INFORMATION SECURITY TRAINING

Las Vegas 2019
Jan 28 – Feb 2

Protect Your Business | Advance Your Career

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

See inside for courses and GIAC certifications in:

- Cyber Defense
- Penetration Testing
- Ethical Hacking
- CISSP® Preparation
- Secure Development
- ICS/SCADA Security

PLUS NEW COURSES
- Enterprise Threat and Vulnerability Assessment
- Defensible Security Architecture

“SANS offers great information security training that gives users actionable items to implement when they are done.”

-Jeff Murray, Campbell Scientific

SAVE $350
Register and pay by Dec 5th
Use code EarlyBird19

www.sans.org/las-vegas
Learn up-to-the-minute cybersecurity techniques at SANS Las Vegas 2019. As threats change constantly and attacks become more aggressive, it is crucial to arm yourself with actionable information you can use to protect your environment. SANS provides relevant and practical training you can implement the day you return to work. 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 instructors are industry professionals who will ensure you not only learn the material, but will be able to apply what you learn your first day back in the office. Our outstanding course material and unparalleled instructors make SANS the best choice in information security education. Register today!

### Courses at a Glance

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td>Introduction to Cyber Security</td>
<td>Page 2</td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>Page 3</td>
</tr>
<tr>
<td>SEC460</td>
<td>Enterprise Threat and Vulnerability Assessment NEW!</td>
<td>Page 4</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>Page 5</td>
</tr>
<tr>
<td>SEC530</td>
<td>Defensible Security Architecture NEW!</td>
<td>Page 6</td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td>Page 7</td>
</tr>
<tr>
<td>SEC599</td>
<td>Defeating Advanced Adversaries – Purple Team Tactics &amp; Kill Chain Defenses</td>
<td>Page 8</td>
</tr>
<tr>
<td>MGT414</td>
<td>SANS Training Program for CISSP® Certification</td>
<td>Page 9</td>
</tr>
<tr>
<td>DEV540</td>
<td>Secure DevOps and Cloud Application Security</td>
<td>Page 10</td>
</tr>
<tr>
<td>ICS410</td>
<td>ICS/SCADA Security Essentials</td>
<td>Page 11</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 12.

**KEYNOTE: An Interactive Look at Software Exploitation and Today’s Threat Landscape** – Stephen Sims

**Stuck in the Box, a SIEM’s Tale** – Justin Henderson

**Zero Trust Architecture** – Justin Henderson

**Danger Stewards: Measuring Risk and Predicting the Future for Fun and Profit** – Doc Blackburn

Save $350 when you register and pay by Dec 5th using code EarlyBird19
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 – $769

“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 – $769

“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.
To determine if SANS SEC301: Introduction to Cyber Security is right for you, ask yourself five simple questions:

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

If you answer yes to any of these questions, then the SEC301: Introduction to Cyber Security training course is for you. Students with a basic knowledge of computers and technology but no prior cybersecurity experience can jump-start their security education with insight and instruction from real-world security experts in SEC301. This completely revised and comprehensive five-day course covers a wide range of baseline topics, including terminology, the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles. The hands-on, step-by-step learning format will enable you to grasp all the information presented even if some of the topics are new to you. You’ll learn fundamentals of cybersecurity that will serve as the foundation of your security skills and knowledge for years to come.

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

“The course provided me with a lot of great information from the low to the high levels in several areas. A lot of the concepts are something I will be able to use in my day-to-day job.”

- Sandy Baguskas, John Hancock

Doc Blackburn has more than 30 years of experience in system and software design, server and network administration, security, and website programming. Doc ran an IT consulting, hosting and design firm for 12 years, and also gained vast experience at various levels of information technology in other roles ranging from technical support to security leadership. He has been involved in the technical design and implementation of NIH-approved and FISMA-compliant information systems. His current work focuses on HIPAA, FERPA, PCI DSS, and FISMA-compliant systems with an emphasis on IT risk management in enterprise environments. Doc holds the ITIL, CISSP®, HCISPP (health care, HIPAA), PCI ISA (payment and card industry), and the GIAC GDF, GSEC, GOPEN, GCiP, GCIA, AND GSLC certifications. He has a bachelor’s degree from the University of Arizona and is currently the IT compliance administrator for the University of Colorado Denver, Anschutz Medical Campus.
For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/las-vegas-2019/courses

@Steph3nSims
SANS Faculty Fellow

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

Laptop Required

Who Should Attend
- 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.

Six-Day Program
Mon, Jan 28 - Sat, Feb 2
This course has extended bootcamp hours
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant performing reverse engineering, exploit development, threat modeling, and penetration testing. Stephen has a MS in information assurance from Norwich University. He is the author of SANS’s only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP®, CISA, Immunity NOP, and many other certifications. In his spare time Stephen enjoys snowboarding and writing music.

Stephen Sims
SANS Faculty Fellow
@Steph3nSims

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/las-vegas-2019/courses

3
Computer exploitation is on the rise. As advanced adversaries become more numerous, more capable, and much more destructive, organizations must become more effective at mitigating their information security risks at the enterprise scale. SEC460 is the premier course focused on building technical vulnerability assessment skills and techniques, while highlighting time-tested practical approaches to ensure true value across the enterprise. The course covers threat management, introduces the core components of comprehensive vulnerability assessment, and provides the hands-on instruction necessary to produce a vigorous defensive strategy from day one. The course is focused on equipping information security personnel from organizations charged with effectively and efficiently securing 10,000 or more systems.

SEC460 begins with an introduction to information security vulnerability assessment fundamentals, followed by in-depth coverage of the Vulnerability Assessment Framework. It then moves into the structural components of a dynamic and iterative information security program. Through a detailed, practical analysis of threat intelligence, modeling, and automation, students will learn the skills necessary to not only use the tools of the trade, but also to implement a transformational security vulnerability assessment program.

SEC460 will teach you how to use real industry-standard security tools for vulnerability assessment, management, and mitigation. It is the only course that teaches a holistic vulnerability assessment methodology while focusing on challenges faced in a large enterprise. You will learn on a full-scale enterprise range chock full of target machines representative of an enterprise environment, leveraging production-ready tools, and a proven testing methodology.

This course takes you beyond the checklist, giving you a tour of the attackers’ perspective that is crucial to discovering where they will strike. Operators are more than the scanner they employ. SEC460 emphasizes this personnel-centric approach by examining the shortfalls of many vulnerability assessment programs in order to provide you with the tactics and techniques required to secure networks against even the most advanced intrusions.

We wrap up the first five days of instruction with a discussion of triage, remediation, and reporting before putting your skills to the test on the final day against an enterprise-grade cyber range with numerous target systems for you to analyze and explore. The cyber range is a large environment of servers, end-users, and networking gear that represents many of the systems and topologies used by enterprises. By adopting an end-to-end approach to vulnerability assessment, you can be confident that your skills will provide much-needed value in securing your medium- or large-scale organization.

Who Should Attend
- Vulnerability assessors
- IT System administrators
- Security auditors
- Compliance professionals
- Penetration testers
- Vulnerability program managers
- Security analysts
- Security architects
- Senior security engineers
- Technical security managers

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.

Adrien de Beaupre
SANS Certified Instructor
@adriendb

"SEC460 has provided me the knowledge to build a great vulnerability management/vulnerability assessment program that vendor courses couldn't provide."
- Eric Osmus,
ConocoPhillips Company
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

Matt Edmondson
SANS Certified Instructor
@matt0177

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. A recognized expert in his field with a knack for communicating complicated technical issues to non-technical personnel, Matt routinely provides cybersecurity instruction to individuals from the Department of Defense, Department of Justice, Department of Homeland Security, Department of Interior, and other agencies, and has spoken frequently at information security conferences and meetings. Matt is a member of the SANS Advisory Board and holds 11 GIAC certifications, including the GREM, GCFA, OPEN, GCIH, GWAPT, GMOB and GCIA. In addition, Matt holds the Offensive Security Certified Professional (OSCP) certification.
Architecture is designed to help students build and maintain a truly defensible security architecture. “The perimeter is dead” is a favorite saying in this age of mobile, cloud, and the Internet of Things. We are indeed living in a new world of “de-perimeterization” where the old boundaries of “inside” and “outside” or “trusted” and “untrusted” no longer apply.

This changing landscape requires a change in mindset, as well as a repurposing of many devices. Where does it leave our classic perimeter devices such as firewalls? What are the ramifications of the “encrypt everything” mindset for devices such as Network Intrusion Detection Systems?

In this course, students will learn the fundamentals of how to build and maintain up-to-date defensible security architecture. There will be a heavy focus on leveraging current infrastructure (and investment), including switches, routers, and firewalls. Students will learn how to reconfigure these devices to better prevent the threat landscape they face today. The course will also suggest newer technologies that will aid in building a robust security infrastructure.

While this is not a monitoring course, it will dovetail nicely with continuous security monitoring, ensuring that security architecture not only supports prevention, but also provides the critical logs that can be fed into a Security Information and Event Management (SIEM) system in a Security Operations Center.

Hands-on labs will reinforce key points in the course and provide actionable skills that students will be able to leverage as soon as they return to work.

You Will Learn To:

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Maximize the current investment by reconfiguring existing equipment to become more defensible
- Configure computer systems and network components to support proper logging and continuous monitoring
- Improve both preventive and detective capabilities
- Improve the security of devices from layer 1 (physical) through layer 7 (application)

Justin Henderson is a passionate and dedicated information technology professional who has been in the field since 2005. Justin focuses on providing comprehensive industry training and uses his knowledge and experience to mentor others. Justin is particularly proficient in working with technical platforms, including operating systems, networking, security, storage, and virtualization, but he has also worked in governance, project management, and service management. He has a BS degree in network design and administration from Western Governors University and has over 40 certifications, including the GPEN and GCWN. Justin has also taught network security at Lake Land College. Some of his other achievements include mentoring individuals in the information technology field as well as developing the virtual dojo, a fully automated cloud computing solution showcase environment.

SEC530: Defensible Security Architecture NEW!

“SEC530 covers defense techniques layer by layer – extremely valuable!”
- Steve Turner, Prudential

Six-Day Program
Mon, Jan 28 - Sat, Feb 2
9:00am - 5:00pm
36 CPEs
Laptop Required

Who Should Attend
- Security architects
- Network engineers
- Network architects
- Security analysts
- Senior security engineers
- System administrators
- Technical security managers
- CND analysts
- Security monitoring specialists
- Cyber threat investigators

Justin Henderson
SANS Certified Instructor
@SecurityMapper

Register at www.sans.org/las-vegas | 301-654-SANS (7267)
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 El Hadary
SANS Instructor
@hassan_hadary

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

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/las-vegas-2019/courses
You just got hired to help our virtual organization “SyncTechLabs” build out a cybersecurity capability. On your first day, your manager tells you: "We looked at some recent cybersecurity trend reports and we feel like we’ve lost the plot. Advanced persistent threats, ransomware, denial of service...We’re not even sure where to start!"

Cyber threats are on the rise: ransomware is affecting small, medium and large enterprises alike, while state-sponsored adversaries are attempting to obtain access to your most precious crown jewels. SEC599: Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses will provide an in-depth understanding of how current adversaries operate and arm you with the knowledge and expertise you need to detect and respond to today’s threats.

SEC599 aims to leverage the purple team concept by bringing together red and blue teams for maximum effect. Recognizing that a prevent-only strategy is not sufficient, the course focuses on current attack strategies and how they can be effectively mitigated and detected using a Kill Chain structure. Throughout the course, the purple team principle will be maintained, where attack techniques are first explained in-depth, after which effective security controls are introduced and implemented.

Course authors Erik Van Buggenhout and Stephen Sims (both certified as GIAC Security Experts) are hands-on practitioners who have achieved a deep understanding of how cyber attacks work through penetration testing and incident response. While teaching penetration testing courses, they were often asked “But how do I prevent this type of attack?” With more than 20 labs plus a full-day defend-the-flag exercise during which students attempt to defend our virtual organization from different waves of attacks against its environment, SEC599 gives students real-world examples of how to prevent attacks.

Our six-day journey will start with an analysis of recent attacks through in-depth case studies. We will explain what types of attacks are occurring and introduce the Advanced Persistent Threat (APT) Attack Cycle as a structured approach to describing attacks. In order to understand how attacks work, students will also compromise our virtual organization “SyncTechLabs” in our Day 1 exercises.

Throughout days 2 through 5 we will discuss how effective security controls can be implemented to prevent, detect, and respond to cyber attacks. Some of the topics we will address include:

- How red and blue teams can improve collaboration, forming a true purple team
- How current advanced adversaries are breaching our defenses
- Security controls structured around the Kill Chain

In designing the course and its exercises, the authors went the extra mile to ensure that attendees “build” something that can be used later on. For this reason, the different technologies illustrated throughout the course (e.g., IDS systems, web proxies, sandboxes, visualization dashboards, etc.) will be provided as usable virtual machines on the course USB.

SEC599 will finish with a bang. During the Defend-the-Flag challenge on the final course day, you will be pitted against advanced adversaries in an attempt to keep your network secure. Can you protect the environment against the different waves of attacks? The adversaries aren’t slowing down, so what are you waiting for?

James Shewmaker is the founder of and principal consultant at Bluenotch Corporation in Long Beach, California, which provides customized security services focusing on investigations, penetration testing, and analysis. James authored and maintains the post-exploitation content in the SANS Security 660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking course. Before becoming a SANS Certified Instructor in 2009, his creative technical work led him on many adventures, including “The Great Translator Invasion of 2003.” James led the development and operations for NetWars as a U.S. Cyber Challenge game in June 2009. He is currently developing an independent cyber challenge, Bunker01, and is involved in the U.S. Cyber Challenge as an instructor at Cyber Camps. James regularly teaches a Tactical Offense and Defense day at these events.
David R. Miller has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on information systems security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security programs. He serves as a security lead and forensic investigator on numerous enterprise-wide IT design and implementation projects for Fortune 500 companies, providing compliance, security, technology, and architectural recommendations and guidance. Projects David has worked on include Microsoft Windows Active Directory enterprise designs, security information and event management systems, intrusion detection and protection systems, endpoint protection systems, patch management systems, configuration monitoring systems, and enterprise data encryption for data at rest, in transit, in use, and within email systems. David is an author, lecturer and technical editor of books, curriculum, certification exams, and computer-based training videos.

Who Should Attend

- Security professionals who are interested in understanding the concepts covered on the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of information security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® eight domains
- Security professionals and managers looking for practical ways the eight domains of knowledge can be applied to their current job

After completing the course students will have:

- Detailed coverage of the eight domains of knowledge
- The analytical skills required to pass the CISSP® exam
- The technical skills required to understand each question
- The foundational information needed to become a Certified Information Systems Security Professional (CISSP®)

External Product Notice:

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

“This training was a comprehensive overview of all topics covered in the CISSP® exam. All in attendance were there for a common goal, including the instructor. It was easy to follow, and the real-world examples given were priceless.”
- Ron Pinnock, Navy Exchange Service Command

“I am new in the domain and this course was the perfect opening – clear explanations, covering all the areas, presenting real-life examples, and great material to support the learning.”
- Sorana Costache, Ubisoft

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/las-vegas-2019/courses
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

Eric Johnson is a Principal Security Consultant at Cypress Data Defense, where he leads secure software development lifecycle consulting, web and mobile application penetration testing, secure code review assessments, static source code analysis, security research, and security tools development. He also founded the Puma Scan static analysis open-source project, which allows software engineers to run security-focused .NET static analysis rules during development and in continuous integration pipelines. At the SANS Institute, Eric authors application security courses on DevOps, cloud security, secure coding, and defending mobile apps. He serves on the advisory board for the SANS Securing the Human Developer awareness training program, delivers security training around the world, and has presented his security research at conferences including BlackHat, OWASP, BSides, JavaOne, UberConf, and ISSA. Eric completed a bachelor of science degree in computer engineering and a master of science degree in information assurance at Iowa State University, and currently holds the CISSP®, GWAPT, GSSP-.NET, and GSSP-Java certifications. He is based in West Des Moines, Iowa and outside the office enjoys spending time with his family, attending Iowa State athletic events, and playing golf.
SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. ICS410: ICS/SCADA Security Essentials provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems (ICS) is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with:

- An understanding of ICS components, purposes, deployments, significant drivers, and constraints
- Hands-on lab learning experiences about control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as ICS penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems. With the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. For their part, IT support personnel who provide the communications paths and network defenses do not always grasp the systems’ operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle.

When these different groups of professionals complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their ICS environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

Five-Day Program
Mon, Jan 28 - Fri, Feb 1
9:00am - 5:00pm
30 CPEs
Laptop Required

Who Should Attend
The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

“It was very beneficial to have members of the OT and IT world in the same room trying to understand the complexities of each of our responsibilities.”
- Elise Bergandino, Lockheed Martin

Stephen Mathezer has had hands-on experience since the early days of the Internet. He has a broad perspective and experience with technology in the real world, having written network software for a very small company while also supporting customers in the Fortune 500. He later spent 15 years working for a large oil and gas company, beginning as a member of the network and operational security teams and eventually managing a team of 25 responsible for security architecture, security operations, industrial control system security operations, and technical security. He has also consulted for a wide variety of companies, providing managed security services and security assessments. Stephen has recently joined ION Secured Networks as a director, allowing him to better focus on his passion for network security. He currently holds the GSEC, GICSP, GCIH, GCFA, GWAPT, GAWN, and GXPN certifications.
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: An Interactive Look at Software Exploitation and Today’s Threat Landscape
Stephen Sims
Let’s take a journey through the most common attack trends and techniques used today by adversaries as well as by security researchers looking to profit from exploit sales and bug bounties. Security researchers, adversaries, and various players between the two closely monitor the landscape for changes, actively respond to these changes, and remain one step ahead of our efforts to maintain an acceptable level of security. It is critical for our defenders to keep up with these forever-changing techniques. Surprisingly, the success of cyber-criminals often depends on basic mistakes still made by users, combined with poor patch management and the failure to use proper exploit mitigations. Join Stephen as he performs several demonstrations exploiting both publicly disclosed and privately disclosed vulnerabilities involving various well-known applications. This presentation will weave in and out of high-level definitions and concepts, all the way to advanced demonstrations and reverse engineering.

Stuck in the Box, a SIEM’s Tale
Justin Henderson
Organizations often spend excessive amounts of money on SIEM products only to end up with a log collection box when they thought they purchased a tactical detection system. Most organizations find themselves with a SIEM but unsure how to use its capabilities. Point solutions are quick to defend deficiencies by stating each environment is different, so you, the customer, must tell them what you want the SIEM to do and then they’ll help you by providing professional services or by replacing your current SIEM with something “better and more advanced.” This is hogwash. Organizations tend to have a lot of overlap, be it the use of Windows systems or network protocols such as DNS. As such, there are high-fidelity detects that can be implemented in every organization.

Enough is enough. If you are looking for techniques and methods to get value out of your current SIEM or are interested in seeing how a new open-source big data solution such as the Elastic Stack (formerly ELK) most likely can beat what you have today, then this talk is for you. It is time to think outside the box. Come find out how one organization spent 14 months deploying a top magic quadrant SIEM solution only to have it beaten by ELK in two weeks.

Zero Trust Architecture
Justin Henderson
Perimeter security and other architecture models continue to fail us. The truth is that users and systems continue to accumulate access over time, and the inside of a network tends to be wide open for the picking. Instead of designing defenses around an outdated architecture, come and learn about zero trust architecture. Zero trust allows you to stray away from the old saying of “trust but verify” and instead switch to a “verify all” approach. No budget, no worries. This presentation focuses on implementing zero trust with systems and software you already own. What can we say, blue team is awesome!

Danger Stewards: Measuring Risk and Predicting the Future for Fun and Profit
Doc Blackburn
Are you having trouble convincing the decision-makers in your business to support security initiatives? Are your concerns being ignored? You are not alone! One of the biggest challenges that InfoSec professionals face today is getting leadership to support their activities. There have been many recent cases of security not getting enough resources until after a breach. Unfortunately, many times the security team is shown the door after the breach because it was considered their fault. Don’t let this happen to you. You know what to do, and how to do it. You know how important it is to your organization. The technology exists to fix your concerns. So, why won’t leadership fund it? Find out how to gain support for your activities and receive the support your security initiatives need.
Register online at www.sans.org/las-vegas

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 January 9, 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.

**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**

<table>
<thead>
<tr>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-5-18</td>
<td>$350</td>
<td>12-26-18</td>
<td>$200</td>
</tr>
</tbody>
</table>

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

---

**SANS Las Vegas returns to Planet Hollywood in January 2019.**

**Top 3 reasons to stay at the Planet Hollywood**

1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Planet Hollywood, 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 Planet Hollywood that you won’t want to miss!

**Special Hotel Rates Available**

A special discounted rate of $98 plus a daily reduced resort fee of $10 plus applicable taxes will be honored based on space availability.

The $10 resort fee includes unlimited local phone calls, fitness center access, and in-room Internet access for up to two devices. The group rate is lower than the 2018 government per diem rate. GSA has yet to release 2019 rates. These rates are only available through January 3, 2019.

**Hotel Information**

**Planet Hollywood**

3667 Las Vegas Boulevard South

Las Vegas, NV 89109

866-919-7472

www.sans.org/event/las-vegas-2019/location

SANS Las Vegas returns to Planet Hollywood in January 2019. Planet Hollywood’s all-new sleeping rooms give off a contemporary feel with edgy artwork and modern furnishings to ensure a comfortable stay. Dine like a movie star and look out for your favorite celebrities at one of the many Planet Hollywood restaurants.

**Registration Information**

Register online at www.sans.org/las-vegas

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.

**Pay Early and Save**

Use code EarlyBird19 when registering early

<table>
<thead>
<tr>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-5-18</td>
<td>$350</td>
<td>12-26-18</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

**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 January 9, 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.
Join the SANS.org community today to enjoy these free resources at www.sans.org/join

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.