San Francisco
Spring 2019
March 11-16

Protect Your Business | Advance Your Career

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

See inside for courses and GIAC certifications in:

- Cyber Defense
- Penetration Testing
- Ethical Hacking
- Monitoring and Detection
- Digital Forensics
- Secure Development

“SANS training introduces very good tools and processes necessary for individuals and enterprises alike to be successful and stay on top of their security posture.”

-Mark Vlcek, Cisco Systems, Inc.

SAVE $350
Register and pay by Jan 16th
Use code EarlyBird19

www.sans.org/san-francisco-spring
SANS instructors are innovative thought leaders teaching constantly updated, practical security techniques. Join us at SANS San Francisco Spring 2019, and learn how to out-think and out-maneuver cyber adversaries with cutting-edge cybersecurity tactics. Take advantage of these opportunities to get the most out of your training:

- Distinguish yourself as an information security leader by preparing for your GIAC Certification.
- Network with like-minded security professionals facing similar challenges.
- Attend evening bonus sessions led by SANS instructors and gain insight into the latest cybersecurity topics.
- Extend your SANS course by four months with an OnDemand Bundle.

SANS is recognized around the world as the best place to develop the deep, hands-on cybersecurity skills most needed right now. Register today for immersion-style training that will provide you with the skills to defend your organization against security breaches and prevent future attacks.

Courses at a Glance

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>4</td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>5</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>6</td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td>7</td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td>8</td>
</tr>
<tr>
<td>FOR518</td>
<td>Mac and iOS Forensic Analysis and Incident Response</td>
<td>9</td>
</tr>
<tr>
<td>DEV540</td>
<td>Secure DevOps and Cloud Application Security</td>
<td>10</td>
</tr>
</tbody>
</table>

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 11.

**General Session – Welcome to SANS**
– David Hoelzer

**KEYNOTE: OODA Security: Taking Back the Advantage**
– Kevin Fiscus

**Hunting Logic Attacks**
– Hassan El Hadary

**No Seriously, I Can Still See You!**
– Jonathan Ham

Save $350 when you register and pay by Jan 16th using code EarlyBird19

Register today for SANS San Francisco Spring 2019!
www.sans.org/san-francisco-spring

@SANSInstitute
Join the conversation: #SANSSSF
SANS Faculty

At SANS, our course authors and instructors are renowned cybersecurity experts, sharing their knowledge through their own real-world examples and top-shelf curriculum. Industry professionals choose SANS training again and again, year after year, for access to these highly regarded experts.

There are only about 100 individuals currently qualified as SANS Certified Instructors, globally, each selected after proving their technical and teaching expertise through years of work and success. They are the founders of international cybersecurity organizations, authors of best-selling books, and developers of the world’s most advanced cyber ranges and Capture-the-Flag challenges. Many of them are regularly called upon to share their expertise with government and commercial organizations around the world.

In addition to their impressive résumés, every member of our faculty is fully committed to providing the most comprehensive training possible. Our instructors do more than just stand in front of a classroom—they’re present for their students every step of the way, with follow-ups, webcasts, mentoring, and more. Their goal is your success, and that dedication is what truly sets SANS training apart from all the rest.

Whether you train with SANS online or at one of our live events, we promise you'll be able to apply what you learn from these top-tier instructors as soon as you return to work.

“\nI have attended several SANS classes over the years and I am always impressed with the level of knowledge and professionalism of the instructors.\n”

-Ron Foupht, Sirius Computer Solutions

Meet the SANS faculty: www.sans.org/san-francisco-spring/instructors
Securing Approval and Budget for Training

Write a formal request
- All organizations are different, but because training requires a significant investment of both time and money, most successful training requests justify the need and benefit in writing (via a short memo and/or a few PowerPoint slides).
- Provide all the necessary information in one place, including copies of the Training Roadmap, instructor bio, Why SANS? summary pages, and a list of additional benefits offered at our live events or online.

Be specific
- How does the course relate to the job you need to be doing? Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context.
- Highlight the specifics of what you’ll be able to do after training. Each SANS course description includes a section titled “You Will Be Able To.” Be sure to include this in your request to make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Establish longer-term expectations
- Information security is a specialized career path within IT, with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense—not a once-and-done item.
- Take a GIAC Certification exam to prove the training worked. Employers value the validation of skills and knowledge that a GIAC Certification provides. Exams are psychometrically designed to establish competency for related job tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expenses into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.
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.*

- 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 – $769

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 – $769

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

-CHRISTINA FORD, DEPARTMENT OF COMMERCE

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

-ROBERT JONES, TEAM JONES, INC.

More Information

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

*GIAC and OnDemand Bundles are only available for certain courses.
SEC401: Security Essentials Bootcamp Style

Six-Day Program
Mon, Mar 11 - Sat, Mar 16
This course has extended bootcamp hours
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required

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 specialists, penetration testers, and auditors who need a solid foundation of security principles to be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

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 the SEC401 course 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.

Jonathan is an independent consultant who specializes in large-scale enterprise security issues from policy and procedures to staffing and training, 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 20 years, advising in both the public and private sectors, from small startups 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 worked in cybersecurity, 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.

Jonathan Ham
SANS Principal Instructor
@jhamcorp

Meets DoDD 8140
Starts March 11, 2019
Enrollment is limited
Register now
Register at www.sans.org/san-francisco-spring | 301-654-SANS (7267)

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

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

Mark Twain said, “It is easier to fool people than to convince them that they’ve been fooled.” Too many IDS/IPS solutions provide a simplistic red/green, good/bad assessment of traffic and too many untrained analysts accept that feedback as the absolute truth. This course emphasizes the theory that a properly trained analyst uses an IDS alert as a starting point for examination of traffic, not as a final assessment. SEC503 imparts the philosophy that the analyst must have access and the ability to examine the alerts to give them meaning and context. You will learn to investigate and reconstruct activity to deem if it is noteworthy or a false indication.

This course delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to master different open-source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material.

Andy Laman has over 25 years of information technology and security experience in multiple industries. Andy has held lead security positions in Fortune 500 and global companies. He is currently an Assistant Vice President responsible for IT Security and Infrastructure. In addition to the CISSP®, Andy holds multiple GIAC certifications including the prestigious GIAC Security Expert (GSE #142) certification as well as several other industry certifications.
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.

“SEC504 is foundational and core strength-building in the most critical areas of incident handling. It reinforces and develops understanding around roles and TTPs of both the adversary and defender.”

-Araceli Ari Gomes, Dell Secureworks

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors, where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively on information security for the past 12 years. Kevin currently holds the CISA, GPEN, GREM, GMOB, GCED, GCFA-Gold, GCIA-Gold, GCIH, GAWN, GPFA, GCWN, GSC-Gold, GSEC, SCSA, KCS, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. He has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. Kevin has taught many of SANS’s most popular classes including SEC401, SEC464, SEC503, SEC504, SEC542, SEC560, SEC561, SEC575, FOR508, and MGT414.
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.

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn. The course features more than 30 formal hands-on labs and 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.

Hassan is an expert in application security. He has performed application security assessments, secure code reviews and penetration tests for critical security applications. Hassan started his career as a programmer, during which time he developed his passion for information security. He received his master’s degree in computer science from the American University in Cairo with a thesis in the field of secure software engineering. Hassan is an active security researcher in bug bounty programs. He has been acknowledged and rewarded by several vendors such as Google, Apple, Facebook, Yahoo, Oracle, Twitter, PayPal, eBay, Etsy, AT&T, Gift Cards, Cisco Meraki, and Groupon. Published vulnerabilities are available on the blog http://hassanhadary.blogspot.com.eg
FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting

Six-Day Program
Mon, Mar 11 - Sat, Mar 16
9:00am - 5:00pm
36 CPEs
Laptop Required

Who Should Attend
- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Information security professionals
- Federal agents and law enforcement personnel
- Red team members, penetration testers, and exploit developers
- SANS FOR500 and SEC504 graduates

FOR508 will help you to:
- Detect how and when a breach occurred
- Identify compromised and affected systems
- Perform damage assessments and determine what was stolen or changed
- Contain and remediate incidents
- Develop key sources of threat intelligence
- Hunt down additional breaches using knowledge of the adversary

DAY 0: A 3-letter government agency contacts you to say an advanced threat group is targeting organizations like yours, and that your organization is likely a target. They won’t tell how they know, but they suspect that there are already several breached systems within your enterprise. An advanced persistent threat, aka an APT, is likely involved. This is the most sophisticated threat that you are likely to face in your efforts to defend your systems and data, and these adversaries may have been actively rummaging through your network undetected for months or even years.

This is a hypothetical situation, but the chances are very high that hidden threats already exist inside your organization’s networks. Organizations can’t afford to believe that their security measures are perfect and impenetrable, no matter how thorough their security precautions might be. Prevention systems alone are insufficient to counter focused human adversaries who know how to get around most security and monitoring tools.

The key is to constantly look for attacks that get past security systems, and to catch intrusions in progress, rather than after attackers have completed their objectives and done significant damage to the organization. For the incident responder, this process is known as “threat hunting.” Threat hunting uses known adversary behaviors to proactively examine the network and endpoints in order to identify new data breaches.

Threat hunting and Incident response tactics and procedures have evolved rapidly over the past several years. Your team can no longer afford to use antiquated incident response and threat hunting techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident. Incident response and threat hunting teams are the keys to identifying and observing malware indicators and patterns of activity in order to generate accurate threat intelligence that can be used to detect current and future intrusions.

This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and hactivists. Constantly updated, FOR508 addresses today’s incidents by providing hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to detect, counter, and respond to real-world breach cases.

GATHER YOUR INCIDENT RESPONSE TEAM – IT’S TIME TO GO HUNTING!

As a Special Agent with the FBI, Eric Zimmerman had responsibilities that included managing on-scene triage. He identified several gaps in an existing process and started creating solutions to address them. What began as building and expanding a few live response tools led Eric down a path that eventually led to him writing more than 50 programs that are now used by nearly 8,800 law enforcement officers in over 80 countries. Much of Eric’s work involved designing and building software related to investigations of sexual abuse of children. In a single year, Eric’s programs led to the rescue of hundreds of children. On-scene triage tools were developed as a result, in May 2012, Eric was given a National Center for Missing and Exploited Children’s DoDD 8140 award, which honors outstanding law enforcement professionals who have performed above and beyond the call of duty. Eric was also presented with the U.S. Attorney Award for Excellence in Law Enforcement in 2013. Today, Eric serves as a Senior Director at Kroll in the company’s cybersecurity and investigations practice. As an instructor, Eric’s focus on understanding the big picture of digital forensics prepares students to perform better analysis, do new research of their own, and identify the best tools or techniques to perform successful investigations – all skills that will have a lifelong impact.

Eric Zimmerman
SANS Certified Instructor
@EricZimmerman
Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are familiar with Windows-only machines.

Times and trends change and forensic investigators and analysts need to change with them. The new FOR518: Mac Forensic Analysis course provides the tools and techniques necessary to take on any Mac case without hesitation. The intense, hands-on forensic analysis skills taught in the course will enable Windows-based investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyze any Mac or iOS system.

This course will teach you:

▐ Mac and iOS Fundamentals: How to analyze and parse the Hierarchical File System (HFS+) by hand and recognize the specific domains of the logical file system and Mac-specific file types.

▐ User Activity: How to understand and profile users through their data files and preference configurations.

▐ Advanced Analysis and Correlation: How to determine how a system has been used or compromised by using the system and user data files in correlation with system log files.

▐ Apple Technologies: How to understand and analyze many Mac and iOS specific technologies, including Time Machine, Spotlight, iCloud, Document Versions, FileVault, Continuity, and FaceTime.

FOR518: Mac Forensic Analysis aims to form a well-rounded investigator by introducing Mac and iOS forensics into a Windows-based forensics world. This course focuses on topics such as the HFS+ file system, Mac-specific data files, tracking of user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac-exclusive technologies. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac or iOS forensics case.

FORENSICATE DIFFERENTLY!

“A we have primarily Mac OS environment and I don’t think I could find a tenth of this information through my own research.”

-Kevin Neely, Pure Storage

Sarah Edwards
SANS Certified Instructor
@iamevltwin

A self-described Mac nerd, Sarah Edwards is a forensic analyst, author, speaker, and both author and instructor of SANS FOR518: Mac Forensic Analysis. She has been a devoted user of Apple devices for many years and has worked specifically in Mac forensics since 2004, carving out a niche for herself when this area of forensics was still new. Although Sarah appreciates digital forensics in all platforms, she has a passion for working within Apple environments and is well known for her work with cutting-edge Mac OS X and iOS, and for her forensic file system expertise. Sarah has more than 12 years of experience in digital forensics, and her passion for teaching is fueled by the ever-increasing presence of Mac devices in today’s digital forensic investigations. Sarah has worked with federal law enforcement agencies on a variety of high-profile investigations in such areas as computer intrusions, criminal cases, counter-intelligence, counter-narcotics, and counter-terrorism. Her research and analytical interests include Mac forensics, mobile device forensics, digital profiling, and malware reverse engineering.
This course covers how developers and security professionals can build and deliver secure software using DevOps and cloud services, specifically Amazon Web Services (AWS). It explains how principles, practices, and tools in DevOps and AWS can be leveraged to improve the reliability, integrity, and security of applications.

The first two days of the course cover how Secure DevOps can be implemented using lessons from successful DevOps security programs. Students build a secure DevOps CI/CD toolchain and understand how code is automatically built, tested, and deployed using popular open-source tools such as git, Puppet, Jenkins, and Docker. In a series of labs you learn to inject security into your CI/CD toolchain using various security tools, patterns, and techniques.

The final three days of the course cover how developers and security professionals can utilize AWS services to build secure software in the cloud. Students leverage the CI/CD toolchain to push application code directly to the cloud instead of to local servers on their class virtual machines. Students analyze and fix applications hosted in the cloud using AWS services and features such as API Gateway, IAM, signed cookies, Security Token Service, autoscaling, KMS, encryption, WAF, and Lambda for Serverless computing.

The course makes extensive use of open-source materials and tooling for automated configuration management (“Infrastructure as Code”), Continuous Integration, Continuous Delivery, Continuous Deployment, containerization, micro-segmentation, automated compliance (“Compliance as Code”), and Continuous Monitoring.

This course also makes extensive use of AWS and associated developer tools such as CloudFormation, CodeCommit, CodeBuild, CodePipeline, and other cloud application services so students can experience how these services can be utilized in their applications.

“I have a security background and interface with engineers/developers every day in my role, and I’m finding the course very useful.”

-Devika Y., Bloomberg

Mark Geeslin is a Senior Principal Software Engineer and Director of Application Security at Asurion. Mark has been working in the software development and security industries for over 25 years in many diverse environments, ranging from high-tech security start-ups to Fortune 100 companies. In recent years he has directed the application security programs at leading software technology firms in Silicon Valley. Besides his extensive experience as a software engineer, Mark’s expertise includes large-scale application security assessments, penetration testing, threat modeling and architectural risk analysis, static and dynamic software security analysis, secure code review, and security research. Mark has earned advanced degrees in both computer science and theology, and currently holds the GWAPT, GMOB, GSSP-Java, GSSP-.NET, and GSEC certifications.
Bonus Sessions

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 information security and get the most for your training dollar.

General Session – Welcome to SANS
David Hoelzer
Join us for a 30-minute overview to help you get the most out of your SANS training experience. You will receive event information and learn about programs and resources offered by SANS. This brief session will answer many questions and get your training off to a great start. This session will be valuable to all attendees but is highly recommended for first-time attendees.

KEYNOTE: OODA Security: Taking Back the Advantage
Kevin Fiscus
OODA, or Observe, Orient, Decide and Act, is a concept first developed for fighter pilots. The concept states that the adversary who can effectively complete the OODA cycle first will go home while the adversary who takes longer enjoys, at best, a long, slow parachute ride to the ground. This concept can be applied to information security. In theory, we defenders should have the advantage, as it is our “house” the attackers are attacking. Unfortunately, that is rarely the case. Over 50% of organizations find out they have been compromised via notification by a third party, meaning that all too often defenders don’t even start their OODA loop until after the attacker has completed the compromise. Making things worse, traditional security controls are failing us because attackers already know how to circumvent or evade them. Fortunately, there is a solution. By making better use of our existing technology and by using some of the attackers’ tools and techniques against them, we can deter, distract, delay, disrupt and detect them. Come learn how we can turn the tables on the bad guys and reclaim the OODA loop initiative.

Hunting Logic Attacks
Hassan El Hadary
One of the most challenging problems for developers these days is to develop secure applications. Development platforms have provided several techniques to protect against common attacks such as Cross-Site Scripting, SQL injection, and others. However, logic attacks are still the hardest to stop, as they are tricky and hard to discover. Logic attacks can enable an attacker to gain access to sensitive data or get control of unauthorized systems. In the era of IoT and complex applications, logic attacks will have a greater impact. In this talk, we will present several logic attack stories where attackers have broken developer defenses. All stories are inspired from findings discovered in real-life professional experiences and from bug bounty programs. Finally, we will discuss the future of such attacks and their impact on IoT systems.

No Seriously, I Can Still See You!
Jonathan Ham
Everything leaves footprints on the network, whether it’s a frontal assault on an Internet-facing SMB, or a lateral move living off the land with harvested creds. The Red Team only has the advantage up until the window breaks (I heard that!). Once you are in my house, I have the advantage (I know that squeaky floorboard!). Here’s what it looks like when you think you can steal my stuff. Obfuscate your Powershell 10x. Drop PEVs via DDE and Word macros. DLL inject mimikatz. Evade AV. Fine. But to be the man-in-the-middle, you have to mess with L2/L3, and to move laterally, you have to do things on L3/L4 that you shouldn’t do. And when you do, I can still see you.
Future Training Events
See www.sans.org for more information.

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.

Sonoma
Santa Rosa, CA
Jan 14-19, 2019

Miami
Miami, FL
Jan 21-26

Las Vegas
Las Vegas, NV
Jan 28 - Feb 2

Future Training Events
See www.sans.org for more information.

Sonoma
Santa Rosa, CA
Jan 14-19, 2019

Miami
Miami, FL
Jan 21-26

Las Vegas
Las Vegas, NV
Jan 28 - Feb 2

Security East
New Orleans, LA
Feb 2-9

Anaheim
Anaheim, CA
Feb 11-16

Northern VA Spring – Tysons
Vienna, VA
Feb 11-16

Dallas
Dallas, TX
Feb 18-23

New York Metro Winter
Jersey City, NJ
Feb 18-23

Scottsdale
Scottsdale, AZ
Feb 18-23

Reno Tahoe
Reno, NV
Feb 25 - Mar 2

Baltimore Spring
Baltimore, MD
Mar 2-9

San Francisco Spring
San Francisco, CA
Mar 11-16

St. Louis
St. Louis, MO
Mar 11-16

Norfolk
Norfolk, VA
Mar 18-23

SANS 2019
Orlando, FL
Apr 1-8

Boston Spring
Boston, MA
Apr 14-19

Seattle Spring
Seattle, WA
Apr 14-19

Northern VA – Alexandria
Alexandria, VA
Apr 23-28

Pen Test Austin
Austin, TX
Apr 29 - May 4

Kansas City
Kansas City, MO
Jun 10-15

SANSFIRE
Washington, DC
Jun 15-22

Rocky Mountain
Denver, CO
Jul 15-20

San Francisco Summer
San Francisco, CA
Jul 22-27

Future Summit Events

Cyber Threat Intelligence
Arlington, VA
Jan 21-28, 2019

Open-Source Intelligence
Alexandria, VA
Feb 25 - Mar 3

ICS Security
Orlando, FL
Mar 18-25

Blue Team
Louisville, KY
Apr 11-18

Cloud Security
San Jose, CA
Apr 29 - May 6

Security Operations
New Orleans, LA
Jun 24 - Jul 1
Register online at www.sans.org/san-francisco-spring
We recommend registering early to 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 server will accept your registration. Sold-out courses will be removed from the online registration. Everyone 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 February 20, 2019. 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.

Top 3 reasons to stay at the Hyatt Centric Fisherman’s Wharf San Francisco
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Hyatt Centric Fisherman’s Wharf San Francisco, you can 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 Hyatt Centric Fisherman’s Wharf San Francisco that you won’t want to miss!

Pay Early and Save*

Pay & enter code by

<table>
<thead>
<tr>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-16-19</td>
<td>$350</td>
<td>2-6-19</td>
<td>$200</td>
</tr>
</tbody>
</table>

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

NewsBites
Twice-weekly, high-level executive summaries of the news most 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 newly discovered attack vectors, vulnerabilities with active new exploits, how recent attacks worked, and other valuable data.

Webcasts

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

Analyst Webcasts
Analyst Webcasts share highlights and key results from our Analyst Program whitepapers and surveys.

WhatWorks Webcasts
The SANS WhatWorks webcasts share 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 (SANS.org account not required)

- 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 September 19th. Register today at www.sans.org/san-diego-fall

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.

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