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

INFORMATION SECURITY TRAINING

Minneapolis 2018
June 25-30

Protect Your Business | Advance Your Career
Eight hands-on, immersion-style courses taught by real-world practitioners

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

“SANS training is more comprehensive and in-depth than anything else I’ve found in the industry.” -Trevor Gibbons, Valspar

SAVE $400
Register and pay by May 2nd
Use code EarlyBird18

www.sans.org/minneapolis
SANS Instructors

Fewer than 100 individuals are currently qualified and designated to teach as SANS Instructors, globally. 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

The line-up of SANS Instructors for SANS Minneapolis includes:

- **Chris Christianson**
  - Certified Instructor
  - @ccchristianson

- **Adrien de Beaupre**
  - Certified Instructor
  - @adriendb

- **Kevin Fiscus**
  - Principal Instructor
  - @kevinbfiscus

- **Jonathan Ham**
  - Certified Instructor
  - @jhamcorp

- **David Mashburn**
  - Certified Instructor
  - @d_mashburn

- **Timothy McKenzie**
  - Instructor
  - @timboloman

- **Greg Porter**
  - Instructor

- **Eric Zimmerman**
  - Certified Instructor
  - @EricRZimmerman

**Evening Bonus Sessions**

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

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

**So, You Wanna Be a Pen Tester?** - Adrien de Beaupre

**Courses at a Glance**

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Days</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>MON 6-25</td>
<td>Page 2</td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>TUE 6-26</td>
<td>Page 3</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>WED 6-27</td>
<td>Page 4</td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td>THU 6-28</td>
<td>Page 5</td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td>FRI 6-29</td>
<td>Page 6</td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td>SAT 6-30</td>
<td>Page 7</td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>Page 8</td>
<td></td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td>Page 9</td>
<td></td>
</tr>
</tbody>
</table>
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 are made via a written document (short memo and/or a few PowerPoint slides) that justifies the need and benefit. Most managers will respect and value the effort.
• Provide all the necessary information in one place. In addition to your request, provide all the right context by including the summary pages on Why SANS?, the Training Roadmap, the instructor bio, and additional benefits available 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 for the decision.
• Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled “You Will Be Able To.” Be sure to include this in your request so that you 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.
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 all are 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, 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.

Chris Christianson is an information security consultant based in Northern California, with 20 years of experience and many technical certifications including the GSEC, GCIA, GREM, GPEN, GWAPT, GCCC, GSF, GCED, CISSP®, CCSE, CCDP, CNRP, IAM, CEH, and IEM. He holds a bachelor of science in management information systems from the University of Atlanta. Before starting his own information security consultant services, Chris worked at Travis Credit Union for 21 years. His last role there was as the Assistant Vice President in Atlanta. He is now the Information Technology Department. Chris has also been an invited expert speaker at conferences and has contributed to numerous industry articles.

"Excellent job this week in presenting all the modules in SEC401. Chris’s enthusiastic delivery approach was fantastic, and I learned a lot from him.” - Robert Chavez, CBN

Register at www.sans.org/minneapolis | 301-654-SANS (7267)
Jonathan is an independent consultant who specializes in large-scale enterprise security issues, from policy and procedure, through staffing and training, to scalable prevention, detection, and response technology and techniques. With a keen understanding of ROI and TCO (and an emphasis on process over products), he has helped his clients achieve greater success for over 20 years, advising in both the public and private sectors, from small start-ups 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 Cyber Incident Response Team for one of the largest U.S. civilian federal agencies. He has held the CISSP®, GSEC, GCIA, and GCIH certifications and is a member of the GIAC Advisory Board. A former combat medic, Jonathan still spends some of his time practicing a different kind of emergency response, volunteering and teaching for both the National Ski Patrol and the American Red Cross.
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.

“"This course gives attendees a view into the hacker mindset, insight into the findings that we receive from our external and application pen tests, and the tools that the security operations team members need to master to track and hunt hackers."" - Joshua Alderete, Oil States International

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, GCWN, GCPP, GSEC, SCSA, RCSE, 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.

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

Kevin Fiscus
SANS Principal Instructor
@kevinbfiscus
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!
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.

Timothy McKenzie has over 20 years of IT and information security experience working in financial, government, defense contractor, and service-related markets. Timothy has been trained in malware research and exploit development, expert penetration, and forensics work. Timothy works for Secureworks as a red team penetration tester, focused primarily on network and web-based attacks. He loves sharing the vast knowledge he has acquired to give back to the information security community.

“Tim did a spectacular job of relating the information provided with his own personal knowledge.”

-Julio C. Nunez, JPMorgan Chase & Co.
This course has extended hours

Network Penetration Testing and Ethical Hacking

As a cybersecurity professional, you have a unique responsibility to find and understand your organization’s vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this task head-on. SEC560 is the must-have course for every well-rounded security professional.

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step-by-step and end-to-end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, mapping out your scope and recon, then dives deep into scanning, target exploit, password attacks, and web app manipulation, with more than 30 detailed hands-on labs throughout. The course is chock-full of practical, real-world tips from some of the world’s best penetration testers to help you do your job safely, efficiently...and masterfully.

Learn the best ways to test your own systems before the bad guys attack.

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test – and on the last day of the course you’ll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You’ll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the knowledge you’ve mastered in this course.

You will bring comprehensive penetration testing and ethical hacking know-how back to your organization.

You will learn how to perform detailed reconnaissance, studying a target’s infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won’t just cover run-of-the-mill options and configurations, we’ll also go over the lesser known but super-useful capabilities of the best pen test toolsets available today. After scanning, you’ll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You’ll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.

Six-Day Program
Mon, June 25 - Sat, June 30
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor:
Adrien de Beaupre

Who Should Attend
- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red and blue team members
- Forensics specialists who want to better understand offensive tactics

"SEC560 provides practical, how-to material that I can use daily in my penetration testing activities – not only technically, but also from a business perspective."
- Steve Nolan, General Dynamics

This course is available via Simulcast. See page 13 for more information

Bundle OnDemand with this course

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/minneapolis-2018/courses
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 organization in order to improve its cyber defence.”

SANS’s 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.

“Implementing and Auditing the Critical Security Controls – In-Depth”

Five-Day Program
Mon, June 25 - Fri, June 29
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Greg Porter

Who Should Attend
- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Staff and clients of federal agencies
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MG512

Bundle OnDemand with this course

“SEC566 gave me not only the knowledge but the tools to be successful.”
- Carla Raisler, HealthTech Solutions

Greg Porter
SANS Instructor

Greg Porter has both led and delivered comprehensive assessment activities that monitor, test, and audit the effectiveness of information system security controls. For the past several years, he has assisted organizations across the health care spectrum, ranging from integrated health care providers and community hospitals to biotech and pharmaceutical organizations. Greg is also the founder of Allegheny Digital, an information security consultancy specializing in enterprise risk management, incident response, and threat monitoring. Greg graduated from the University of Pittsburgh, received his master’s degrees from Carnegie Mellon University, and holds a number of professional certifications.
FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting will help you to:

- Detect how and when a breach occurred
- Identify compromised and affected systems
- Determine what attackers took 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.

This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and hactivism. Constantly updated, FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting 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!

Six-Day Program
Mon, June 25 – Sat, June 30
9:00am – 5:00pm
36 CPEs
Laptop Required
Instructor: Eric Zimmerman

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

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 took 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 these children. As a result, in May 2012, Eric was given a National Center for Missing and Exploited Children’s 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. Eric’s teaching philosophy focuses on the long-term gains achieved by not only understanding the nuts and bolts of how to run a tool and consume output, but also getting a deeper understanding of how tools work “under the hood.” His 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
@EricRZimmerman

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/minneapolis-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: 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 attackers. Come learn how we can turn the tables on the bad guys and reclaim the OODA loop initiative.

**So, You Wanna Be a Pen Tester?**

Adrien de Beaupre

This presentation will discuss the things that you will actually need to become a penetration tester. Be prepared for a no-fluff honest discussion. You will need attitude, aptitude, initiative, desire, dedication, discipline, integrity, ethics, experience, knowledge, and tools.

---

**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 computer security, and get the most for your training dollar.

**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 attackers. Come learn how we can turn the tables on the bad guys and reclaim the OODA loop initiative.

**So, You Wanna Be a Pen Tester?**

Adrien de Beaupre

This presentation will discuss the things that you will actually need to become a penetration tester. Be prepared for a no-fluff honest discussion. You will need attitude, aptitude, initiative, desire, dedication, discipline, integrity, ethics, experience, knowledge, and tools.
Future Training Events

Pre-RSA® Conference Training
San Francisco, CA  Apr 11-16
Baltimore Spring
Baltimore, MD  Apr 21-28
Seattle Spring
Seattle, WA  Apr 23-28

Security West
San Diego, CA  May 11-18
Northern VA Reston Spring
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

Future Summit Events

Blue Team
Louisville, KY  Apr 23-30
Automotive Cybersecurity
Chicago, IL  May 1-8
DFIR
Austin, TX  Jun 7-14
Security Operations
New Orleans, LA  Jul 30 - Aug 6
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

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.
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 June 6, 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*
Pay & enter code by
DATE DISCOUNT DATE DISCOUNT
5-2-18 $400.00 5-23-18 $200.00

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

Millennium Hotel Minneapolis
1313 Nicollet Mall
Minneapolis, MN 55403
612-332-6000
www.sans.org/event/minneapolis-2018/location

Situated along the tree-lined streets of Nicollet Mall, Millennium Minneapolis is the closest full-service hotel to the Minneapolis Convention Center and is also moments away from the city’s cultural districts. The 321 guest rooms and suites combine contemporary elegance with a residential feel and feature stunning views. Come stay, and experience the delights of the Twin Cities.

Special Hotel Rates Available
A special discounted rate of $183.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through May 27, 2018.

Top 3 reasons to stay at the Millennium Hotel Minneapolis
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Millennium Hotel Minneapolis, 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 Millennium Hotel Minneapolis that you won’t want to miss!

Registration Information
Register online at www.sans.org/minneapolis
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.

SANS Simulcast
To register for a SANS Minneapolis 2018 Simulcast course, please visit www.sans.org/event/minneapolis-2018/attend-remotely

Pay Early and Save*
Use code EarlyBird18 when registering early

SANS Voucher Program
Expand your training budget!

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 June 6, 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.

Special Hotel Rates Available
A special discounted rate of $183.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through May 27, 2018.

Top 3 reasons to stay at the Millennium Hotel Minneapolis
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Millennium Hotel Minneapolis, 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 Millennium Hotel Minneapolis that you won’t want to miss!

Registration Information
Register online at www.sans.org/minneapolis
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.

SANS Simulcast
To register for a SANS Minneapolis 2018 Simulcast course, please visit www.sans.org/event/minneapolis-2018/attend-remotely

Pay Early and Save*
Use code EarlyBird18 when registering early

SANS Voucher Program
Expand your training budget!

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 June 6, 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.
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 portal 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 December 27th. www.sans.org/dallas

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.