The Most Trusted Source for Information Security Training, Certification, and Research

INFORMATION SECURITY TRAINING

Boston
Summer 2018
August 6-11

Protect Your Business | Advance Your Career

Nine hands-on, immersion-style courses taught by real-world practitioners

See inside for courses offered in:
Cyber Defense
Penetration Testing
Digital Forensics
Ethical Hacking
Critical Security Controls
Security Management
Monitoring and Detection

“SANS training is industry-leading. The knowledge is bleeding-edge, and the training is challenging.”
-Jarred Rossin, Cummins Inc.

SAVE $400
Register and pay by June 13th
Use code EarlyBird18
www.sans.org/boston-summer
Evening Bonus Sessions
Take advantage of these extra evening presentations and add more value to your training. Learn more on page 11

**KEYNOTE: WMI Attacks: What You Don’t Know CAN Hurt You**
-Chad Tilbury

**HTTPdeux**
-Adrien de Beaupre

**Save $400 when you register and pay by June 13th using code EarlyBird18**

Courses at a Glance

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td>Introduction to Cyber Security</td>
<td>Page 1</td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>Page 2</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>Page 3</td>
</tr>
<tr>
<td>SEC505</td>
<td>Securing Windows and PowerShell Automation</td>
<td>Page 4</td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td>Page 5</td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td>Page 6</td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>Page 7</td>
</tr>
<tr>
<td>FOR500</td>
<td>Windows Forensic Analysis</td>
<td>Page 8</td>
</tr>
<tr>
<td>MGT514</td>
<td>Security Strategic Planning, Policy, and Leadership</td>
<td>Page 9</td>
</tr>
</tbody>
</table>

SANS Instructors
Fewer than 100 individuals are currently qualified and designated to teach as SANS Instructors worldwide. This select group of professionals includes recognized industry experts and real-world practitioners, all of whom have proven to be engaging teachers in the classroom. Their up-to-date examples and deep knowledge ensure that what you learn in class will be relevant to your job.

For instructor bios, visit: [www.sans.org/instructors](http://www.sans.org/instructors)

The line-up of SANS Instructors for SANS Boston Summer 2018 includes:

- Adrien de Beaupre
  - Certified Instructor
  - [@adriendb](http://twitter.com/adriendb)
- Ted Demopoulos
  - Principal Instructor
  - [@TedDemop](http://twitter.com/TedDemop)
- Jason Fossen
  - Faculty Fellow
  - [@JasonFossen](http://twitter.com/JasonFossen)
- Michael Murr
  - Principal Instructor
  - [@mikemurr](http://twitter.com/mikemurr)
- My-Ngoc Nguyen
  - Certified Instructor
  - [@MenopNi](http://twitter.com/MenopNi)
- Bryan Simon
  - Certified Instructor
  - [@BryanOnSecurity](http://twitter.com/BryanOnSecurity)
- James Tarala
  - Senior Instructor
  - [@isaudit](http://twitter.com/isaudit)
- Chad Tilbury
  - Senior Instructor
  - [@chadtilbury](http://twitter.com/chadtilbury)
- Jason Fossen
  - Faculty Fellow
  - [@JasonFossen](http://twitter.com/JasonFossen)
- Bryan Simon
  - Certified Instructor
  - [@BryanOnSecurity](http://twitter.com/BryanOnSecurity)
- Mark Williams
  - Instructor
  - [@securemdw](http://twitter.com/securemdw)

Register today for SANS Boston Summer 2018!
[www.sans.org/boston-summer](http://www.sans.org/boston-summer)

Join the conversation:
#SANSBoston
To determine if SANS SEC301: Introduction to Cyber Security is right for you, ask yourself five simple questions:

- Do you have basic computer knowledge, but are new to cybersecurity 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 cybersecurity and need formal training and certification?

If you answer yes to any of these questions, then SEC301: Introduction to Cyber Security training course is for you. Students with a basic knowledge of computers and technology but no prior cybersecurity experience can jump-start their security education with insight and instruction from real-world security experts in SEC301.

This completely revised and comprehensive five-day course covers a wide range of baseline topics, including terminology, the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles. The hands-on, step-by-step learning format will enable you to grasp all the information presented even if some of the topics are new to you. You’ll learn fundamentals of cybersecurity that will serve as the foundation of your security 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 SANS course in this progression, SEC401: Security Essentials Bootcamp Style. 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.

“SANS instructors have an uncanny ability to take complex/complicated subject matter and distill it to terms easily understood by non-technical students.”

- F. Molinari, Citibank
SEC401: Security Essentials Bootcamp Style

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.

Is SEC401: Security Essentials Bootcamp Style the right course for you?

STOP and ask yourself the following questions:

- Do you fully understand why some organizations get compromised and others do not?
- If there were compromised systems on your network, are you confident that you would be able to find them?
- Do you know the effectiveness of each security device and are you certain that they are all configured correctly?
- Are proper security metrics set up and communicated to your executives to drive security decisions?

If you do not know the answers to these questions, then SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

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. Our 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 rise in advanced persistent threats, 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 will 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.

Ted Demopoulos’ first significant exposure to computers was in 1977 when he had unlimited access to his high school’s PDP-11 and hacked at it incessantly. He consequently almost flunked out but learned he liked playing with computers a lot. His business pursuits began in college and have been continuous ever since. His background includes over 25 years of experience in information security and business, including 20+ years as an independent consultant. Ted helped start a successful information security company, was the CTO at a “textbook failure” of a software startup, and has advised several other businesses. Ted is a frequent speaker at conferences and other events, quoted often by the press. He also has written two books on social media, has an ongoing software concern www.sans.edu in Austin, Texas in the virtualization space, and is the recipient of a Department of Defense Award of Excellence. In his spare time, he is also a food and wine geek, and enjoys fly fishing and playing with his children.
The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection and 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.

This course enables you to turn the tables on computer attackers by helping you understand their 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. 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 for, 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, exploiting, and defending systems. This course 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
- 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

Michael Murr 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. He has led SANS Online Training 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.

“I last took SEC504 five plus years ago and so much has changed since then. I love SANS and how they help us to stay up-to-date on the latest techniques so we can better defend our networks.”

- Adam Fowler, GMAC
If you are an IT manager or CIO, the aim for this course is to have it pay for itself 10 times over within two years, because automation isn’t just good for SecOps/DevOps; it can save money too.

This course is designed for systems engineers, security architects, and the Security Operations (SecOps) team. The focus of the course is on how to automate the NSA Top 10 Mitigations and the CIS Critical Security Controls related to Windows, especially the ones that are difficult to implement in large environments.

SEC505 will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) certification exam to prove your Windows security expertise. The GCWN certification counts towards a Master’s Degree in Information Security from the SANS Technology Institute (www.sans.edu) and satisfies the Department of Defense 8140 computing environment requirement. The GCWN is also a foundational certification for soldiers in the U.S. Army’s 255-S Information Protection Program. For DoD students, we will see how to apply the NSA/DISA Secure Host Baseline.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. We don’t cover patch management, share permissions, or other such basics – the aim is to go far beyond that. Come have fun learning PowerShell and Windows security at the same time!
Six-Day Program
Mon, Aug 6 - Sat, Aug 11
This course has extended bootcamp hours
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Bryan Simon

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

We continue to underestimate the tenacity of our adversaries! Organizations are investing significant time and financial and human resources 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, which is 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 will 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 this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

SEC511 will take you on quite a journey. We start by exploring traditional security architecture to assess its current state and the attacks against it. Next, we discuss and discover modern security design that represents a new proactive approach to such architecture that can be easily understood and defended. We then transition to how to actually build the network and endpoint security, and then carefully navigate our way through automation, NSM/CDM/CSM. For timely detection of potential intrusions, the network and systems must be proactively and continuously monitored for any changes in the security posture that might increase the likelihood that attackers will succeed.

Your SEC511 journey will conclude with one last hill to climb! The final day (Day 6) features a Capture-the-Flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. Course authors Eric Conrad and Seth Misenar have designed the Capture-the-Flag competition to be fun, engaging, comprehensive, and challenging. You will not be disappointed!

This course offers invaluable insight into not only the what of monitoring, but also the why – highly recommended!”
- Jason Nickola, DTS

SEC511: Continuous Monitoring and Security Operations

Bryan Simon
SANS Certified Instructor
@BryanOnSecurity

Bryan Simon is an internationally recognized expert in cybersecurity who has been working in the information technology and security field since 1991. 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. He has instructed individuals from the FBI, NATO, and the UN on cybersecurity issues, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in IT security and was most recently profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 13 GIAC certifications including GSEC, GCWN, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GED, GCUX, GSF, and GMON. Bryan’s scholastic achievements have resulted in the honor of sitting as a current member of the SANS Institute Advisory Board and in his acceptance into the prestigious SANS Cyber Guardian program. Bryan teaches SEC401: Security Essentials Bootcamp Style; SEC501: Advanced Security Essentials – Enterprise Defender; SEC505: Securing Windows and Powershell Automaton; and SEC511: Continuous Monitoring and Security Operations.
Web applications play a vital role in every modern organization. However, if your organization doesn’t properly test and secure its web apps, adversaries can 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 scanning to professional, thorough, and high-value web application penetration testing.

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 business tools within any organization. Unfortunately, there is no “patch Tuesday” for custom web applications, and major industry studies find 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 effective web application penetration testing requires something deeper.

SEC542 enables students to assess a web application’s security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations.

In this course, students will come to understand major web application flaws and their exploitation. Most importantly, they’ll learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations. Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. This course will help you demonstrate the true impact of web application flaws through exploitation.

SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn. In addition to having more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way that hammers home lessons learned.

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

SEC542: Web App Penetration Testing and Ethical Hacking

Six-Day Program
Mon, Aug 6 - Sat, Aug 11
9:00am - 5:00pm
36 CPEs
Laptop Required:
Adrien de Beaupre

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

“SEC542 shows a hands-on way of doing web app penetration testing – not just how to use this tool, or that tool.”
-Christopher J. Stover, Infogressive Inc.

Adrien de Beaupre
SANS Certified Instructor
@adriendb

Adrien de Beaupre works as an independent consultant in beautiful Ottawa, Ontario. His work experience includes technical instruction, vulnerability assessment, penetration testing, intrusion detection, incident response and forensic analysis. He is a member of the SANS Internet Storm Center (isc.sans.edu). He is actively involved with the information security community, and has been working with SANS since 2000. Adrien holds a variety of certifications including the GXPN, GPEN, GWAPT, GCICH, GCIA, GSEC, CISSP®, OPST, and OPSA. When not geeking out he can be found with his family, or at the dojo.
Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

As threats evolve, an organization’s security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course that teaches students the Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle. The British government’s Center for the Protection of National Infrastructure describes the Controls as the “baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence.”

SANS in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

The course shows security professionals how to implement the Controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.
FOR500: Windows Forensic Analysis

All organizations must prepare for cyber crime occurring on their computer systems and within their networks. Demand has never been greater for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world’s best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

FOR500: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can’t protect what you don’t understand, and understanding forensic capabilities and artifacts is a core component of information security. You’ll learn to recover, analyze, and authenticate forensic data on Windows systems. You’ll understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. You’ll be able to use your new skills to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR500 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out—attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 10 artifacts.

FOR500 is continually updated. This course utilizes a brand-new intellectual property theft and corporate espionage case that took over six months to create. You work in the real world and your training should include real practice data. Our development team used incidents from their own experiences and investigations and created an incredibly rich and detailed scenario designed to immerse students in a true investigation. The case demonstrates the latest artifacts and technologies an investigator might encounter while analyzing Windows systems. The detailed step-by-step workbook meticulously outlines the tools and techniques that each investigator should follow to solve a forensic case.

MASTER WINDOWS FORENSICS — YOU CAN’T PROTECT WHAT YOU DON’T KNOW ABOUT

Six-Day Program
Mon, Aug 6 - Sat, Aug 11
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Chad Tilbury

Who Should Attend
- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

“This course is a must-do for all incident responders and computer security incident response team leads to be able to answer critical questions quickly and determine the scope of an incident.”

-Brad Milhorn, NTT Data Services

Chad has nearly 20 years of experience working with government agencies, defense contractors, and Fortune 500 companies. He has served as a special agent with the Air Force Office of Special Investigations, where he conducted computer forensics examinations for a variety of crimes and ushered counter-espionage techniques into the digital age. Chad has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. In addition, Chad has worked as a computer security engineer and forensic lead for a major defense contractor and served 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 60 countries. Today, Chad brings his wealth of experience to his role as technical director at CrowdStrike, where he specializes in incident response, corporate espionage, and computer forensics. In addition to being a graduate of the U.S. Air Force Academy, Chad holds B.S. and M.S. degrees in computer science, as well as the GCFA, GCIH, GREM, and ENCE certifications.

SANS Technology Institute
www.sans.edu

Bundle OnDemand with this course

Register at www.sans.org/boston-summer | 301-654-SANS (7267)
As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to do three things:

- **Develop Strategic Plans**
  Strategic planning is hard for people in IT and IT security because we spend so much time responding and reacting. We almost never get to practice until we get promoted to a senior position and then we are not equipped with the skills we need to run with the pack. Learn how to develop strategic plans that resonate with other IT and business leaders.

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

- **Develop Management and Leadership Skills**
  Leadership is a capability that must be learned, exercised and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organization’s mission. Learn to utilize management tools and frameworks to better lead, inspire, and motivate your teams.

Using case studies from Harvard Business School, team-based exercises, and discussions that put students in real-world scenarios, students will participate in activities that they can then carry out with their own team members when they return to work.

The next generation of security leadership must bridge the gap between security staff and senior leadership by strategically planning how to build and run effective security programs. After taking this course you will have the fundamental skills to create strategic plans that protect your company, enable key innovations, and work effectively with your business partners.

**Mark Williams**
SANS Instructor
@securemdw

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/boston-summer-2018/courses](http://www.sans.org/event/boston-summer-2018/courses)
Extend and Validate Your Training

Add an OnDemand Bundle OR GIAC Certification Attempt to your course within seven days of this event to get bundle pricing.*

Extend Your Training Experience with an OnDemand Bundle

- Four months of supplemental online review
- 24/7 online access to your course lectures, materials, quizzes, and labs
- Subject-matter-expert support to help you increase your retention of course material

OnDemand Bundle price – $729

“‘The course content and OnDemand delivery method have both exceeded my expectations.’

- ROBERT JONES, TEAM JONES, INC.

Get Certified with GIAC Certifications

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- Two practice exams included
- Four months of access to complete the attempt

GIAC bundle price – $729

“‘GIAC is the only certification that proves you have hands-on technical skills.’

- CHRISTINA FORD, DEPARTMENT OF COMMERCE

More Information
www.sans.org/ondemand/bundles | www.giac.org

*GIAC and OnDemand Bundles are only available for certain courses.
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: WMI Attacks: What You Don’t Know CAN Hurt You**

Chad Tilbury

In the spectrum of things that keep enterprise security teams up at night, WMI should be heading to the forefront. Advanced adversaries are increasingly adding WMI-based attacks to their repertoires, and most teams are woefully unprepared to face this new threat. You need to understand what you are up against, and attendees will leave this presentation with a comprehensive overview of the state of WMI hacking, including real-world examples of nation-state and criminal actor tradecraft. Once you have a strong understanding of the threat, Chad will pivot to defense and discuss detection tools and analysis techniques. While parts of this presentation will necessarily be technical, even less technically oriented attendees will leave with a greater understanding of the threat and a checklist of actionable steps to better increase their organization’s security posture.

**HTTPdeux**

Adrien de Beaupre

The presentation will discuss the relatively new HTTP2 protocol that has been recently adopted as a standard and is being widely used. Most browsers and web servers can support it, but relatively little security research has been done on the new protocol. There are very few tools to perform security testing, and penetration testing is challenging. The presentation will include a demo of a HTTP2 vulnerability being exploited.

---

**SANS SECURITY AWARENESS**

Security Awareness Training by the Most Trusted Source

Protect Your Employees

Keep your organization safe with flexible, computer-based training.

- **End User**
  - Train employees on their own schedule
- **CIP**
  - Modify modules to address specific audiences
- **ICS Engineers**
  - Increase comprehension – courses translated into many languages
- **Developers**
  - Test learner comprehension through module quizzes
- **Healthcare**
  - Track training completion for compliance reporting purposes

Learn more about SANS Security Awareness at:

[securingthehuman.sans.org](http://securingthehuman.sans.org)
Future Training Events

Northern VA Spring – Reston: Reston, VA | May 20-25
Atlanta: Atlanta, GA | May 29 - Jun 3
Rocky Mountain: Denver, CO | Jun 4-9
Crystal City: Arlington, VA | Jun 18-23
Minneapolis: Minneapolis, MN | Jun 25-30
Vancouver: Vancouver, BC | Jun 25-30
Charlotte: Charlotte, NC | Jul 9-14

SANSFIRE

Washington, DC | Jul 14-21

Boston Summer: Boston, MA | Aug 6-11
San Antonio: San Antonio, TX | Aug 6-11
New York City Summer: New York, NY | Aug 13-18
Northern VA – Alexandria: Alexandria, VA | Aug 13-18
Virginia Beach: Virginia Beach, VA | Aug 20-31
Chicago: Chicago, IL | Aug 20-25
San Francisco Summer: San Francisco, CA | Aug 26-31
Tampa-Clearwater: Tampa, FL | Sep 4-9
Baltimore Fall: Baltimore, MD | Sep 10-15

Network Security

Las Vegas, NV | Sep 23-28

Northern VA Fall – Tysons: Tysons, VA | Oct 13-20
Rocky Mountain Fall: Denver, CO | Oct 15-20
Seattle Fall: Seattle, WA | Oct 15-20
Houston: Houston, TX | Oct 29 - Nov 3
Dallas Fall: Dallas, TX | Nov 5-10
San Diego Fall: San Diego, CA | Nov 12-17

Future Summit Events

DFIR: Austin, TX | Jun 7-14
Security Awareness: Charleston, SC | Aug 6-15
Data Breach: New York City, NY | Aug 20-27
Threat Hunting & Incident Response: New Orleans, LA | Sep 6-13
Alaska: Anchorage, AK | Sep 10-15
Oil & Gas Cybersecurity: Houston, TX | Oct 1-6

Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit www.sans.org/community for up-to-date Community course information.
Register online at www.sans.org/boston-summer

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

Select your course 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.

Cancellation & Access Policy

If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply.

All substitution requests must be submitted by email to registration@sans.org.

If an attendee must cancel and no substitute is available, a refund can be issued for any received payments by July 18, 2018. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.

SANS Voucher Program

Expand your training budget!

Extend your fiscal year. The SANS Voucher Program provides flexibility and may earn you bonus funds for training.

www.sans.org/vouchers

Pay Early and Save*

Use code EarlyBird18 when registering early

<table>
<thead>
<tr>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-13-18</td>
<td>$400.00</td>
<td>7-4-18</td>
<td>$200.00</td>
</tr>
</tbody>
</table>

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.

Omni Parker House

60 School Street
Boston, MA 02108
617-227-8600

www.sans.org/event/boston-spring-2018/location

Hotel Information

Top 3 reasons to stay at the Omni Parker House

1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Omni Parker House, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
3. SANS schedules morning and evening events at the Omni Parker House that you won’t want to miss!

Special Hotel Rates Available

A special discounted rate of $220.00 S/D will be honored based on space availability.

The group rate is lower than the government per diem rate. Should the government per diem rate fall below the group rate, 20% of the guest room block will be made available at the prevailing government per diem rate. These rates include high-speed Internet in your room and are only available through 5pm EST on July 16, 2018.

This grand luxury hotel has been symbolic of Boston’s rich history and culture since 1855. Old World charm and elegance are accompanied by all of the modern conveniences of a world-class establishment. Nestled in the heart of downtown Boston, Omni Parker House is located along the Freedom Trail and at the foot of Beacon Hill, Boston Common, Quincy Market and Faneuil Hall Marketplace. Omni Parker House is just 2.3 miles from Logan International Airport (10 minutes).

Registration Information

Register online at www.sans.org/boston-summer

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

SANS Voucher Program

Expand your training budget!

Extend your fiscal year. The SANS Voucher Program provides flexibility and may earn you bonus funds for training.

www.sans.org/vouchers

Cancellation & Access Policy

If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply.

All substitution requests must be submitted by email to registration@sans.org. If an attendee must cancel and no substitute is available, a refund can be issued for any received payments by July 18, 2018. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.
Join the SANS.org community today to enjoy these free resources at www.sans.org/account

Newsletters

NewsBites
Twice-weekly, high-level executive summaries of the most important news relevant to cybersecurity professionals.

OUCH!
The world’s leading monthly free security awareness newsletter designed for the common computer user.

@RISK: The Consensus Security Alert
A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data.

Webcasts

Ask the Experts Webcasts
SANS experts bring current and timely information on relevant topics in IT security.

Analyst Webcasts
A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

WhatWorks Webcasts
The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT security issues.

Tool Talks
Tool Talks are designed to give you a solid understanding of a problem, and how a vendor's commercial tool can be used to solve or mitigate that problem.

Other Free Resources (No SANS account is necessary)

• InfoSec Reading Room
• Top 25 Software Errors
• 20 Critical Controls
• Security Policies
• Intrusion Detection FAQs
• Tip of the Day

• Security Posters
• Thought Leaders
• 20 Coolest Careers
• Security Glossary
• SCORE (Security Consensus Operational Readiness Evaluation)

Save $400 when you pay for any 4-, 5-, or 6-day course and enter the code “EarlyBird18” by June 13th. www.sans.org/boston-summer

As the leading provider of information defense, security, and intelligence training to military, government, and industry groups, the SANS Institute is proud to be a Corporate Member of the AFCEA community.

5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

To be removed from future mailings, please contact unsubscribe@sans.org or (301) 654-SANS (7267). Please include name and complete address. NALT-BRO-Boston-2018