christopher Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. Mr. Crowley is the course author for SANS Management 535 - Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the Year Award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. @CCrowMontance

FORENSICS 508

Advanced Digital Forensics and Incident Response

SANS

Six-Day Program
Mon, Mar 23 - Sat, Mar 28
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Chad Tilbury

- GIAC Cert: GCFA
- STI Master's Program
- Cyber Guardian
- DoDD 8570

DFIR
digital-forensics.sans.org

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

Over 80% of all breach victims learn of a compromise from third party notifications, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years.

Who Should Attend

- IT 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 looking to take their skills to the next level

Incident response tactics and procedures have evolved rapidly over the past several years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in your enterprise; they are compromising hundreds. Your team can no longer afford antiquated incident response techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to remediate the incident rapidly.

FOR508: will help your incident response team to determine:

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

This in-depth incident response course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks, including APT adversaries, organized crime syndicates, and hactivism. The completely up to date incident response course (FOR508) addresses today's incidents by providing real-life, hands-on incident response tactics and techniques that elite responders are successfully using in real-world breach cases.

During a targeted attack, an organization needs the best incident response team in the field. FOR508: Advanced Digital Forensics and Incident Response will train you and your team to be ready to respond, detect, scope, and stop intrusions and data breaches.

GATHER YOUR INICDENT RESPONSE TEAM – IT'S TIME TO GO HUNTING

giac.org | sans.org/cyber-guardian | sans.edu | sans.org/8570

"Real-case examples and class discussion around real-world "best-practice" is a valuable part of learning"
-Edgar Zayas, U.S. Securities and Exchange Commission

"This course [FOR508] really takes you from 0-60 in understanding the core concepts of forensics, especially the file system."
-Matthew Harvey, U.S. DoJ

Chad Tilbury *SANS Senior Instructor*

Chad Tilbury has been responding to computer intrusions and conducting forensic investigations since 1998. His extensive law enforcement and international experience stems from working with a broad cross-section of Fortune 500 corporations and government agencies around the world. During his service as a Special Agent with the Air Force Office of Special Investigations, he investigated and conducted computer forensics for a variety of crimes, including hacking, abduction, espionage, identity theft, and multi-million dollar fraud cases. He has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. Chad has worked as a computer security engineer and forensic lead for a major defense contractor and as the Vice President of Worldwide Internet Enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over sixty countries. Chad is a graduate of the U.S. Air Force Academy and holds a B.S. and M.S. in Computer Science as well as GCFA, GCIH, GREM, and ENCE certifications. He is currently a consultant specializing in incident response, corporate espionage, and computer forensics. @chadtilbury

HOUSTON 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: The Internet of Evil Things

Johannes Ullrich, Ph.D.

Embedded systems are the new target. As our networks grow uncontrolled and unsupervised, forgotten machines will take over and rule us all soon. Analyzing the embedded malware that comes with this presents a number of challenges. Current debuggers and virtualization techniques that mimic these systems are incomplete and will not allow us to completely analyze malware the way we are used to in good old desktop malware environments. These malware blackboxes need different instrumentations and techniques. We will present some ideas on how to analyze these malware samples, and introduce you to embedded system analysis (unless your bot is removing this event from your smart watch's reminder list).

The 13 Absolute Truths of Security

Keith Palmgren

Here we will take a non-technical look at each of the thirteen absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls

Kevin Fiscus

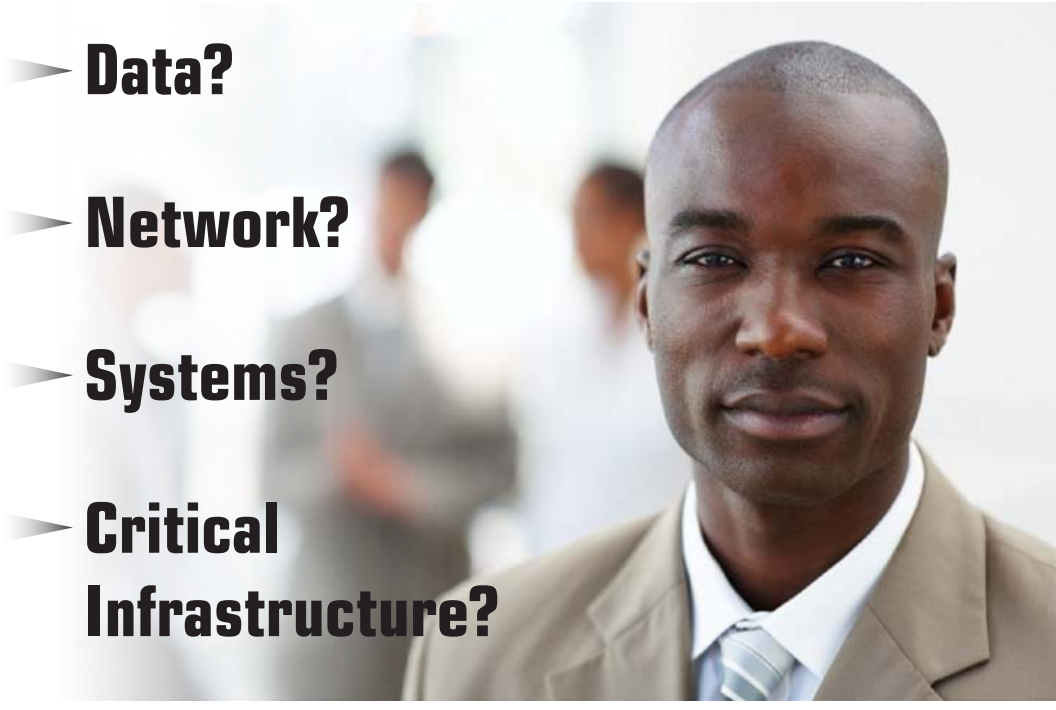
It's all about the information! Two decades after the movie Sneakers, the quote remains as relevant, if not more so. The fact that someone hacks into an environment is interesting but not that relevant. What is important is what happens after the compromise. If the data is destroyed or modified, organizations are negatively impacted but the benefits to an attacker for destruction or alteration are somewhat limited. Stealing information however, is highly profitable. Identity theft, espionage, and financial attacks involve the exfiltration of sensitive data. As a result, organizations deploy tools to detect and/or stop that data exfiltration. While these tools can be extremely valuable, many have serious weaknesses; attackers can encode, hide, or obfuscate the data, or can use secret communication channels. This session will talk about and demonstrate a range of these methods.

Debunking the Complex Password Myth

Keith Palmgren

In this one-hour talk, we will look at the technical and non-technical (human nature) issues behind passwords. Attendees will gain a more complete understanding of passwords and receive solid advice on creating more easily remembered AND significantly stronger passwords at work and at home for their users, themselves, and even their children.

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***

FUTURE SANS TRAINING EVENTS

SANS Security East 2015
New Orleans, LA | January 16-21 | #SecurityEast

SANS Cyber Threat Intelligence SUMMIT & TRAINING 2015
Washington, DC | February 2-9 | #CTISummit

SANS Scottsdale 2015
Scottsdale, AZ | February 16-21 | #SANSScottsdale

10TH ANNUAL ICS Security SUMMIT – ORLANDO 2015
Orlando, FL | February 23 - March 2 | #SANSICS

SANS DFIR Monterey 2015
Monterey, CA | February 23-28 | #DFIRMonterey

SANS Cyber Guardian 2015
Baltimore, MD | March 2-7 | #CyberGuardian

SANS Northern Virginia 2015
Reston, VA | March 9-14 | #SANSNoVA

SANS 2015
Orlando, FL | April 11-18 | #SANS2015

Visit sans.org for a complete schedule.

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

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

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

OnSite sans.org/onsite
Live Training at Your Office Location

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

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

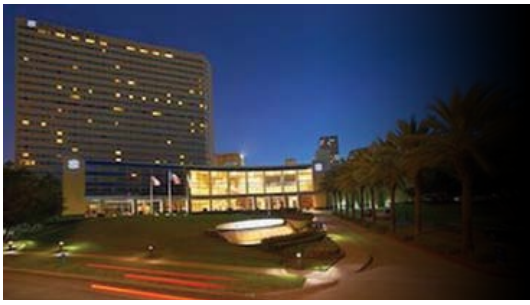
ONLINE TRAINING

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

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

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

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



SANS HOUSTON 2015

Hotel Information

Training Campus

Royal Sonesta Hotel Houston

2222 West Loop South
Houston, TX 77027
sans.org/event/houston-2015/location

Located in the heart of the Galleria area, the newly renovated, AAA rated Four Diamond Royal Sonesta Hotel Houston is in the shopping, dining and entertainment hub of Uptown Houston. It is conveniently positioned near key destinations including downtown Houston, the Museum and Theater districts, and Reliant Park.

Special Hotel Rates Available

A special discounted rate of $189.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through March 8, 2015. To make reservations, please call (800) 766-3782 and ask for the SANS Institute Houston 2015 group rate.

Top 5 reasons to stay at the Royal Sonesta Hotel Houston

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 Royal Sonesta Hotel Houston, 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 Royal Sonesta Hotel Houston that you won't want to miss!
5. Everything is in one convenient location!

SANS HOUSTON 2015

Registration Information

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

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

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

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

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	1/28/15	$400.00	2/25/15	$200.00

Some restrictions apply.

Group Savings (Applies to tuition only)*

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

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

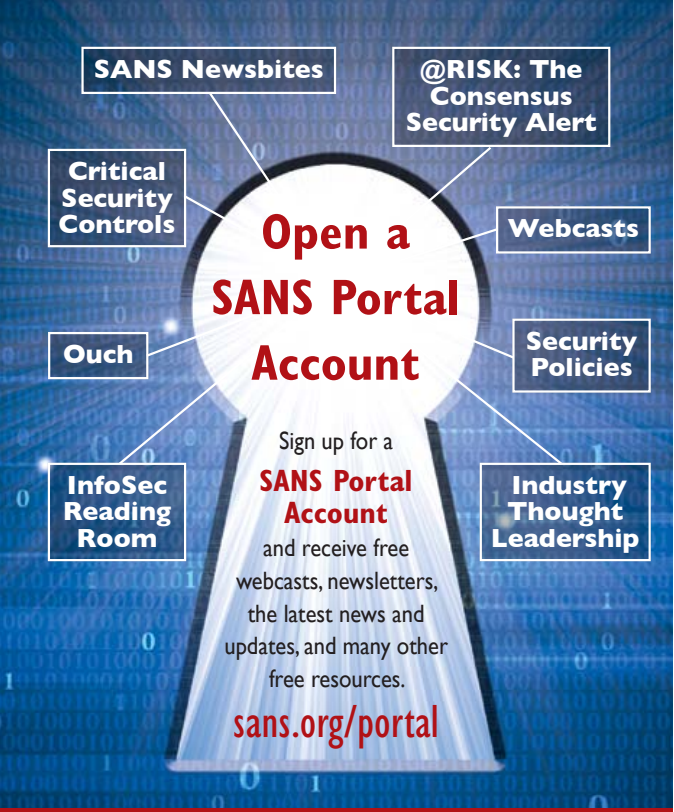
**Early-bird rates and/or other discounts cannot be combined with the group discount.*

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 March 4, 2015 – processing fees may apply.

SANS Voucher Credit Program

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



Register and pay by January 28TH and

SAVE $400

on Houston courses.

sans.org/info/168567