CYBERSECURITY TRAINING
California 2019

San Francisco Summer  July 22-27
San Jose       Aug 12-27
San Francisco Fall  Sep 23-28
San Diego     Oct 7-12
Santa Monica  Oct 21-26

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

www.sans.org/california
Courses at a Glance

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Page</th>
<th>GIAC Cert</th>
<th>OnDemand Bundle</th>
<th>Meets DoDD 8140 (8570) Requirements</th>
<th>San Francisco Summer</th>
<th>San Jose Fall</th>
<th>San Francisco Fall</th>
<th>San Diego Fall</th>
<th>Santa Monica Fall</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td>Introduction to Cyber Security</td>
<td>13</td>
<td>GISF</td>
<td></td>
<td></td>
<td>SEC301</td>
<td></td>
<td></td>
<td>SEC301</td>
<td></td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>14</td>
<td>GSEC</td>
<td></td>
<td></td>
<td>SEC401</td>
<td>SEC401</td>
<td>SEC401</td>
<td>SEC401</td>
<td></td>
</tr>
<tr>
<td>SEC460</td>
<td>Enterprise Threat and Vulnerability Assessment</td>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td>SEC460</td>
<td></td>
<td></td>
<td>SEC460</td>
<td></td>
</tr>
<tr>
<td>SEC487</td>
<td>Open-Source Intelligence (OSINT) Gathering and Analysis</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td>SEC487</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>18</td>
<td>GCIA</td>
<td></td>
<td></td>
<td>SEC503</td>
<td></td>
<td></td>
<td></td>
<td>SEC503</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits &amp; Incident Handling</td>
<td>19</td>
<td>GCIH</td>
<td></td>
<td></td>
<td>SEC504</td>
<td></td>
<td></td>
<td></td>
<td>SEC504</td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td>20</td>
<td>GMON</td>
<td></td>
<td></td>
<td>SEC511</td>
<td></td>
<td></td>
<td></td>
<td>SEC511</td>
</tr>
<tr>
<td>SEC530</td>
<td>Defensible Security Architecture and Engineering</td>
<td>21</td>
<td>GDSA</td>
<td></td>
<td></td>
<td>SEC530</td>
<td></td>
<td></td>
<td></td>
<td>SEC530</td>
</tr>
<tr>
<td>SEC540</td>
<td>Cloud Security and DevOps Automation</td>
<td>22</td>
<td></td>
<td></td>
<td></td>
<td>SEC540</td>
<td>SEC540</td>
<td>SEC540</td>
<td>SEC540</td>
<td></td>
</tr>
<tr>
<td>SEC545</td>
<td>Cloud Security Architecture and Operations</td>
<td>23</td>
<td></td>
<td></td>
<td></td>
<td>SEC545</td>
<td></td>
<td></td>
<td></td>
<td>SEC545</td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics</td>
<td>24</td>
<td>GCDA</td>
<td></td>
<td></td>
<td>SEC555</td>
<td></td>
<td></td>
<td></td>
<td>SEC555</td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td>25</td>
<td>GPEN</td>
<td></td>
<td></td>
<td>SEC560</td>
<td></td>
<td></td>
<td></td>
<td>SEC560</td>
</tr>
<tr>
<td>SEC575</td>
<td>Mobile Device Security and Ethical Hacking</td>
<td>26</td>
<td>GMOB</td>
<td></td>
<td></td>
<td>SEC575</td>
<td></td>
<td></td>
<td></td>
<td>SEC575</td>
</tr>
<tr>
<td>SEC599</td>
<td>Defeating Advanced Adversaries – Purple Team Tactics &amp; Kill Chain Defenses</td>
<td>27</td>
<td>GDAT</td>
<td></td>
<td></td>
<td>SEC599</td>
<td>SEC599</td>
<td>SEC599</td>
<td>SEC599</td>
<td></td>
</tr>
<tr>
<td>SEC642</td>
<td>Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques</td>
<td>28</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SEC642</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC660</td>
<td>Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
<td>29</td>
<td>GXPN</td>
<td></td>
<td></td>
<td>SEC660</td>
<td></td>
<td></td>
<td></td>
<td>SEC660</td>
</tr>
<tr>
<td>FOR500</td>
<td>Windows Forensic Analysis</td>
<td>30</td>
<td>GCFE</td>
<td></td>
<td></td>
<td>FOR500</td>
<td>FOR500</td>
<td>FOR500</td>
<td></td>
<td>FOR500</td>
</tr>
<tr>
<td>FOR518</td>
<td>Mac and iOS Forensic Analysis and Incident Response</td>
<td>31</td>
<td></td>
<td></td>
<td></td>
<td>FOR518</td>
<td></td>
<td></td>
<td></td>
<td>FOR518</td>
</tr>
<tr>
<td>FOR572</td>
<td>Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response</td>
<td>32</td>
<td>GNFA</td>
<td></td>
<td></td>
<td>FOR572</td>
<td></td>
<td></td>
<td></td>
<td>FOR572</td>
</tr>
<tr>
<td>MGT414</td>
<td>SANS Training Program for CISSP® Certification</td>
<td>33</td>
<td>GISP</td>
<td></td>
<td></td>
<td>MGT414</td>
<td></td>
<td></td>
<td></td>
<td>MGT414</td>
</tr>
<tr>
<td>MGT512</td>
<td>Security Leadership Essentials for Managers</td>
<td>34</td>
<td>GSLC</td>
<td></td>
<td></td>
<td>MGT512</td>
<td></td>
<td></td>
<td></td>
<td>MGT512</td>
</tr>
<tr>
<td>MGT514</td>
<td>Security Strategic Planning, Policy, and Leadership</td>
<td>35</td>
<td>GSTRT</td>
<td></td>
<td></td>
<td>MGT514</td>
<td></td>
<td></td>
<td></td>
<td>MGT514</td>
</tr>
<tr>
<td>ICS410</td>
<td>ICS/SCADA Security Essentials</td>
<td>36</td>
<td>GICSP</td>
<td></td>
<td></td>
<td>ICS410</td>
<td></td>
<td></td>
<td></td>
<td>ICS410</td>
</tr>
<tr>
<td>ICS456</td>
<td>Essentials for NERC Critical Infrastructure Protection</td>
<td>37</td>
<td>GICP</td>
<td></td>
<td></td>
<td>ICS456</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Courses are subject to change. Please visit [www.sans.org](http://www.sans.org) for the most up-to-date information.
At the SANS Institute, our mission is to deliver the cutting-edge information security knowledge and skills that companies, military organizations, and governments need to protect their people and assets.

TRAINING ON THE CUTTING EDGE
SANS offers more than 65 unique courses, all designed to align with dominant security team roles, duties, and disciplines. Our courses prepare students to face today’s threats and tomorrow’s challenges. The SANS curriculum spans the full range of cybersecurity fields, including Cyber Defense, Penetration Testing & Ethical Hacking, Digital Forensics & Incident Response, Threat Hunting, Audit, Management, Critical Infrastructure and Control Systems Security, Secure Software Development, and more.

In SANS courses, students are immersed in hands-on lab exercises designed to help them practice, hone, and perfect what they’ve learned. We constantly update and rewrite our courses to ensure that the tools and techniques we’re teaching are always current and on the cutting edge.

LEARN FROM THE BEST
The SANS faculty is simply unmatched. All of our instructors are active security practitioners who bring their extensive knowledge and real-world experiences directly to the classroom. SANS instructors work for high-profile organizations as red team leaders, CISOs, technical directors, and research fellows. In addition to their respected technical credentials, they’re also expert teachers. Their passion for the topics they teach shines through, making the SANS classroom—both live and online—dynamic and effective.

RECOGNIZED AS A SUPERIOR INVESTMENT
Information security professionals from every member of the Fortune 100, and from small and mid-sized firms alike, say they return to SANS training again and again because they trust their training will result in practical and high-quality capabilities. SANS training is also embedded in government and military programs in the United States and its allies around the world for the same reason.

Customer feedback drives our continuous effort to maintain the quality and impact of SANS training so that we continue to deserve your trust.

GIAC SKILLS VALIDATION
GIAC certifications are designed to ensure that students can apply their knowledge and skills in a real-world setting. More than 30 certifications align with SANS training courses, validating student mastery for professional use in critical, specialized InfoSec domains and job-specific roles. See www.giac.org for more information.

A TRAINING FORMAT FOR EVERY STUDENT
SANS holds more than 300 live training events around the world each year, so you can find a convenient time and place to take your course. These events provide an engaging learning environment and multiple opportunities to network with other security professionals and with SANS instructors and staff. SANS training is also offered online, with several convenient options to suit your learning style. All of our online courses include at least four months of access to the course material, so students can revisit and rewind content anytime, anywhere.

THE SANS PROMISE
At the heart of everything we do is the SANS Promise: Students will be able to use their new skills as soon as they return to work.

REGISTER FOR SANS TRAINING
Learn more about SANS courses, and register online, at www.sans.org.

The SANS suite of education resources for information security professionals includes:
At SANS, our course authors and instructors are renowned cybersecurity experts who share their knowledge through their own real-world examples and top-shelf curriculum. Industry professionals choose SANS training again and again, year after year, for access to these highly regarded experts. There are only about 100 individuals in the world currently qualified as SANS Certified Instructors. Each is selected after proving his or her technical and teaching expertise through years of work and success. The instructors are the founders of international cybersecurity organizations, authors of best-selling books, and developers of the world’s most advanced cyber ranges and Capture-the-Flag challenges. Many are regularly called upon to share their expertise with government and commercial organizations around the world.

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

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

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

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

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

Establish longer-term expectations
- Information security is a specialized career path within IT, with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense—not a once-and-done item.
- Take a GIAC Certification exam to prove the training worked. Employers value the validation of skills and knowledge that a GIAC Certification provides. Exams are psychometrically designed to establish competency for related job tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expenses into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.
The job roles and skills required in information security grow and change as the organization scales. While every professional needs a baseline of knowledge and capabilities in cyber defense and incident response, over time you will develop specialized members of your team to work together in particular areas.

Four critical job roles typically emerge:

- **Security Monitoring & Detection Professionals** – Identifying security anomalies within your environment requires an increasingly sophisticated set of skills. All too often, vendor training teaches to the tool, without explaining how the tool works or how it can be best used. To deploy detection and monitoring tools and interpret their output, you need a more robust understanding of tools, techniques, and analysis.

- **Pen Testers & Vulnerability Analysts** – A professional who can find weaknesses is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires a different set of tools and a different way of thinking, but it’s still essential in improving defenses.

- **Forensic Investigators & Incident Responders** – Larger organizations need specialized professionals who can move beyond first-level incident response. Whether you’re maintaining a trail of evidence or hunting for threats, you need the skills to analyze attacks and develop appropriate remediation and recovery plans.

- **Security Managers** – As their staffs of talented technologists grow, organizations require effective leaders to manage them. These managers won’t necessarily perform hands-on work, but they must understand enough about underlying technologies and frameworks to help set security strategy, develop appropriate policies, interact with their skilled practitioners, and measure outcomes.

Within (or beyond) these four areas, a high-performing security organization will develop individuals further, with some individual professionals able to cover more areas, while others go deeper into just one specialty. Along the entire spectrum from Active Defense to Cloud Defense, and from Python for InfoSec professionals to Malware Reengineering, SANS offers more than 30 courses to train for specialized roles or learn about more advanced topics, meeting the needs of security professionals at every level.
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.*

Special Pricing

Extend Your Training Experience with an OnDemand Bundle

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

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.
SANS provides top-notch, quality training. The instructors are passionate and genuinely care about influencing and leading the future of security.
-Dave Ferguson, CareFirst, Inc.

Courses and Certifications Offered

SEC401: Security Essentials Bootcamp Style
GIAC Security Essentials (GSEC)

SEC460: Enterprise Threat and Vulnerability Assessment

SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling
GIAC Certified Incident Handler (GCIH)

SEC530: Defensible Security Architecture and Engineering
GIAC Defensible Security Architecture (GDSA)

SEC540: Cloud Security and DevOps Automation

SEC555: SIEM with Tactical Analytics
GIAC Certified Detection Analyst (GCDA)

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

FOR500: Windows Forensic Analysis
GIAC Certified Forensic Examiner (GCFE)

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response NEW
GIAC Network Forensic Analyst (GNFA)

ICS410: ICS/SCADA Security Essentials
Global Industrial Cyber Security Professional (GICSP)

“SANS provides top-notch, quality training. The instructors are passionate and genuinely care about influencing and leading the future of security.”
-Dave Ferguson, CareFirst, Inc.

Instructor Biographies

www.sans.org/san-francisco-summer/instructors

Hotel Information

Hilton San Francisco Union Square
$269 per night through June 28, 2019

Use code EarlyBird19
Pay by May 29 to receive $350 off
Pay by June 19 to receive $200 off

Early Bird Discounts

San Francisco, CA | July 22-27, 2019
www.sans.org/san-francisco-summer
#SANSSF

Courses are subject to change. Please visit www.sans.org for the most up-to-date information.
The materials and instructors are excellent and the content is relevant to current security operations in any industry. The combination of labs and NetWars provides hands-on experience that really helps to understand the content.

-Jerry Bunn, Digital Realty

Early Bird Discounts
Use code EarlyBird19

Pay by June 19 to receive $350 off
Pay by July 10 to receive $200 off

Courses and Certifications Offered

SEC401: Security Essentials Bootcamp Style
GIAC Security Essentials (GSEC)

SEC540: Cloud Security and DevOps Automation

SEC575: Mobile Device Security and Ethical Hacking
GIAC Mobile Device Security Analyst (GMOB)

SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses
GIAC Defending Advanced Threats (GDAT)

SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

MGT414: SANS Training Program for CISSP® Certification
GIAC Information Security Professional (GISP)

Simulcast is available with this course

Courses are subject to change. Please visit www.sans.org for the most up-to-date information.

Instructor Biographies

www.sans.org/san-jose/instructors

Hotel Information

DoubleTree by Hilton San Jose
$225 per night through July 19, 2019
San Francisco Fall
San Francisco, CA  |  September 23-28, 2019
www.sans.org/san-francisco-fall
#SANSSF

Early Bird Discounts  Use code EarlyBird19
Pay by July 31 to receive $350 off
Pay by August 21 to receive $200 off

Courses and Certifications Offered

SEC401: Security Essentials Bootcamp Style
GIAC Security Essentials (GSEC)

GIAC Certified Enterprise Defender (GCED)

SEC545: Cloud Security Architecture and Operations

SEC560: Network Penetration Testing and Ethical Hacking
GIAC Penetration Tester (GPEN)

FOR500: Windows Forensic Analysis
GIAC Certified Forensic Examiner (GCFE)

MGT512: Security Leadership Essentials for Managers
GIAC Security Leadership (GSLC)

MGT514: Security Strategic Planning, Policy, and Leadership
GIAC Strategic Planning, Policy, and Leadership (GSTRT)

“The exposure to top-notch instruction, relevant information, and hands-on labs provides a comprehensive learning experience”
-Ryan Paros, NCCI Holdings, Inc

Instructor Biographies
www.sans.org/san-francisco-fall/instructors

Hotel Information
Hyatt Centric Fisherman’s Wharf
$269 per night through September 3, 2019

Courses are subject to change. Please visit www.sans.org for the most up-to-date information.
“SANS is the best in the Information Security training space, no one else comes close! What I learned will improve our Blue Teaming effort to better protect our environment and our clients.”

-Jodie Monette, HealthEast

Courses and Certifications Offered

SEC301: Introduction to Cyber Security  
GIAC Information Security Fundamentals (GISF)

SEC401: Security Essentials Bootcamp Style  
GIAC Security Essentials (GSEC)

SEC503: Intrusion Detection In-Depth  
GIAC Certified Intrusion Analyst (GCIA)

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling  
GIAC Certified Incident Handler (GCIH)

SEC511: Continuous Monitoring and Security Operations  
GIAC Continuous Monitoring Certification (GMON)

SEC530: Defensible Security Architecture and Engineering  
GIAC Defensible Security Architecture (GDSA)

SEC545: Cloud Security Architecture and Operations

SEC555: SIEM with Tactical Analytics  
GIAC Certified Detection Analyst (GCDA)

MGT414: SANS Training Program for CISSP® Certification  
GIAC Information Security Professional (GISP)

ICS410: ICS/SCADA Security Essentials  
Global Industrial Cyber Security Professional (GiCSP)

Early Bird Discounts  
Pay by August 14 to receive $350 off  
Pay by September 4 to receive $200 off

Hotel Information

The Westin San Diego Gaslamp Quarter  
$230 per night through September 16, 2019

Instructor Biographies

www.sans.org/san-diego/instructors

San Diego  
San Diego, CA | October 7-12, 2019  
www.sans.org/san-diego  
#SANSSanDiego

NetWars

Challenge your skills at the Cyber Defense NetWars Tournament

Courses are subject to change. Please visit www.sans.org for the most up-to-date information.
Courses and Certifications Offered

SEC401: Security Essentials Bootcamp Style
GIAC Security Essentials (GSEC)

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling
GIAC Certified Incident Handler (GCIH)

FOR500: Windows Forensic Analysis
GIAC Certified Forensic Examiner (GCFE)

FOR518: Mac and iOS Forensic Analysis and Incident Response

ICS456: Essentials for NERC Critical Infrastructure Protection
GIAC Critical Infrastructure Protection (GCIP)

“SANS training showed me how to think outside the box when looking at the servers and network devices I have to protect. The camaraderie, being able to see things from other perspectives, and having someone to talk to that has real-world experience was awesome.”

-Robin Vaughn, Turner Broadcasting

Early Bird Discounts
Use code EarlyBird19
Pay by August 28 to receive $350 off
Pay by September 18 to receive $200 off

Instructor Biographies
www.sans.org/santa-monica/instructors

Hotel Information
DoubleTree Suites by Hilton Hotel Santa Monica
$249 per night through October 5, 2019

Courses are subject to change. Please visit www.sans.org for the most up-to-date information.
Experience
NetWars at:

San Diego 2019
October 10 & 11
Cyber Defense NetWars Tournament

“NetWars takes the concepts in the class and gives you an opportunity to put them into action. Highly recommended!”
– Kyle McDaniel, Lenovo

Develop skills in:
• Cyber Defense
• Penetration Testing

Participation in NetWars is free for students taking 4-, 5-, or 6-day courses.

NetWars takes place in the evening, after class, and gives you an immediate opportunity to apply what you’ve learned in a fun, competitive, hands-on, and educational environment!

Seating is limited, so add NetWars when you register for your course.

Play solo or on a team of up to five players

www.sans.org/netwars
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.

Developed 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 GIAC 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. A lot of the concepts are something I will be able to use in my day-to-day job.”

-Sandy Baguskas, John Hancock
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.
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 mid-sized to large 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.

SEC460 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 organization.

“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
Immeasurable amounts of personal and potentially incriminating data are currently stored in the websites, apps, and social media platforms that people access and update daily via their devices. Those data can become evidence for citizens, governments, and businesses to use in solving real financial, employment, and criminal issues with the help of a professional information gatherer.

Many people think using their favorite Internet search engine is sufficient to find the data they need and do not realize that most of the Internet is not indexed by search engines. SEC487 teaches students legitimate and effective ways to find, gather, and analyze these data from the Internet. You’ll learn about reliable places to harvest data using manual and automated methods and tools. Once you have the information, we’ll show you how to ensure that it is sound, how to analyze what you’ve gathered, and how to make sure it is useful to your investigations.

This is a foundational course in open-source intelligence (OSINT) gathering and, as such, will move quickly through many areas of the field. You will learn current, real-world skills, techniques, and tools that law enforcement, private investigators, cyber attackers, and defenders use to scour the massive amount of information across the Internet, analyze the results, and pivot on interesting pieces of data to find other areas for investigation. Our goal is to provide the OSINT knowledge base for students to be successful in their fields whether they are cyber defenders, threat intelligence analysts, private investigators, insurance claims investigators, intelligence analysts, law enforcement personnel, or just someone curious about OSINT.

Throughout the course week, students will participate in numerous hands-on labs using the tools and techniques that are the basis for gathering free data from the Internet. More than 20 labs in this course use the live Internet and dark web to help students gain real-world confidence. You’ll leave the course knowing not just how to use search features on a website, but all of the scenario-based requirements and OSINT techniques needed to gather truly important OSINT data.

Course Author Statement

“I recognized that the barrier to performing excellent OSINT was not that there was no free data on the Internet. It was that there was too much data on the Internet. The challenge transitioned from ‘how do I find something’ to ‘how do I find only what I need?’ This course was born from this need to help others learn the tools and techniques to effectively gather and analyze OSINT data from the Internet.”

-Micah Hoffman

“Fantastic introduction to a wide spectrum of OSINT techniques and practices, with great interactive labs and lots of deep dives!”

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

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

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

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

“SEC501 is a very valuable course to a Network/Security Administrator. The first chapter of Defensible Network Architecture is worth the price of admission in of itself.”

-Ryan Bast, Subzero Group, Inc.
Reports of prominent organizations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?

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

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

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

“The labs were instrumental in reinforcing the instructor-led material, making it easier to grasp the concepts.”

-Richard Llanas, SSCLANT
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
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!
SEC530: Defensible Security Architecture and Engineering 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, and 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 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)
SEC540: Cloud Security and DevOps Automation

SEC540 gives developers and security professionals the tools needed to build and deliver secure software using DevOps and cloud services, specifically Amazon Web Services (AWS). It explains how the principles, practices, and tools of DevOps and AWS can improve the reliability, integrity, and security of applications.

The first two days of the course examine the implementation of Secure DevOps using lessons from successful DevOps security programs. Using popular open-source tools such as GitLab, Puppet, Jenkins, Graphana, and Docker, you will create a secure DevOps CI/CD toolchain that can automatically build, test, and deploy infrastructure and applications. In a series of labs, you will inject security into your CI/CD toolchain using a variety of security tools, patterns, and techniques.

The final three days of the course will teach you to shift your DevOps workloads to the cloud and secure software using AWS. With your CI/CD toolchain, you will build a cloud infrastructure that can deploy applications and microservices to the cloud, instead of to local servers. You’ll also analyze and fix cloud infrastructure and application vulnerabilities using AWS security services and tools such as API Gateway, IAM, CloudFront Signed URLs, Security Token Service, KMS, encryption, WAF, Lambda for Serverless computing, CFN NAG scanner, AWS Security Benchmark, and much more.

SEC40 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. It also uses Jenkins and AWS developer tools such as CloudFormation, CodeCommit, CodeBuild, CodePipeline, and other cloud application services, so you can experience the use of these services when securing infrastructure and applications.

“SEC540 opened my eyes to a new way of thinking about operations and security unlike anything since SEC401: Security Essentials.”

-Todd Anderson, OBE
As more organizations move data and infrastructure to the cloud, security is becoming a major priority. Operations and development teams are finding new uses for cloud services, and executives are eager to save money and gain new capabilities and operational efficiency by using these services. But will information security prove to be an Achilles’ heel? Many cloud providers do not provide detailed control information about their internal environments, and quite a few common security controls used internally may not translate directly to the public cloud.

SEC545: Cloud Security Architecture and Operations will tackle these issues one by one. We’ll start with a brief introduction to cloud security fundamentals, then cover the critical concepts of cloud policy and governance for security professionals. For the rest of day one and all of day two, we’ll move into technical security principles and controls for all major cloud types (SaaS, PaaS, and IaaS). We’ll learn about the Cloud Security Alliance framework for cloud control areas, then delve into assessing risk for cloud services, looking specifically at technical areas that need to be addressed.

The course then moves into cloud architecture and security design, both for building new architectures and for adapting tried-and-true security tools and processes to the cloud. This will be a comprehensive discussion that encompasses network security (firewalls and network access controls, intrusion detection, and more), as well as all the other layers of the cloud security stack. We’ll visit each layer and the components therein, including building secure instances, data security, identity and account security, and much more. We’ll devote an entire day to adapting our offense and defense focal areas to the cloud. This will involve looking at vulnerability management and pen testing, as well as covering the latest and greatest cloud security research. On the defense side, we’ll delve into incident handling, forensics, event management, and application security.

We wrap up the course by taking a deep dive into SecDevOps and automation, investigating methods of embedding security into orchestration and every facet of the cloud life cycle. We’ll explore tools and tactics that work, and even walk through several cutting-edge use cases where security can be automated entirely in both deployment and incident detection-and-response scenarios using APIs and scripting.

“If an organization is starting its journey to the cloud, SEC545 is a must for security practitioners to take!”

-Troy Davidson, Suncor
Many organizations have logging capabilities but lack the people and processes to analyze them. In addition, logging systems collect vast amounts of data from a variety of data sources that require an understanding of the sources for proper analysis. This course is designed to provide individuals with the training, methods, and processes to enhance existing logging solutions. The course will also help you understand the when, what, and why behind the logs. This is a lab-heavy course that utilizes SOF-ELK, a SANS-sponsored free Security Information and Event Management (SIEM) solution, to provide hands-on experience and the mindset for large-scale data analysis.

Today, security operations do not suffer from a “big data” problem but rather a “data analysis” problem. Let’s face it, there are multiple ways to store and process large amounts of data without any real emphasis on gaining insight into the information collected. Added to that is the daunting idea of an infinite list of systems from which one could collect logs. It is easy to get lost in the perils of data saturation. This course moves away from the typical churn-and-burn log systems and moves instead towards achieving actionable intelligence and developing a tactical Security Operations Center (SOC).

This course is designed to demystify the SIEM architecture and process by navigating the student through the steps of tailoring and deploying a SIEM to full SOC integration. The material will cover many bases in the “appropriate” use of a SIEM platform to enrich readily available log data in enterprise environments and extract actionable intelligence. Once the information is collected, the student will be shown how to present the gathered input into usable formats to aid in eventual correlation. Students will then iterate through the log data and events to analyze key components that will allow them to learn how rich this information is, how to correlate the data, how to start investigating based on the aggregate data, and finally, how to go hunting with this newly gained knowledge. They will also learn how to deploy internal post-exploitation tripwires and breach canaries to nimbly detect sophisticated intrusions. Throughout the course, the text and labs will not only show how to manually perform these actions, but also how to automate many of the processes mentioned so students can employ these tasks the day they return to the office.

The underlying theme is to actively apply Continuous Monitoring and analysis techniques by utilizing modern cyber threat attacks. Labs will involve replaying captured attack data to provide real-world results and visualizations.

“The immediate value of the course material is unlike any course or training I’ve received. A++.”

-David Savercool, Cart Container
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, scoping and recon, then dives deep into scanning, target exploitation, 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.

You’ll 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.

After taking SEC560, 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.

“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
Imagine an attack surface that is spread across your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports numerous different wireless technologies all ripe for attack. Such a surface already exists today: mobile devices. These devices are the biggest attack surface in most organizations, yet these same organizations often don’t have the skills needed to assess them.

SEC575 NOW COVERS ANDROID PIE AND IOS 12

SEC575: Mobile Device Security and Ethical Hacking is designed to give you the skills you need to understand the security strengths and weaknesses in Apple iOS and Android devices. Mobile devices are no longer a convenience technology: they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores throughout the world. Users rely on mobile devices more today than ever before – we know it, and the bad guys do too. The SEC575 course examines the full gamut of these devices.

LEARN HOW TO PEN TEST THE BIGGEST ATTACK SURFACE IN YOUR ENTIRE ORGANIZATION

With the skills you learn in SEC575, you will be able to evaluate the security weaknesses of built-in and third-party applications. You’ll learn how to bypass platform encryption and how to manipulate apps to circumvent client-side security techniques. You’ll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You’ll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS, and you’ll bypass lock screen to exploit lost or stolen devices.

TAKE A DEEP DIVE INTO EVALUATING MOBILE APPS, OPERATING SYSTEMS, AND THEIR ASSOCIATED INFRASTRUCTURES

Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you’ll review ways to effectively communicate threats to key stakeholders. You’ll leverage tools, including Mobile App Report Cards, to characterize threats for managers and decision-makers, while also identifying sample code and libraries that developers can use to address risks in in-house applications.

YOUR MOBILE DEVICES ARE GOING TO COME UNDER ATTACK – HELP YOUR ORGANIZATION PREPARE FOR THE ONSLAUGHT!

In employing your newly learned skills, you’ll apply a step-by-step mobile device deployment penetration test. Starting with gaining access to wireless networks to implement man-in-the-middle attacks and finishing with mobile device exploits and data harvesting, you’ll examine each step of the test with hands-on exercises, detailed instructions, and tips and tricks learned from hundreds of successful penetration tests. By building these skills, you’ll return to work prepared to conduct your own test, or better informed on what to look for and how to review an outsourced penetration test.

Mobile device deployments introduce new threats to organizations, including advanced malware, data leakage, and the disclosure to attackers of enterprise secrets, intellectual property, and personally identifiable information assets. Further complicating matters, there simply are not enough people with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you’ll be able to differentiate yourself as having prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test – all critical skills to protect and defend mobile device deployments.

“SEC575 provides an incredible amount of information, and the hands-on labs are awesome. It is a must-have for mobile penetration testers.”

-Richard Takacs, Integrity360

Who Should Attend
- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing, deploying or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets

Six-Day Program
9:00am - 5:00pm
36 CPEs
Laptop Required

Who Should Attend
- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing, deploying or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets

“SEC575 provides an incredible amount of information, and the hands-on labs are awesome. It is a must-have for mobile penetration testers.”

-Richard Takacs, Integrity360
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 you with 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 “SyncTechLabs” 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, you will also compromise our virtual organization 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?

---

“Security architects
Security engineers
Technical security managers
Security Operations Center analysts, engineers, and managers
IT administrators
Penetration testers who want to better understand how defensive controls work
IT administrators
Individuals looking to better understand how persistent cyber adversaries operate and how the IT environment can be improved to better prevent, detect, and respond to incidents

“The course discusses a lot of important aspects (the entire kill chain). It gives good insight into potential attacks and mitigation.”

- Kevin Giesekam, Dutch Police

---

Simulcast from San Jose
Bundle OnDemand with this course
Can your web apps withstand the onslaught of modern advanced attack techniques?

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

Are you ready to put your web apps to the test with cutting-edge skills?

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

This course offers hands-on learning of advanced web app exploitation skills.

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

“SEC642 is quality content for senior penetration testers – a nice extension of standard WAPT courses!”

-Caleb Jaren, Microsoft
This course is designed as a logical progression point for those who have completed SEC560: Network Penetration Testing and Ethical Hacking, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered includes weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, return-oriented programming (ROP), Windows exploit-writing, and much more!

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, you need a strong desire to learn, the support of others, and the opportunity to practice and build experience. SEC660 provides attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios. This course goes far beyond simple scanning for low-hanging fruit, and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

SEC660 starts off by introducing the advanced penetration concept, and provides an overview to help prepare students for what lies ahead. The focus of day one is on network attacks, an area often left untouched by testers. Topics include accessing, manipulating, and exploiting the network. Attacks are performed against NAC, VLANs, OSPF, 802.1X, CDP, IPv6, VOIP, SSL, ARP, SNMP, and others. Day two starts off with a technical module on performing penetration testing against various cryptographic implementations. The rest of the day is spent on network booting attacks, escaping Linux restricted environments such as chroot, and escaping Windows restricted desktop environments. Day three jumps into an introduction of Python for penetration testing, Scapy for packet crafting, product security testing, network and application fuzzing, and code coverage techniques. Days four and five are spent exploiting programs on the Linux and Windows operating systems. You will learn to identify privileged programs, redirect the execution of code, reverse-engineer programs to locate vulnerable code, obtain code execution for administrative shell access, and defeat modern operating system controls such as ASLR, canaries, and DEP using ROP and other techniques. Local and remote exploits, as well as client-side exploitation techniques, are covered. The final course day is dedicated to numerous penetration testing challenges requiring you to solve complex problems and capture flags.
All organizations must prepare for cyber crime occurring on their computer systems and within their networks. Demand has never been greater for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world’s best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

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

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

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

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

-Brad Milhorn, NTT Data Services
FOR518: Mac and iOS Forensic Analysis and Incident Response

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

The constantly updated FOR518: Mac and iOS Forensic Analysis and Incident Response course provides the techniques and skills necessary to take on any Mac or iOS case without hesitation. The intense hands-on forensic analysis and incident response skills taught in the course will enable analysts to broaden their capabilities and gain the confidence and knowledge to comfortably analyze any Mac or iOS device. In addition to traditional investigations, the course presents intrusion and incident response scenarios to help analysts learn ways to identify and hunt down attackers that have compromised Apple devices.

This course will teach you:

- Mac and iOS Fundamentals: How to analyze and parse the Hierarchical File System (HFS+) and Apple File System (APFS) by hand and recognize the specific domains of the logical file system and Mac-specific file types.
- User Activity: How to understand and profile users through their data files and preference configurations.
- Advanced Intrusion Analysis and Correlation: How to determine how a system has been used or compromised by using the system and user data files in correlation with system log files.
- Apple Technologies: How to understand and analyze many Mac and iOS-specific technologies, including Time Machine, Spotlight, iCloud, Document Versions, FileVault, Continuity, and FaceTime.

FOR518: Mac and iOS Forensic Analysis and Incident Response aims to train a well-rounded investigator by diving deep into forensic and intrusion analysis of Mac and iOS. The course focuses on topics such as the HFS+ and APFS file systems, Mac-specific data files, tracking of user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac-exclusive technologies. A computer forensic analyst who completes this course will have the skills needed to take on a Mac or iOS forensics case.

FORENSICATE DIFFERENTLY!

“[FOR518] is valuable in providing me with foundational knowledge of the file system and artifacts.”

- Kevin Neely, Pure Storage
FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

FIGHT CRIME. UNRAVEL INCIDENTS...ONE BYTE (OR PACKET) AT A TIME.

Take your system-based forensic knowledge onto the wire. Incorporate network evidence into your investigations, provide better findings, and get the job done faster.

It is exceedingly rare to work any forensic investigation that doesn’t have a network component. Endpoint forensics will always be a critical and foundational skill for this career, but overlooking attackers’ network communications is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, uncover attackers that have been active for months or longer, or even prove useful in definitively proving a crime actually occurred.

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking – we’ll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence as well as how to place new collection platforms while an incident is already under way.

Whether you are a consultant responding to a client’s site, a law enforcement professional assisting victims of cybercrime and seeking prosecution of those responsible, an on-staff forensic practitioner, or a member of the growing ranks of “threat hunters,” this course offers hands-on experience with real-world scenarios that will help take your work to the next level.

The hands-on labs in this class cover a wide range of tools and platforms, including the venerable tcpdump and Wireshark for packet capture and analysis; NetworkMiner for artifact extraction; and open-source tools including nfdump, tcpxtract, tcpflow, and more. Newly added tools in the course include the SOF-ELK platform, a VMware appliance pre-configured with the ELK stack. This “big data” platform includes the Elasticsearch storage and search database, the Logstash ingest and parse utility, and the Kibana graphical dashboard interface. Together with the custom SOF-ELK configuration files, the platform gives forensicators a ready-to-use platform for log and NetFlow analysis. For full-packet analysis and hunting at scale, the Moloch platform is also used. Through all of the in-class labs, your shell scripting abilities will also be used to make easy work of ripping through hundreds and thousands of data records.
MGT414: SANS Training Program for CISSP® Certification

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam.

MGT414 focuses solely on the eight domains of knowledge as determined by (ISC)² that form a critical part of the CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

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
Security managers need both technical knowledge and management skills to gain the respect of technical team members, understand what technical staff are actually doing, and appropriately plan and manage security projects and initiatives. This is a big and important job that requires an understanding of a wide array of security topics.

This course empowers you to become an effective security manager and get up to speed quickly on information security issues and terminology. You won’t just learn about security, you will learn how to manage security.

To accomplish this goal the course covers a wide range of security topics across the entire security stack. Data, network, host, application, and user controls are covered in conjunction with key management topics that address the overall security lifecycle. This also includes governance and technical controls focused on protecting, detecting, and responding to security issues.

This approach prepares you to:

- Make sense of different cybersecurity frameworks
- Understand and analyze risk
- Understand the pros and cons of different reporting relationships
- Manage technical people
- Build a vulnerability management program
- Inject security into modern DevOps workflows
- Strategically leverage a SIEM
- Change behavior and build a security-aware culture
- Effectively manage security projects
- Enable modern security architectures and the cloud

MGT512 uses case studies, group discussions, team-based exercises, and in-class games to help students absorb both technical and management topics.

This course prepares you for the GSLC certification that meets the requirement of the DoD 8570 IAM Level 1, 2, 3.

Notice:
Please note that some course material for SEC401 and MGT512 may overlap. We recommend SEC401 for those interested in a more technical course of study, and MGT512 for those primarily interested in a leadership-oriented but less technical learning experience.

“This course was very relevant to my new role as Director of IT.”
-Brian Harris, Jackson EMC

“This course is highly useful for giving me a sound baseline of technical and general skills to help me manage an effective team.”
-Richard Ward, REA Group
As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to do three things:

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

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

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

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

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

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

The course is informative and relevant to anyone working with or alongside industrial control systems.”

- Abrael Delgado, Compuquip Technologies

ICS410: ICS/SCADA Security Essentials

Five-Day Program
9:00am - 5:00pm
30 CPEs
Laptop Required

Meet DoDD 8140 (8570) Requirements
www.sans.org/8140

Bundle OnDemand with this course

GICSP Industrial Cyber Security Professional
www.giac.org/gicsp

“GICSP” is the intellectual property of GIAC and is used under license. GIAC and SANS Institute are independent organizations.
This five-day course empowers students with knowledge of the “what” and the “how” of the version 5/6 standards. The course addresses the role of the Federal Energy Regulatory Commission (FERC), North American Reliability Corporation (NERC), and the Regional Entities, provides multiple approaches for identifying and categorizing Bulk Electric System (BES) cyber systems, and helps asset owners determine the requirements applicable to specific implementations. Additionally, the course covers implementation strategies for the version 5/6 requirements with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance.

The course features 25 hands-on labs range from securing workstations to digital forensics and lock picking.

The SANS ICS456: NERC Critical Infrastructure Protection Essentials course was developed by SANS ICS team members with extensive electric industry experience, including former Registered Entity Primary Contacts, a former NERC officer, and a Co-Chair of the NERC Critical Infrastructure Protection (CIP) Interpretation Drafting Team. Together the authors bring real-world, practitioner experience gained from developing and maintaining NERC CIP and NERC 693 compliance programs and actively participating in the standards development process.

You Will Learn:

- BES cyber system identification and strategies for lowering their impact rating
- Nuances of NERC defined terms and CIP standards applicability and how subtle changes in definitions can have a big impact on your program
- The significance of properly determining cyber system impact ratings and strategies for minimizing compliance exposure
- Strategic implementation approaches for supporting technologies
- How to manage recurring tasks and strategies for CIP program maintenance
- Effective implementations for cyber and physical access controls
- How to break down the complexity of NERC CIP in order to communicate with your leadership
- What to expect in your next CIP audit, how to prepare supporting evidence, and how to avoid common pitfalls
- How to understand the most recent Standards Development Team’s efforts and how that may impact your current CIP program

“This is best-in-class NERC CIP training. The courseware provides valuable compliance approaches and software tools for peer collaboration to build consent on implementation.”

-Jeff Mantong, WAPA
Job-Specific, Specialized Focus

Today’s cyber attacks are highly sophisticated and exploit specific vulnerabilities. Broad and general InfoSec certifications are no longer enough. Professionals need the specific skills and specialized knowledge required to meet multiple and varied threats. That’s why GIAC has more than 30 certifications, each focused on specific job skills and each requiring unmatched and distinct knowledge.

Deep, Real-World Knowledge

Theoretical knowledge is the ultimate security risk. Deep, real-world knowledge and hands-on skills are the only reliable means to reduce security risk. Nothing comes close to a GIAC certification to ensure that this level of real-world knowledge and skill has been mastered.

Most Trusted Certification Design

The design of a certification exam impacts the quality and integrity of a certification. GIAC exam content and question design are developed through a rigorous process led by GIAC’s on-staff psychometrician and reviewed by experts in each area. More than 78,000 certifications have been issued since 1999. GIAC certifications meet ANSI standards.

“Attackers are always evolving, and having a GIAC cert prepares you to evolve with them. It allows you to implement the appropriate methods and best practices in your company while understanding it’s a continuous fight.”

– Jason Sevilla, Cyber Intelligence Analyst
You can attend live SANS courses remotely with Simulcast

Simulcast is a great way to attend SANS cybersecurity courses remotely, with content streamed directly from the classroom to you. Additionally, Simulcast offers four months of access to revisit recorded lectures and labs and includes subject-matter-expert support.

Here are some benefits of taking your SANS training on the Simulcast platform:

- Dedicated, pre-event setup support so you are ready for class on day 1
- You can complete your course in one week through live, scheduled daytime sessions with SANS Certified Instructors
- In-class moderators who actively convey your questions to the instructor and ensure an interactive experience
- Teaching assistants available to support complex content and lab questions during your training sessions
- No travel, which extends training dollars and saves time
- The same instruction and learning outcomes as live training, with an additional four months of online access to recordings and virtual labs to absorb the course content

Simulcast Events | Courses

San Jose 2019  |  San Jose, CA  |  August 12-17  |  www.sans.org/san-jose
SEC540  |  SEC575  |  SEC599

Register now at www.sans.org/simulcast/courses

“I’m at home taking the online Simulcast class but I feel like I’m there in the room. I don’t feel isolated at all. I just have access to my comforts while taking the class.”

- Deona Vastine, State of California
SANS Training Formats

After selecting your training path or course, compare SANS multiple live and online training formats for the structure and schedule that works best for you. SANS is committed to ensuring your training experience always exceeds expectations.

Live Classroom Instruction

Training Events
Our most recommended format, live SANS training events deliver SANS’s top instructors teaching multiple courses at a single time and location. The events feature:

• Focused, immersive learning without the distractions of your office environment
• Direct access to SANS Certified Instructors
• Interactions with and learning from other professionals
• SANS@Night events, NetWars, vendor presentations, industry receptions, and many other activities

Our live training events in North America, serving thousands of students, are held in Orlando, Washington DC, Las Vegas, New Orleans, and San Diego. Regional events with hundreds of students are held in most major metropolitan areas during the year. See page 40 for upcoming training events in North America.

Summits
SANS Summits focus one or two days on a single topic of particular interest to the community. Speakers and talks are curated to ensure the greatest applicability to participants.

Community SANS Courses
Same SANS courses, courseware, and labs, taught by up-and-coming instructors in a regional area. Smaller classes allow for more extensive instructor interaction. No need to travel; commute each day to a nearby location.

Private Classes
Bring a SANS Certified Instructor to your location to train a group of your employees in your own environment. Save on travel and address sensitive issues or security concerns in your own environment.

“‘The decision to take five days away from the office is never easy, but so rarely have I come to the end of a course and had no regret whatsoever. This was one of the most useful weeks of my professional life.’

—Dan Trueman, Novae PLC

Online Training

SANS Online Training delivers the same world-renowned instructors, content, and learning results as SANS live training options, with several unique and valuable benefits. Students who train online enjoy subject-matter-expert support throughout the course, online access to all course labs, and the ability to revisit content without limits.

No matter where you are or when you can train, SANS has courses that will fit around your life.

Top Reasons to Take SANS Training Online:

• **Rewind** your training, so you can review complex details or topics
• **Revisit** content to ensure you master key concepts
• **Reinforce** your learning with subject-matter experts and labs
• **Retain** your knowledge of course content with four months of access

Our SANS OnDemand, vLive, Simulcast, and SelfStudy formats are backed by nearly 100 professionals who ensure we deliver the same quality instruction online (including support) as we do at live training events.

“I love the material, I love the SANS Online delivery, and I want the entire industry to take these courses.”

—Nick Sewell, IIT
2019 Training Events
See www.sans.org for more information.

**Security West**
San Diego, CA  May 9-16

- Northern VA Spring – Reston
  Reston, VA  May 19-24
- New Orleans
  New Orleans, LA  May 19-24
- Atlanta
  Atlanta, GA  May 28 - Jun 2
- San Antonio
  San Antonio, TX  May 28 - Jun 2
- Kansas City
  Kansas City, MO  Jun 10-15

**SANSFIRE**
Washington, DC  Jun 15-22

- Charlotte
  Charlotte, NC  Jul 8-13
- Pittsburgh
  Pittsburgh, PA  Jul 8-13
- Columbia
  Columbia, MD  Jul 15-20
- Rocky Mountain
  Denver, CO  Jul 15-20
- San Francisco Summer
  San Francisco, CA  Jul 22-27
- Boston Summer
  Boston, MA  Jul 29 – Aug 3
- Crystal City
  Arlington, VA  Aug 5-10
- San Jose
  San Jose, CA  Aug 12-17
- Minneapolis
  Minneapolis, MN  Aug 12-17
- Chicago
  Chicago, IL  Aug 19-24
- Virginia Beach
  Virginia Beach, VA  Aug 19-30
- New York City
  New York, NY  Aug 25-30
- Tampa-Clearwater
  Clearwater, FL  Aug 25-30

**Network Security**
Las Vegas, NV  Sep 9-16

**2019 Summit Events**

- Cloud Security
  San Jose, CA  Apr 29 – May 6
- Enterprise Defense
  Redondo Beach, CA  Jun 3-10
- Security Operations
  New Orleans, LA  Jun 24 – Jul 1
- DFIR
  Austin, TX  Jul 25 – Aug 1
- Security Awareness
  San Diego, CA  Aug 5-14
- Supply Chain Cybersecurity
  Arlington, VA  Aug 12-19
- Oil & Gas Cybersecurity
  Houston, TX  Sep 16-22

**2019 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.
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
- SCORM (Security Consensus Operational Readiness Evaluation)

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

Save $350 when you pay for any 4-, 5-, or 6-day course early. Enter the code “EarlyBird19” when registering.

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

5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407