THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

SANS Capital City 2015

Washington, DC July 6-11

Choose from these popular courses:

Intro to Information Security **NEW!**

Continuous Monitoring and Security Operations **NEW!**

Security Essentials Bootcamp Style

Hacker Tools, Techniques, Exploits, and Incident Handling

Web App Penetration Testing and Ethical Hacking

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Virtualization and Private Cloud Security

SANS Training Program for CISSP Certification®

Defending Web Applications Security Essentials

"Best training I've had in a long time; can't wait for my next SANS event!"

-Christopher Costa, Raytheon

GIAC Approved Training

Register at
sans.org/event/capital-city-2015

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

Cyber intrusions are the top of the news on a regular basis, and cyber adversaries are more determined than ever to acquire your organization's private information. You can fight back by making plans now to attend **SANS Capital City 2015** cybersecurity training event from July 6-11 in DC.

SANS Capital City 2015 offers nine hands-on immersion courses in IT security, security management, and defending web applications. The line-up includes our new ***SEC511: Continuous Monitoring and Security Operations***, which shows you how to build a proactive and defensible security architecture that can detect potential security breaches before they're even hatched!

All SANS courses are taught by award-winning industry experts whose goal is to intensively and rapidly scale up your cybersecurity knowledge. SANS instructors apply the concepts and techniques they teach on a daily basis and are considered to be among the best in the world.

This brochure provides you with course descriptions and instructor bios as well as information on extra bonus sessions such as ***SANS@ Night*** presentations and keynote addresses by industry leaders – great enhancements to your classroom training that are free to participants at SANS Capital City 2015.

Seven of our courses offered at Capital City 2015 are associated with ***GIAC Certification***, and three are aligned with ***DoD Directive 8570***. Some of the certifications may help you earn your master's degree at the ***SANS Technology Institute***, which has trained IT security professionals at some of the largest government agencies, defense institutions, and commercial entities in the world. Find out more about GIAC and STI in this brochure.

You can supplement your SANS training with the ***OnDemand Bundle*** option when purchasing a course and gain four months of online access to your course's custom e-learning program, which includes lecture video or audio files, quizzes, and labs – all accessible through your SANS account after your live training ends.

Our campus for SANS Capital City 2015 is the ***Capital Hilton***, located just two blocks north of the White House and near all of the museums, memorials, theatres, art galleries, shopping, and dining that our nation's capital has to offer. Please visit **dcpages.com/Tourism** for more information. A special discounted room rate of $205 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through June 11.

Save $400 by entering discount code "EarlyBird15" on the registration page and paying for any 4-6 day course by May 13! Start making your training and travel plans now; let your colleagues and friends know about SANS Capital City 2015!

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

"From a security operations engineer standpoint, the material and information in course SEC511 is highly relevant."
-Steven Williams,
BNSF Railway

"I don't think I would have been able to follow and grasp the most technical issues without the instructor's style of presentation, he really made the whole experience very enjoyable."
-Valentina Soria,
Bank of England

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

Courses-at-a-Glance

<table>
<tr><th></th><th></th><th>MON 7/6</th><th>TUE 7/7</th><th>WED 7/8</th><th>THU 7/9</th><th>FRI 7/10</th><th>SAT 7/11</th></tr>
<tr><td>SEC301</td><td>Intro to Information Security NEW!</td><td colspan="5">Page 2</td><td></td></tr>
<tr><td>SEC401</td><td>Security Essentials Bootcamp Style</td><td colspan="6">Page 3</td></tr>
<tr><td>SEC504</td><td>Hacker Tools, Techniques, Exploits & Incident Handling</td><td colspan="6">Page 4</td></tr>
<tr><td>SEC511</td><td>Continuous Monitoring and Security Operations NEW!</td><td colspan="6">Page 5</td></tr>
<tr><td>SEC542</td><td>Web App Penetration Testing and Ethical Hacking</td><td colspan="6">Page 6</td></tr>
<tr><td>SEC579</td><td>Virtualization and Private Cloud Security</td><td colspan="6">Page 7</td></tr>
<tr><td>SEC660</td><td>Adv. Pen Testing, Exploit Writing, and Ethical Hacking</td><td colspan="6">Page 8</td></tr>
<tr><td>MGT414</td><td>SANS Training Program for CISSP Certification®</td><td colspan="6">Page 9</td></tr>
<tr><td>DEV522</td><td>Defending Web Applications Security Essentials</td><td colspan="6">Page 10</td></tr>
</table>

@SANSInstitute   *Join the conversation:* #SANSDC

PROTECT YOUR

Data

Network

Systems

Critical Infrastructure

Top Four Reasons to Get GIAC Certified

1. Promotes hands-on technical skills and improves knowledge retention
2. Provides proof that you possess hands-on technical skills
3. Positions you to be promoted and to earn respect from your peers
4. Proves to hiring managers that you are technically qualified for the job

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. GIAC offers over 27 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

Get Certified! www.giac.org

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 will help you build knowledge and skills in management or technical engineering.

Master's Degree Programs:

- ▸ **M.S. in Information Security Engineering**
- ▸ **M.S. in Information Security Management**

Specialized Graduate Certificates:

- ▸ **Penetration Testing & Ethical Hacking**
- ▸ **Incident Response**
- ▸ **Cybersecurity Engineering (Core)**

SANS Technology Institute, an independent subsidiary of SANS,
is accredited by The Middle States Commission on Higher Education.
3624 Market Street | Philadelphia, PA 19104 | 267.285.5000
an institutional accrediting agency recognized by the U.S. Secretary
of Education and the Council for Higher Education Accreditation.

Now eligible for Veterans Education benefits!

Learn more at www.sans.edu | info@sans.edu

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.

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.

SECURITY 301

Intro to Information Security

NEW

Five-Day Program
Mon, Jul 6 - Fri, Jul 10
9:00am - 5:00pm
Laptop Required
30 CPEs
Instructor: Keith Palmgren

- GIAC Cert: GISF
- OnDemand Bundle

To determine if the SANS SEC301course is right for you, ask yourself five simple questions:

- Are you new to information security and in need of an introduction to the fundamentals?
- Are you bombarded with complex technical security terms that you don't understand?
- Are you a non-IT security manager who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o'clock news?
- Do you need to be conversant in basic security concepts, principles, and terms, even if you don't need "deep in the weeds" detail?
- Have you decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification?

If you answer yes to any of these questions, the **SEC301: Introduction to Information Security** training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised five-day comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

This course is designed for students who have no prior knowledge of security and limited knowledge of technology. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

Written by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the **Global Information Security Fundamentals (GISF)** certification test, as well as for the next course up the line, **SEC401: Security Essentials Bootcamp**. It also delivers on the SANS promise:You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.

Who Should Attend

- People who are new to information security and in need of an introduction to the fundamentals of security
- Those who feel bombarded with complex technical security terms they don't understand, but want to understand
- Non-IT security managers who worry their company will be the next mega-breach headline story on the 6 o'clock news
- Professionals in all disciplines who need to be conversant in basic security concepts, principles, and terms, but who don't need "deep in the weeds" detail
- Those who have decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification

"Really interesting course – I feel as if I'm getting a great overview of security, and I now know the areas where I need more training to best get my job done."
RACHEL SHAW, QUALCOMM INCORPORATED

"The instructor was very articulate, and I appreciated the analogies and the outline at the beginning of the day."
-GAVIN SEWELL, NTT/CSL

GIAC INFORMATION SECURITY FUNDAMENTALS GISF
giac.org

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

Keith Palmgren *SANS Certified Instructor*

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

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, Jul 6 - Sat, Jul 11
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Jonathan Ham

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

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks

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

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

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

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

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

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

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

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

GSEC
giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

▶II
Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

Jonathan Ham *SANS Certified Instructor*

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

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Mon, Jul 6 - Sat, Jul 11
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Michael Murr

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

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

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

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. General security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

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

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

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

giac.org

sans.edu

sans.org/cyber-guardian

sans.org/8570

▶❚❚ Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

Michael Murr *SANS Certified Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years, has conducted numerous investigations and computer forensic examinations, and has performed specialized research and development. Michael has taught SANS SEC504 (Hacker Techniques, Exploits, and Incident Handling), SANS FOR508 (Computer Forensics, Investigation, and Response), and SANS FOR610 (Reverse-Engineering Malware); has led SANS@Home courses; and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. Michael holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about digital forensics on his forensic computing blog. E: mmurr@code-x.net T: @mikemurr

SECURITY 511

Continuous Monitoring and Security Operations

NEW

Six-Day Program
Mon, Jul 6 - Sat, Jul 11
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Seth Misenar
▸ OnDemand Bundle

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying to combat cyber threats and prevent cyber attacks, but despite this tremendous effort organizations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses.

The underlying challenge for organizations victimized by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organizations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/ Continuous Security Monitoring (CSM), taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach would be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and Day five will greatly increase your understanding and enhance your skills in implementing Continuous Monitoring utilizing NIST framework.

Who Should Attend

- Security architects
- Senior security engineers
- Technical security managers
- SOC analysts
- SOC engineers
- SOC managers
- CND analysts
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)

"When students walk out, they have a list of action items in hand for making their organization one of the most effective vehicles for frustrating adversaries."
-Eric Conrad and Seth Misenar, SANS

"The material in SEC511 is excellent, and I appreciate the background/pen test material build up to defense. Good defense understands offense."
-Kenneth Hall, BCBSMS

▶II
Bundle OnDemand
with this course
sans.org/ondemand

Seth Misenar *SANS Principal Instructor*

Seth Misenar serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security though leadership, independent research, and security training. Seth's background includes network and web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as both physical and network security consultant for Fortune 100 companies as well as the HIPAA and information security officer for a state government agency. Prior to becoming a security geek, Seth received a BS in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is no stranger to certifications and thus far has achieved credentials which include, but are not limited to, the following: CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. E: smisenar@sans.org T: @sethmisenar

SECURITY 542

Web App Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Jul 6 - Sat, Jul 11
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Micah Hoffman

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

Who Should Attend

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

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

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

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

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

> "This course is giving me a thorough understanding of how web app vulnerabilities can actually be exploited, and therefore why that needed to be fixed.
> -Anna Canning,
> Cannon IT Services LLC

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

giac.org

sans.edu

sans.org/
cyber-guardian

▶II
Bundle OnDemand
WITH THIS COURSE
sans.org/ondemand

Micah Hoffman *SANS Instructor*

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

SECURITY 579

Virtualization and Private Cloud Security

Six-Day Program
Mon, Jul 6 - Sat, Jul 11
9:00am - 5:00pm
Laptop Required
36 CPEs
Instructor: Paul A. Henry
▸ OnDemand Bundle

One of today's most rapidly evolving and widely deployed technologies is server virtualization. Many organizations are already realizing the cost savings from implementing virtualized servers, and systems administrators love the ease of deployment and management for virtualized systems. There are even security benefits of virtualization – easier business continuity and disaster recovery, single points of control over multiple systems, role-based access, and additional auditing and logging capabilities for large infrastructures.

With these benefits comes a dark side, however. Virtualization technology is the focus of many new potential threats and exploits and presents new vulnerabilities that must be managed. In addition, there are a vast number of configuration options that security and system administrators need to understand, with an added layer of complexity that has to be managed by operations teams. Virtualization technologies also connect to network infrastructure and storage networks and require careful planning with regard to access controls, user permissions, and traditional security controls.

In addition, many organizations are evolving virtualized infrastructure into private clouds – internal shared services running on virtualized infrastructure. Security architecture, policies, and processes will need to adapt to work within a cloud infrastructure, and there are many changes that security and operations teams will need to accommodate to ensure assets are protected.

Who Should Attend

- Security personnel who are tasked with securing virtualization and private cloud infrastructure
- Network and systems administrators who need to understand how to architect, secure, and maintain virtualization and cloud technologies
- Technical auditors and consultants who need to gain a deeper understanding of VMware virtualization from a security and compliance perspective

"Overall, it's a great course! The exploits and PoC are cutting edge!! This is the future of IT and security knowledge is power!"
-Joe Marshall, Exelon

"This course (SEC579) was excellent! As always, SANS training is top notch."
-JD Lovering, GE Capital

"Paul was great and shared so much of his experience with us which helped solidify the concepts."
-Stephanie Padilla, Intel Security

"Great course! Anyone involved with managing virtual system environments will benefit from taking SEC579."
-Randall Riley, Defense Security Services

▶II
Bundle OnDemand
with this course
sans.org/ondemand

Paul A. Henry *SANS Senior Instructor*

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

SECURITY 660

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SANS

Six-Day Program
Mon, Jul 6 - Sat, Jul 11
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Stephen Sims

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

This course is designed as a logical progression point for those who have completed **SEC560: Network Penetration Testing and Ethical Hacking**, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered includes weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, return-oriented programming (ROP), Windows exploit-writing, and much more!

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, you need a strong desire to learn, the support of others, and the opportunity to practice and build experience. SEC660 engages attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios. This course goes far beyond simple scanning for low-hanging fruit, and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

Who Should Attend

- Network and systems penetration testers
- Incident handlers
- Application developers
- IDS engineers

giac.org

sans.edu

sans.org/cyber-guardian

▶❚❚ **BUNDLE ONDEMAND** WITH THIS COURSE
sans.org/ondemand

"Stephen is an excellent instructor. It's rare to find an instructor that is so adept yet still make the material approachable."
-Don Bailey,
Blackbird Technologies

"This course (SEC660) gave me the background and tools I'll need to go deeper!"
-Kristine Amari, DoD

"Excellent labs that show real scenarios that will help in understanding exploit of vulnerable ties."
-Pedro Diaz,
Cameron University

Stephen Sims *SANS Senior Instructor*

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant performing reverse engineering, exploit development, threat modeling, and penetration testing. Stephen has an MS in information assurance from Norwich University and is a course author and senior instructor for the SANS Institute. He is the author of SANS' only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP, CISA, Immunity NOP, and many other certifications. In his spare time Stephen enjoys snowboarding and writing music. E: stephen.sims@hotmail.com T: @Steph3nSims

MANAGEMENT 414

SANS Training Program for CISSP Certification®

NEW

Six-Day Program
Mon, Jul 6 - Sat, Jul 11
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: David R. Miller

- GIAC Cert: GISP
- DoDD 8570
- OnDemand Bundle

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

"Best security training I have ever received and had just the right amount of detail for each domain."
-Tony Barnes,
United States Sugar Corp

SANS offers the first course updated for the 2015 version of the CISSP® exam. Eric Conrad and Seth Misenar, authors of the bestselling Syngress CISSP® Study Guide, have fully updated the course to address the 2015 version of the CISSP® exam.

MGT414: SANS Training Program for CISSP® Certification is an accelerated review course designed to prepare you to pass the exam. The course takes into account the 2015 updates to the CISSP® exam and prepares students to navigate all types of questions included on the new version of the exam.

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

After completion of this course, students will have a strong working knowledge of the 8 domains of knowledge and be better placed to pass the exam.

Who Should Attend

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

You Will Be Able To:

- Understand the 8 domains of knowledge that are covered on the CISSP® exam.
- Analyze questions on the exam and be able to select the correct answer.
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam.
- Understand and explain all of the concepts covered in the 8 domains of knowledge.
- Apply the skills learned across the 8 domains to solve security problems when you return to work

GIAC INFORMATION SECURITY PROFESSIONAL GISP
giac.org

sans.org/8570

Bundle OnDemand
with this course
sans.org/ondemand

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

David R. Miller *SANS Instructor*

David has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on the topics of information systems security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security program, including policy writing, network architecture design to include security zones, development of incident response teams and programs, design and implementation of public key infrastructures (PKI), security awareness training programs, specific security solution designs like secure remote access and strong authentication architectures, disaster recovery planning and business continuity planning, and pre-audit compliance gap analysis and remediation. He performs as a security lead and forensic investigator on numerous enterprise-wide IT design and implementation projects for fortune 500 companies, providing compliance, security, technology, and architectural recommendations and guidance. Projects include Microsoft Windows Active Directory enterprise designs, Security Information and Event Management (SIEM) systems, Intrusion Detection and Protection Systems (IDS / IPS), endpoint protection systems, patch management systems, configuration monitoring systems, enterprise data encryption for data at rest, in transit, in use, and within email systems, to describe a few. David is an author, a lecturer and technical editor of books, curriculum, certification exams, and computer-based training videos. E: DMiller@MicroLinkCorp.com

SANS

DEVELOPER 522

Defending Web Applications Security Essentials

Six-Day Program
Mon, Jul 6 - Sat, Jul 11
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor:
Johannes Ullrich, Ph.D.

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

This is the course to take if you have to defend web applications!

Traditional network defenses, such as firewalls, fail to secure web applications. The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure them. DEV522 covers the OWASP Top 10 and will help you to better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world implementations that really work. The testing aspect of vulnerabilities will also be covered so you can ensure your application is tested for the vulnerabilities discussed in class.

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding-level implementation.

DEV522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting Web applications. It is particularly well suited to application security analysts, developers, application architects, pen testers, and auditors who are interested in recommending proper mitigations to web security issues, and to infrastructure security professionals who have an interest in better defending their web applications.

The course will cover the topics outlined by OWASP's Top 10 risks document as well as additional issues the authors found of importance in their day-to-day web application development practice.The topics that will be covered include:

- Infrastructure security
- Server configuration
- Authentication mechanisms
- Application language configuration
- Application coding errors like SQL injection and cross-site scripting
- Cross-site request forging
- Authentication bypass
- Web services and related flaws
- Web 2.0 and its use of web services
- XPATH and XQUERY languages and injection
- Business logic flaws
- Protective HTTP headers

The course will make heavy use of hands-on exercises. It will conclude with a large defensive exercise, reinforcing the lessons learned throughout the week

Who Should Attend

- Application developers
- Application security analysts or managers
- Application architects
- Penetration testers who are interested in learning about defensive strategies
- Security professionals who are interested in learning about web application security
- Auditors who need to understand defensive mechanisms in web applications
- Employees of PCI-compliant organizations who need to be trained to comply with PCI requirements

GWEB
giac.org

sans.edu

▶❚❚
BUNDLE
ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"I'm responsible for the web app sec for my company but have never been a developer. I feel I now have the knowledge needed to sit with my developers to understand and discuss in greater depth the security of our web application!"
-JAMES BAKER, PASS KEY

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. E: jullrich@sans.edu T: @johullrich

SANS@NIGHT EVENING TALKS

Enrich your SANS training experience!

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

KEYNOTE: Evolving Threats *Paul A. Henry*

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

Continuous Ownage: Why you Need Continuous Monitoring *Seth Misenar*

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

The 13 Absolute Truths of Security *Keith Palmgren*

Keith Palmgren has identified thirteen absolute truths of security - things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these thirteen absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the 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.

Debunking the Complex Password Myth *Keith Palmgren*

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

Running Away from Security: Web App Vulnerabilities and OSINT Collide *Micah Hoffman*

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

FUTURE SANS TRAINING EVENTS

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

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

SANS Houston ICS Security Training
Houston, TX | June 1-6 | #SANSICS

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

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

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

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

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

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

SANS San Antonio 2015
San Antonio, TX | August 17-22 | #SANSSATX

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

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

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

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

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

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

ONLINE TRAINING

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

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

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

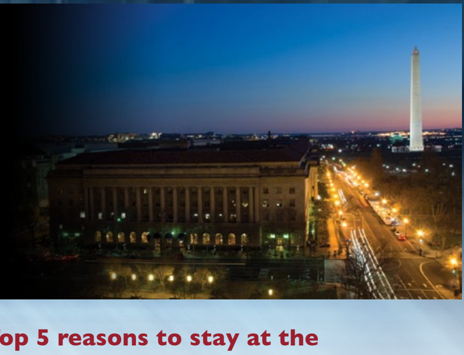
OnDemand Bundles sans.org/ondemand/bundles
Extend Your Training with an OnDemand Bundle Including Four Months of E-learning

SANS CAPITAL CITY 2015

Hotel Information

Training Campus
Capital Hilton

1001 16th Street NW
Washington, DC 20036
sans.org/event/capital-city-2015/location



Downtown DC is where it's at. Just two blocks from the White House and three Metro stations, Capital Hilton is the perfect home base for you in our nation's capital. You can even walk to the National Mall, Washington Monument, memorials and more.

Special Hotel Rates Available

A special discounted rate of $205.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through June 11, 2015.

Top 5 reasons to stay at the Capital Hilton

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 Capital Hilton, 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 Capital Hilton that you won't want to miss!

5 Everything is in one convenient location!

SANS CAPITAL CITY 2015

Registration Information

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

Register online at sans.org/event/capital-city-2015/courses

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

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

Use code **EarlyBird15** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**5/13/15**	**$400.00**	**6/10/15**	**$200.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

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

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

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by June 17, 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