THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

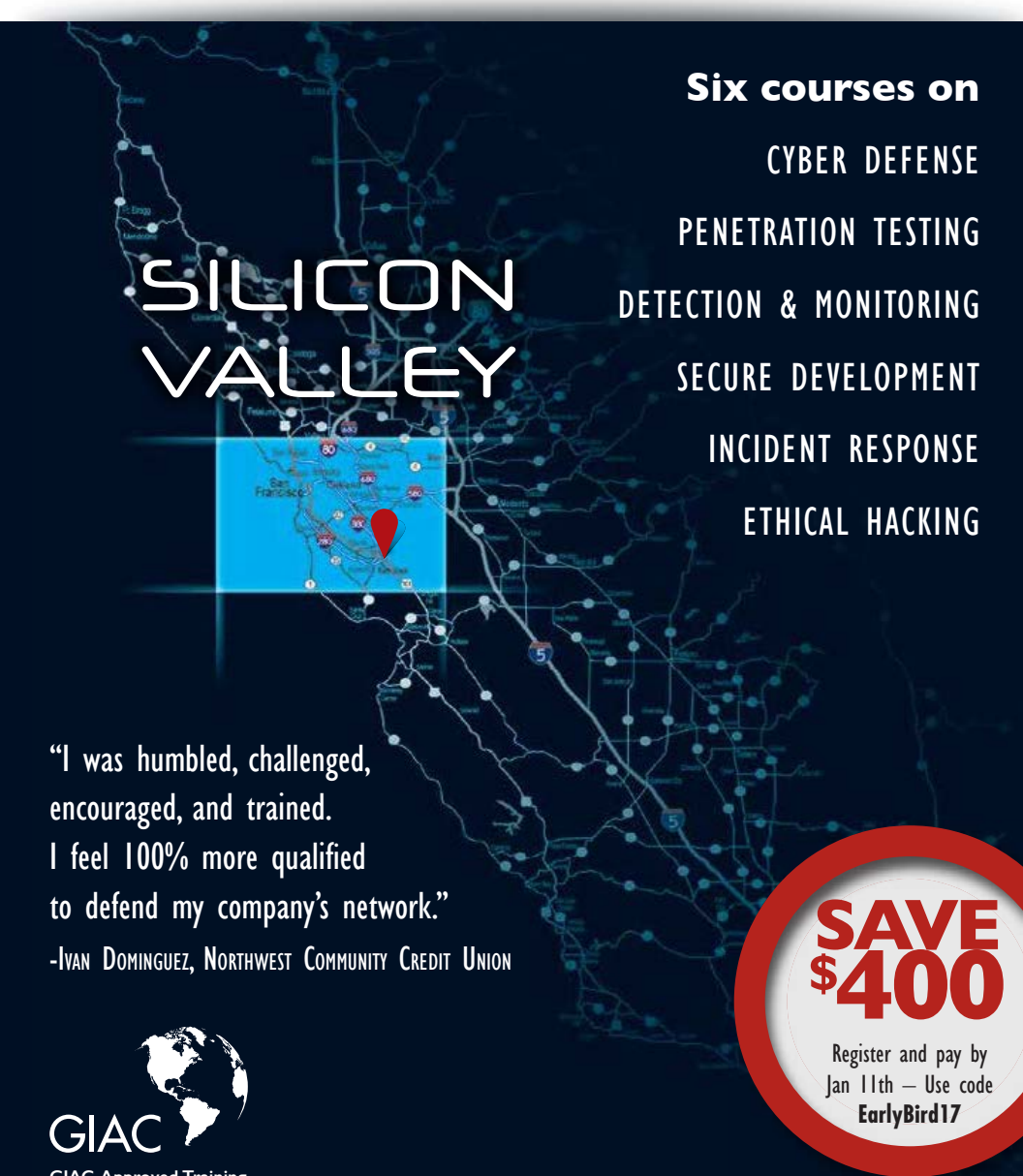
SANS San Jose 2017

San Jose, CA March 6-11

PROTECT YOUR COMPANY AND ADVANCE YOUR CAREER
WITH HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS



Six courses on

CYBER DEFENSE

PENETRATION TESTING

DETECTION & MONITORING

SECURE DEVELOPMENT

INCIDENT RESPONSE

ETHICAL HACKING

"I was humbled, challenged, encouraged, and trained. I feel 100% more qualified to defend my company's network."

-Ivan Dominguez, Northwest Community Credit Union

SAVE $400

Register and pay by Jan 11th – Use code **EarlyBird17**

GIAC

GIAC-Approved Training

www.sans.org/san-jose

SANS Instructors

SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses. This guarantees that what you learn in class will be up to date and relevant to your job. The SANS San Jose 2017 lineup of instructors includes:

Adrien de Beaupre
Certified Instructor
@adriendb

Matt Edmondson
SANS Instructor
@matt0177

Paul A. Henry
Senior Instructor
@phenrycissp

Seth Misenar
Senior Instructor
@sethmisenar

Michael Murr
Principal Instructor
@mikemurr

Clay Risenhoover
Certified Instructor
@AuditClay

Bryan Simon
Certified Instructor
@BryanOnSecurity

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 8.

KEYNOTE: ***Evolving Threats*** – Paul Henry

Actionable Detects: Blue Team Cyber Defense Tactics – Seth Misenar

Python for OSINT Domination – Matt Edmondson

HTTPdeux – Adrien de Beaupre

Save $400 when you register and pay by Jan 11th using code EarlyBird17

Courses at a Glance

The Value of SANS Training & YOU

EXPLORE

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

RELATE

- Consider how security needs in your workplace will be met with the knowledge you'll gain in a SANS course
- Know the education you receive will make you an expert resource for your team

VALIDATE

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

SAVE

- Register early to pay less using early-bird specials

ADD VALUE

- Network with fellow security experts in your industry
- Prepare thoughts and questions before arriving to share with the group
- Attend SANS@Night talks and activities to gain even more knowledge and experience from instructors and peers alike

ALTERNATIVES

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

ACT

- Bring the value of SANS training to your career and organization by registering for a course today, or contact us at 301-654-SANS with further questions

Return on Investment

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

REMEMBER

the SANS promise:

You will be able to apply our information security training the day you get back to the office!

SEC401:
Security Essentials Bootcamp Style

SANS

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

www.giac.org/gsec

www.sans.edu

www.sans.org/8140

www.sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"Loved this course! So practical. My customer's systems will be more secure as a result of this course."
-Howard Foster, Schneider Electric

This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. You'll 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*!

With the rise of 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'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.

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic analysts, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

Bryan Simon *SANS Certified Instructor*

Bryan Simon is an internationally recognized expert in cybersecurity and 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 organizations such as the FBI, NATO, and the UN in matters of cybersecurity, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. 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 12 GIAC certifications including GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, GCUX, and GISF. Bryan's scholastic achievements have resulted in the honor of sitting as a current member of the Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program. Bryan is a SANS instructor for SEC401, SEC501, SEC505, and SEC511. @BryanOnSecurity

SEC501:

Advanced Security Essentials – Enterprise Defender

SANS

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

www.giac.org/gced

www.sans.edu

www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand

"Paul Henry is an excellent instructor who presents large volumes of information effectively."
-Rowley Molina, Altria

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

Who Should Attend

- Incident response and penetration testers
- Security Operations Center engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

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

"We aren't just learning how to use the tools, we also have real-world examples to avoid possible pitfalls. There is cloud-based analysis that is so useful, but I would never have thought of using it had Paul not covered it."
-Stuart Long, Bank of England

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

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

Paul A. Henry *SANS Senior Instructor*

Paul is one of the world's foremost global information security and computer forensic experts, with more than 20 years' experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a 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. He 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 U.S. Department of Defense's Satellite Data Project, and both government and telecommunications projects throughout Southeast Asia. Paul is frequently cited by major publications as an expert on perimeter security, incident response, computer forensics, and general security trends, and serves as an expert commentator for network broadcast outlets such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications such as the *Information Security Management Handbook*, to which he is a consistent contributor. Paul is a featured speaker at seminars and conferences worldwide, delivering presentations on diverse topics such as anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, perimeter security, and incident response. @phenrycissp

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

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

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.**

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

"This course prepares you for anything and everything that comes your way as a security professional." -Matthew Nappi, Stony Brook University

This course enables you to turn the tables on computer attackers by helping you to 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 attacks. 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 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.**

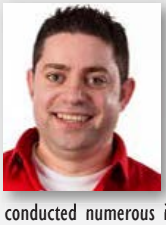
www.giac.org/gcih

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
with this course
www.sans.org/ondemand



Michael Murr *SANS Principal Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years. He has conducted numerous investigations and computer forensic examinations, and performed specialized research and development. Michael has taught SEC504: Hacker Techniques, Exploits, and Incident Handling; FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting; and FOR610: Reverse-Engineering Malware. He has also 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. He 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 (www.forensicblog.org). @mikemurr

Matt Edmondson *SANS Instructor*

Matt performs technical duties for the U.S. government and is a Principal at Argelius Labs, where he performs security assessments and consulting work. Matt's extensive experience with digital forensics includes conducting numerous examinations and testifying as an expert witness on multiple occasions. Matt is a member of the SANS Advisory Board and holds 11 GIAC certifications, including GREM, GCFA, GPEN, GCIH, GWAPT, GMOB and GCIA. In addition, Matt holds the Offensive Security Certified Professional (OSCP) certification. @matt0177

SEC511:

Continuous Monitoring and Security Operations

New Extended Bootcamp Hours to Enhance Your Skills

SANS

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

www.giac.org/gmon

www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"This course had great lessons that will be actionable to what I do day to day, and it will help me fill in the gaps at my current work environment."
-Kevin South, Navient Corporation

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying to prevent and combat 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.

Who Should Attend

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

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.

"Seth is an amazing teacher. His knowledge and passion for InfoSec definitely shows."
-Eric Luellen, SAS

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 is 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.

Seth Misenar *SANS Senior Instructor*

Seth Misenar is the founder of Jackson, Mississippi-based Context Security, where he provides information security thought leadership, independent research, and security training. Seth's background includes network and web application penetration testing, vulnerability assessment, regulatory compliance, security architecture design, and general security consulting. He has previously served as both physical and network security consultant for Fortune 100 companies and the Health Insurance Portability and Accountability Act, and as information security officer for a state government agency. Prior to becoming a security geek, Seth received a bachelor's of science degree 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 that include CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. @sethmisenar

SEC642:

Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

NEW

Six-Day Program
Mon, Mar 6 - Sat, Mar 11
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
36 CPEs
Laptop Required
Instructor:
Adrien de Beaupre

Who Should Attend

- Web penetration testers
- Red team members
- Vulnerability assessment personnel
- Network penetration testers
- Security consultants
- Developers
- QA testers
- System administrators
- IT managers
- System architects

Can Your Web Apps Withstand the Onslaught of Modern Advanced Attack Techniques?

Modern web applications are growing more sophisticated and complex as they utilize exciting new technologies and support ever-more critical operations. Long gone are the days of basic HTML requests and responses. Even in the age of Web 2.0 and AJAX, the complexity of HTTP and modern web applications is progressing at breathtaking speed. With the demands of highly available web clusters and cloud deployments, web applications are looking to deliver more functionality in smaller packets, with a decreased strain on backend infrastructure. Welcome to an era that includes tricked-out cryptography, WebSockets, HTTP/2, and a whole lot more. Are your web application assessment and penetration testing skills ready to evaluate these impressive new technologies and make them more secure?

"This course is outstanding! I would highly recommend it to pen testers who already have a good grasp on SEC542's content."
-Mark Geeslin, Citrix

Are You Ready to Put Your Web Apps to the Test with Cutting-Edge Skills?

This pen testing course is designed to teach you the advanced skills and techniques required to test modern web applications and next-generation technologies. The course uses a combination of lecture, real-world experiences, and hands-on exercises to teach you the techniques to test the security of tried-and-true internal enterprise web technologies, as well as cutting-edge Internet-facing applications. The final course day culminates in a Capture-the-Flag competition where you will apply the knowledge you acquired during the previous five days in a fun environment based on real-world technologies.

"It's the perfect course for someone who has a background in web app pen test but wants to really gain advanced skills."
-Matthew Sullivan, Webfilings

Hands-on Learning of Advanced Web App Exploitation Skills

We begin by exploring advanced techniques and attacks to which all modern-day complex applications may be vulnerable. We'll learn about new web frameworks and web backends, then explore encryption as it relates to web applications, digging deep into practical cryptography used by the web, including techniques to identify the type of encryption in use within the application and methods for exploiting or abusing it. We'll look at alternative front ends to web applications and web services such as mobile applications, and examine new protocols such as HTTP/2 and WebSockets. The final portion of class will focus on how to identify and bypass web application firewalls, filtering, and other protection techniques.

Adrien de Beaupre *SANS Certified Instructor*

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, GCIH, GCIA, GSEC, CISSP, OPST, and OPSA. When not geeking out he can be found with his family, or at the dojo. @adriendb

DEV522:
Defending Web Applications Security Essentials

SANS

Six-Day Program
Mon, Mar 6 - Sat, Mar 11
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
36 CPEs
Laptop Required
Instructor: Clay Risenhoover

www.giac.org/gweb

www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"This course goes over security issues that every web developer and appsec employee needs."
-ALLEN OTT, BOEING

"The course helped me realize the importance of securing web applications and applying secure coding rules for development efforts."
-LERMA WINCHELL, VYSTAR CREDIT UNION

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

The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure them. Traditional network defenses, such as firewalls, fail to secure web applications. DEV522 covers the OWASP Top 10 Risks and will help you 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 applications that have been proven to work. The testing aspect of vulnerabilities will also be covered so that 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, auditors who are interested in recommending proper mitigations for web security issues, and infrastructure security professionals who have an interest in better defending their web applications.

The course will also cover additional issues the authors have found to be important in their day-to-day web application development practices. 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 and conclude with a large defensive exercise that reinforces 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

Clay Risenhoover *SANS Certified Instructor*

Clay is the president of Risenhoover Consulting, Inc., an IT management consulting firm based in Durant, Oklahoma. Founded in 2003, RCI provides IT audit and IT management consulting services to clients in multiple sectors. Clay's experience includes positions in software development, technical training, LAN and WAN operations, and IT management in both the private and public sectors. He has a master's degree in computer science and holds a number of technical and security certifications, including the GPEN, GSNA, CISA, CISM, GWEB, and CISSP. @AuditClay

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 Henry

For nearly two decades, defenders have fallen into the "Crowd Mentality Trap." They 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 attacker's 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.

Actionable Detects: Blue Team Cyber Defense Tactics

Seth Misenar

Organizations relying on third parties to detect breaches can go almost a full year before finding out they have been compromised. Detect the breach yourself, and on average you will find it within about a month of the initial occurrence. Considering detection and defense against modern adversaries too costly to perform yourself can be a very expensive miscalculation if you take into account the substantially increased price of response when a breach drags on. This constantly updated presentation provides you with thoughts, tactics, techniques, and procedures to once again take pride in your Blue Team cyber capabilities. Not applying these lessons learned could prove costly in the face of threat actors that are constantly adapting. Dig in and learn to hold your head high when talking about your defensive cyber operations capabilities.

Python for OSINT Domination

Matt Edmondson

In just about every engagement, the first step is reconnaissance and information gathering. There can be an overwhelming amount of information out there and anything you can do to automate the process of acquiring and analyzing it will make your life a lot easier. This presentation will start with simple data mining techniques where APIs and basic scraping can be used. We then address possible challenges to an automated approach, such as sites that require user interaction to log in, click buttons, scroll down, etc. Working proof of concept code will be provided for all of the topics discussed.

HTTPdeux

Adrien de Beaupre

The presentation will discuss the relatively new HTTP2 protocol that has recently been widely adopted as a standard. 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. There will be a demo of a HTTP2 vulnerability being exploited.

Employers need good talent. Veterans need good jobs. SANS VetSuccess Immersion Academy delivers both.

Introducing the SANS VetSuccess Immersion Academy, an intensive, accelerated program that provides the real-world training and certifications needed to fill critical jobs in cybersecurity.

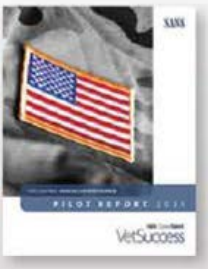
For employers, the academy is a faster, more reliable, and less expensive way to find, train, certify, and employ highly qualified cybersecurity talent.

For transitioning veterans, the academy provides free accelerated training and certifications to quickly and effectively launch careers in cybersecurity.

Find out how your organization can benefit from hiring graduates or sponsoring an academy to meet your specific talent needs.

Read the Pilot Program Results Report
Visit sans.org/vetsuccess

SANS | CyberTalent
IMMERSION ACADEMY



Read the Pilot Program Results Report
Visit sans.org/vetsuccess

Enhance Your Training Experience

Add an

OnDemand Bundle & GIAC Certification Attempt*

to your course within seven days of this event for just $689 each.

SPECIAL 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

"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 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.

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events www.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 www.sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

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

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

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

ONLINE TRAINING

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

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

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

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

FUTURE SANS TRAINING EVENTS

Security East 2017
New Orleans, LA | Jan 9-14

Las Vegas 2017
Las Vegas, NV | Jan 23-30

Cyber Threat Intelligence
SUMMIT & TRAINING 2017
Arlington, VA | Jan 25 - Feb 1

SOUTHERN CALIFORNIA
Anaheim 2017
Anaheim, CA | Feb 6-11

Scottsdale 2017
Scottsdale, AZ | Feb 20-25

Dallas 2017
Dallas, TX | Feb 27 - Mar 4

Tysons Corner Spring 2017
McLean, VA | Mar 20-25

ICS Security
SUMMIT & TRAINING 2017
Orlando, FL | Mar 20-27

Pen Test Austin 2017
Austin, TX | Mar 27 - Apr 1

SANS 2017
Orlando, FL | Apr 7-14

Threat Hunting and IR
SUMMIT & TRAINING 2017
Orlando, FL | Apr 18-25

Baltimore Spring 2017
Baltimore, MD | Apr 24-29

Automotive Cybersecurity
SUMMIT & TRAINING 2017
Detroit, MI | May 1-8

Security West 2017
San Diego, CA | May 9-18

Information on all events can be found at
www.sans.org/security-training/by-location/all

SANS SAN JOSE 2017

Hotel Information

Training Campus

Crowne Plaza San Jose Silicon Valley

777 Bellew Drive
Milpitas, CA 95035
408-321-9500
www.sans.org/event/san-jose-2017/location

Experience everything Silicon Valley has to offer when you stay at this newly renovated hotel. Located in the "Capitol of Silicon Valley" and just a short distance from the San Jose International Airport, this hotel offers spacious rooms and amenities to accommodate your travel needs.

Special Hotel Rates Available

A special discounted rate of $213.00 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 February 13, 2017.

Top 5 reasons to stay at Crowne Plaza San Jose Silicon Valley

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 Crowne Plaza San Jose Silicon Valley, 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 Crowne Plaza San Jose Silicon Valley that you won't want to miss!
5. Everything is in one convenient location!

SANS SAN JOSE 2017

Registration Information

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

Register online at www.sans.org/san-jose

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.

Use code **EarlyBird17** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**1-11-17**	**$400.00**	**2-1-17**	**$200.00**

Some restrictions 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

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 February 15, 2017 – processing fees may apply.

Open a **SANS Account** today to enjoy these FREE resources:

WEBCASTS

Ask The Expert 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 to show how a vendor's commercial tool can be used to solve or mitigate that problem.

NEWSLETTERS

NewsBites – Twice-weekly high-level executive summary 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

OTHER FREE RESOURCES

- 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)

www.sans.org/account