Protect Your Business | Advance Your Career

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

See inside for courses offered in:
- Cyber Defense
- Penetration Testing
- Monitoring and Detection
- Digital Forensics
- Security Management

PLUS NEW COURSES
- SIEM with Tactical Analytics
- Secure DevOps and Cloud
- Application Security

“The experience, professionalism, and presentation of the speakers, along with the structured and relevant training with hands-on labs, make SANS the premier InfoSec training opportunity.”
- Jason Cathey, Bank of the Ozarks

SAVE $400
Register and pay by July 4th
Use code EarlyBird18

www.sans.org/virginia-beach
## SANS Instructors

The line-up of SANS Instructors for SANS Virginia Beach 2018 includes:

<table>
<thead>
<tr>
<th>Instructor</th>
<th>Role</th>
<th>@username</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carlos Cajigas</td>
<td>Certified Instructor</td>
<td>Carlos_Cajigas</td>
</tr>
<tr>
<td>G. Mark Hardy</td>
<td>Principal Instructor</td>
<td>g_mark</td>
</tr>
<tr>
<td>Justin Henderson</td>
<td>Certified Instructor</td>
<td>SecurityMapper</td>
</tr>
<tr>
<td>David Hoelzer</td>
<td>Faculty Fellow</td>
<td>lt_audit</td>
</tr>
<tr>
<td>Ryan Johnson</td>
<td>Certified Instructor</td>
<td>ForensicRj</td>
</tr>
<tr>
<td>Timothy McKenzie</td>
<td>Instructor</td>
<td>timboloman</td>
</tr>
<tr>
<td>Seth Misenar</td>
<td>Faculty Fellow</td>
<td>sethmisenar</td>
</tr>
<tr>
<td>G. Mark Hardy</td>
<td>Faculty Fellow</td>
<td>g_mark</td>
</tr>
<tr>
<td>Ryan Johnson</td>
<td>Certified Instructor</td>
<td>ForensicRj</td>
</tr>
<tr>
<td>Keith Palmgren</td>
<td>Senior Instructor</td>
<td>kpatmgren</td>
</tr>
<tr>
<td>Peter Szczepankiewicz</td>
<td>Certified Instructor</td>
<td>@_s14</td>
</tr>
<tr>
<td>Jonathan Thyer</td>
<td>Certified Instructor</td>
<td>joff_thyer</td>
</tr>
<tr>
<td>Jake Williams</td>
<td>Senior Instructor</td>
<td>MalwareJake</td>
</tr>
<tr>
<td>Joshua Wright</td>
<td>Senior Instructor</td>
<td>joswr1ght</td>
</tr>
<tr>
<td>Carlos Cajigas</td>
<td>Certified Instructor</td>
<td>Carlos_Cajigas</td>
</tr>
<tr>
<td>Ted Demopoulos</td>
<td>Principal Instructor</td>
<td>TedDemop</td>
</tr>
<tr>
<td>Kevin Fiscus</td>
<td>Principal Instructor</td>
<td>kevinbfiscus</td>
</tr>
<tr>
<td>Eric Johnson</td>
<td>Certified Instructor</td>
<td>emjohn20</td>
</tr>
<tr>
<td>Kevin Fiscus</td>
<td>Principal Instructor</td>
<td>kevinbfiscus</td>
</tr>
<tr>
<td>Seth Misenar</td>
<td>Faculty Fellow</td>
<td>sethmisenar</td>
</tr>
<tr>
<td>Ryan Johnson</td>
<td>Certified Instructor</td>
<td>ForensicRj</td>
</tr>
<tr>
<td>Keith Palmgren</td>
<td>Senior Instructor</td>
<td>kpatmgren</td>
</tr>
<tr>
<td>Peter Szczepankiewicz</td>
<td>Certified Instructor</td>
<td>@_s14</td>
</tr>
<tr>
<td>Jonathan Thyer</td>
<td>Certified Instructor</td>
<td>joff_thyer</td>
</tr>
<tr>
<td>Jake Williams</td>
<td>Senior Instructor</td>
<td>MalwareJake</td>
</tr>
<tr>
<td>Joshua Wright</td>
<td>Senior Instructor</td>
<td>joswr1ght</td>
</tr>
</tbody>
</table>

## Courses at a Glance (Week 1)

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td>Introduction to Cyber Security</td>
<td></td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td></td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits &amp; Incident Handling</td>
<td></td>
</tr>
<tr>
<td>SEC542</td>
<td>Web App Penetration Testing and Ethical Hacking</td>
<td></td>
</tr>
<tr>
<td>SEC573</td>
<td>Automating Information Security with Python</td>
<td></td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td></td>
</tr>
<tr>
<td>MGT512</td>
<td>SANS Security Leadership Essentials for Managers with Knowledge Compression™</td>
<td></td>
</tr>
<tr>
<td>DEV540</td>
<td>Secure DevOps and Cloud Application Security</td>
<td></td>
</tr>
</tbody>
</table>

## Courses at a Glance (Week 2)

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td></td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td></td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics</td>
<td></td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td></td>
</tr>
<tr>
<td>SEC575</td>
<td>Mobile Device Security and Ethical Hacking</td>
<td></td>
</tr>
<tr>
<td>FOR500</td>
<td>Windows Forensic Analysis</td>
<td></td>
</tr>
<tr>
<td>FOR572</td>
<td>Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response</td>
<td></td>
</tr>
<tr>
<td>MGT514</td>
<td>Security Strategic Planning, Policy, and Leadership</td>
<td></td>
</tr>
</tbody>
</table>
Extend and Validate Your Training

Add an OnDemand Bundle OR GIAC Certification Attempt
to your course within seven days of this event to get bundle pricing.*

Extend Your Training Experience with an OnDemand Bundle

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

OnDemand Bundle price – $729

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

-Robert Jones, Team Jones, Inc.

Get Certified with GIAC Certifications

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- Two practice exams included
- Four months of access to complete the attempt

GIAC bundle price – $729

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

-Christina Ford, Department of Commerce

More Information

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

*GIAC and OnDemand Bundles are only available for certain courses.
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 Global Information Security Fundamentals (GISF) certification test, as well as for the next SANS course in this progression, SEC401: Security Essentials Bootcamp Style. It also delivers on the SANS promise: You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.

“The course provided me with a lot of great information.... A lot of the concepts are something I will be able to use in my day-to-day job.”
- Sandy Baguskas, John Hancock
SEC401: Security Essentials Bootcamp Style

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

Is SEC401: Security Essentials Bootcamp Style the right course for you?

STOP and ask yourself the following questions:

- Do you fully understand why some organizations get compromised and others do not?
- If there were compromised systems on your network, are you confident that you would be able to find them?
- Do you know the effectiveness of each security device and are you certain that they are all configured correctly?
- Are proper security metrics set up and communicated to your executives to drive security decisions?

If you do not know the answers to these questions, then the SEC401 course will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

Learn to build a security roadmap that can scale today and into the future.

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization’s critical information assets and business systems. Our course will show you how to prevent your organization’s security problems from being headline news in the Wall Street Journal!

Prevention is ideal but detection is a must.

With the rise in advanced persistent threats, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organization’s network depends on the effectiveness of the organization’s defense. Defending against attacks is an ongoing challenge, with new threats emerging all of the time, including the next generation of threats. Organizations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

- What is the risk?
- Is it the highest priority risk?
- What is the most cost-effective way to reduce the risk?

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you will need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.
Six-Day Program
Mon, Aug 20 - Sat, Aug 25
This course has extended
bootcamp hours
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: David Hoelzer

Who Should Attend
- Intrusion detection (all levels), system, and security analysts
- Network engineers/administrators
- Hands-on security managers

Reportsof 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/IP 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.

“Who has employed new material. Students who may already know the material or who have quickly mastered new material. 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, SSC-20

David Hoelzer has authored more than 20 sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past 25 years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at the SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. As a SANS instructor, David has trained security professionals from organizations including the NSA, DHHS, Fortune 500 companies, various Department of Defense sites, national laboratories, and many colleges and universities. David is a research fellow at the Center for Cybermedia Research, as well as at the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC). He also is an adjunct research associate for the UNLV Cybermedia Research Lab and a research fellow with the Internet Forensics Lab. David has written and contributed to more than 15 peer-reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas-based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open-source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a B.S. in IT, Summa Cum Laude, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University.
Six-Day Program
Mon, Aug 20 - Sat, Aug 25
This course has extended hours
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor:
Peter Szczepankiewicz

Who Should Attend
- Incident handlers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

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.

“I last took SEC504 five plus years ago and so much has changed since then. I love SANS and how they help us to stay up-to-date on the latest techniques so we can better defend our networks.”

-Adam Fowler, GMAC

Peter Szczepankiewicz
GCIH Incident Handler
www.giac.org/gcih

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/virginia-beach-2018/courses
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), or Network Security Monitoring (NSM) taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach will be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

SEC511 will take you on quite a journey. We start by exploring traditional security architecture to assess its current state and the attacks against it. Next, we discuss and discover modern security design that represents a new proactive approach to such architecture that can be easily understood and defended. We then transition to how to actually build the network and endpoint security, and then carefully navigate our way through automation, NSM/CDM/CSM. For timely detection of potential intrusions, the network and systems must be proactively and continuously monitored for any changes in the security posture that might increase the likelihood that attackers will succeed.

Your SEC511 journey will conclude with one last hill to climb! The final day (Day 6) features a Capture-the-Flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. Course authors Eric Conrad and Seth Misenar have designed the Capture-the-Flag competition to be fun, engaging, comprehensive, and challenging. You will not be disappointed!
Web applications play a vital role in every modern organization. However, if your organization doesn’t properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

SEC542 helps students move beyond push-button scanning to professional, thorough, and high-value web application penetration testing.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no “patch Tuesday” for custom web applications, and major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

SEC542 enables students to assess a web application’s security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations.

In this course, students will come to understand major web application flaws and their exploitation. Most importantly, they’ll learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations. Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. This course will help you demonstrate the true impact of web application flaws through exploitation.

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn. The course features more than 30 formal hands-on labs and culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way that hammers home lessons learned.

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

Timothy McKenzie
SANS Instructor
@timboloman
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 class is designed to provide individuals with the training, methods, and processes to enhance existing logging solutions. This class 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 class 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.

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

Who Should Attend
- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center analysts, engineers, and managers
- CND analysts
- Security monitoring specialists
- System administrators
- Cyber threat investigators
- Individuals working to implement Continuous Security Monitoring
- Individuals working in a hunt team capacity

“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.

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

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

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

You will learn how to perform detailed reconnaissance, studying a target’s infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won’t just cover run-of-the-mill options and configurations, we’ll also go over the lesser known but super-useful capabilities of the best pen test toolsets available today. After scanning, you’ll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You’ll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.
SEC573: Automating Information Security with Python

All security professionals, including penetration testers, forensics analysts, network defenders, security administrators, and incident responders, have one thing in common: CHANGE. Change is constant. Technology, threats, and tools are constantly evolving. If we don’t evolve with them, we’ll become ineffective and irrelevant, unable to provide the vital defenses our organizations increasingly require.

Maybe your chosen operating system has a new feature that creates interesting forensics artifacts that would be invaluable for your investigation, if only you had a tool to access it. Often for new features and forensics artifacts, no such tool has yet been released. You could try moving your case forward without that evidence or hope that someone creates a tool before the case goes cold. Or you can write a tool yourself.

Perhaps an attacker bypassed your defenses and owned your network months ago. If existing tools were able to find the attack, you wouldn’t be in this situation. You are bleeding sensitive data and the time-consuming manual process of finding and eradicating the attacker is costing you money and hurting your organization big time. The answer is simple if you have the skills: Write a tool to automate your defenses.

Finally, what do you do when “off-the-shelf” tools and exploits fall short? As a penetration tester you need to evolve as quickly as the threats you are paid to emulate, so the answer is simple, if you have the skills: You write your own tool.

Writing a tool is easier said than done, right? Not really. Python is a simple, user-friendly language that is designed to make automating tasks that security professionals perform quick and easy. Whether you are new to coding or have been coding for years, SEC573: Automating Information Security with Python will have you creating programs to make your job easier and make you more efficient. This self-paced class starts from the very beginning assuming you have no prior experience or knowledge of programming. We cover all of the essentials of the language up front. If you already know the essentials, you will find that the pyWars lab environment allows advanced developers to quickly accelerate to more advanced material in the class. The self-paced style of the class will meet you where you are to let you get the most out of what is being taught.

Beyond the essentials we discuss file analysis, packet analysis, forensics artifact carving, networking, database access, website access, process execution, exception handling, object-oriented coding, and more.

This course is designed to give you the skills you need for tweaking, customizing, or outright developing your own tools. We put you on the path of creating your own tools, empowering you in automating the daily routine of today’s information security professional, and in achieving more value in less time. Again and again, organizations serious about security emphasize their need for skilled tool builders.

There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it. Join us and learn Python in-depth and fully weaponized.

Who Should Attend
- Security professionals who benefit from automating routine tasks so they can focus on what’s most important
- Forensics analysts who can no longer wait on someone else to develop a commercial tool to analyze artifacts
- Network defenders who sift through mountains of logs and packets to find evildoers in their networks
- Penetration testers who are ready to advance from script kiddie to professional offensive computer operations operator
- Security professionals who want to evolve from security tool consumer to security solution provider

“SEC573 is excellent. I went from having almost no Python coding ability to being able to write functional and useful programs.”

-Caleb Jaren, Microsoft

Jonathan (Joff) Thyer is a senior security consultant, researcher, and penetration tester with Black Hills Information Security. Joff has over 15 years of experience in the IT industry as an enterprise network architect, network security defender, and information security consultant. Joff has experience with intrusion detection and prevention systems, vulnerability analysis, penetration testing, engineering network infrastructure defense (including Cisco ISE deployment), and software development. Joff has taught Mastering Packet Analysis and mentored for the SEC03: Intrusion Detection In-Depth course. Joff is also a co-host on the Security Weekly podcast, which features the latest information security news, research, interviews, and technical information. Joff holds a bachelor’s degree in mathematics and master’s degree in computer science. He also holds the the GIAC GPEN: Penetration Tester certification.

Jonathan Thyer
SANS Certified Instructor
@joff_thyer

SANS Technology Institute
www.sans.edu

Bundle OnDemand with this course

Register at www.sans.org/virginia-beach | 301-654-SANS (7267)
SEC575: Mobile Device Security and Ethical Hacking

Imagine an attack surface spread throughout 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. You don’t need to imagine any further because this already exists today: mobile devices. These devices are the biggest attack surface in most organizations, yet these same organizations often don’t have personnel with the skills needed to assess them.

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.

This course is designed to give you the skills you need to understand the security strengths and weaknesses in Apple iOS, Android, and wearable devices including Apple Watch and Android Wear. With these skills, you will evaluate the security weaknesses of built-in and third-party applications. You’ll learn how to bypass platform encryption, and how to manipulate Android apps to circumvent obfuscation 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 devices, and you’ll exploit lost or stolen devices to harvest sensitive mobile application data.

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 management and decision-makers, while identifying sample code and libraries that developers can use to address risks for in-house applications.

You’ll then use your new skills to apply a mobile device deployment penetration test in a step-by-step fashion. 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 in conducting such a 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, and you’ll be better informed about 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 of enterprise secrets, intellectual property, and personally identifiable information assets to attackers. 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 being 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.

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 |

Joshua Wright is a senior technical analyst with Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through his experiences as a penetration tester, Josh has worked with hundreds of organizations on attacking and defending mobile devices and wireless systems, ethically disclosing significant product and protocol security weaknesses to well-known organizations. As an open-source software advocate, Josh has conducted cutting-edge research resulting in several software tools that are commonly used to evaluate the security of widely deployed technology targeting WiFi, Bluetooth, and ZigBee wireless systems, smart grid deployments, and the Android and Apple iOS mobile device platforms. As the technical lead of the innovative CyberCity, Josh also oversees and manages the development of critical training and educational missions for cyber warriors in the U.S. military, government agencies, and critical infrastructure providers.

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/virginia-beach-2018/courses](http://www.sans.org/event/virginia-beach-2018/courses)
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 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**

**Six-Day Program**
Sun, Aug 26 - Fri, Aug 31
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Carlos Cajigas

**Who Should Attend**
- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

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

Carlos Cajigas
SANS Certified Instructor
@Carlos_Cajigas

A native of San Juan, Puerto Rico, Carlos began his career with the West Palm Beach Police Department in Florida, first as a police officer and eventually as a digital forensics detective, examiner, and instructor specializing in computer crime investigations. During his law enforcement tenure, Carlos conducted examinations on hundreds of digital devices, from computers and mobile phones to GPS devices, and served as both a fact and expert witness. Today, Carlos is a senior incident response analyst at IBM, where he is responsible for responding to computer and network security threats for clients located in North and South America. In addition, he holds various certifications in the digital forensics field including EnCase Certified Examiner (ENCE), Certified Forensic Computer Examiner (CFCE) from IACIS, and the GIAC Certifications GCFE and GCFA.

Register at [www.sans.org/virginia-beach](http://www.sans.org/virginia-beach) | 301-654-SANS (7267)
FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting will help you to:

- Detect how and when a breach occurred
- Identify compromised and affected systems
- Determine what attackers took or changed
- Contain and remediate incidents
- Develop key sources of threat intelligence
- Hunt down additional breaches using knowledge of the adversary

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

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

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

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

Six-Day Program
Mon, Aug 20 - Sat, Aug 25
9:00am - 5:00pm
36 CPEs
Required Laptop
Instructor: Jake Williams

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

"FOR508 analyzes Advanced Persistent Threat samples that are affecting our industry today. This training can’t get any better!”
- Neel Mehta, Chevron

Jake Williams is a principal consultant at Rendition Infosec. He has more than a decade of experience in secure network design, penetration testing, incident response, forensics, and malware reverse engineering. He is well-versed in cloud forensics and previously developed a cloud forensics course for a U.S. government client. Jake regularly responds to cyber intrusions by state-sponsored actors in the financial, defense, aerospace, and healthcare sectors using cutting-edge forensics and incident response techniques. He often develops custom tools to deal with specific incidents and malware-reversing challenges. Additionally, Jake performs exploit development and has privately disclosed a multitude of zero day exploits to vendors and clients. He found vulnerabilities in one of the state counterparts to healthcare.gov and recently exploited antivirus software to perform privilege escalation.
FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

This course will enable you to 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 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 back on the job. We will cover the full spectrum of network evidence, 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 back on the job.

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. Previous SANS SEC curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS Forensics alumni from FOR500 (formerly FOR408) and FOR508 can take their existing knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same caliber of real-world problems without the use of disk or memory images.

Register at www.sans.org/virginia-beach | 301-654-SANS (7267)

Ryan Johnson
SANS Certified Instructor
@ForensicRJ

Six-Day Program
Sun, Aug 26 - Fri, Aug 31
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Ryan Johnson

Who Should Attend
- Incident response team members and forensicators
- Hunt team members
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- Anyone interested in computer network intrusions and investigations
- Security Operations Center personnel and information security practitioners

“This class teaches security pros how to boil the ocean. Every network-focused investigator should be taking this course.”

-Jacob Grant,
Arctic Wolf Networks

Ryan started out performing digital forensic exams for local law enforcement in Durham, N.C. That work led Ryan to join a team of media exploitation analysts working for the U.S. Army in Iraq. During his year in Iraq he helped gather actionable intelligence, streamline processes, and enhance equipment resources for in-country teams. When he returned stateside, Ryan began to work on computer intrusion cases. Since then he’s traveled the globe teaching digital forensics for the U.S. State Department’s Anti-Terrorism Assistance Program and served as a digital forensics analyst and consultant. Ryan co-authored several of the State Department’s digital forensics courses as well as the book Mastering Windows Network Forensics and Investigations, Second Edition. Ryan also currently serves as the Global Head of CSIRT at PricewaterhouseCoopers, where he leads the response, readiness and investigations functions.

Register at www.giac.org/gnfa

GNFA
Network Forensic Analyst
www.giac.org/gnfa

“ForensicRJ”
SANS Certified Instructor
www.giac.org/gnfa
GNFA
Network Forensic Analyst
www.giac.org/gnfa

6 Day Program
Sun, Aug 26 - Fri, Aug 31
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Ryan Johnson

Who Should Attend
- Incident response team members and forensicators
- Hunt team members
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- Anyone interested in computer network intrusions and investigations
- Security Operations Center personnel and information security practitioners

“This class teaches security pros how to boil the ocean. Every network-focused investigator should be taking this course.”

-Jacob Grant,
Arctic Wolf Networks

Ryan Johnson
SANS Certified Instructor
@ForensicRJ

Register at www.sans.org/virginia-beach | 301-654-SANS (7267)
This completely updated course is designed to empower advancing managers who want to 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. Lecture sections are intense; the most common student comment is that it’s like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

Essential security topics covered in this management track include network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, web application security, and offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression™ special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA’s CAQC program for Security+ 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

Knowledge Compression™
Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class that aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

G. Mark Hardy is founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 35 years, and is an internationally recognized expert and keynote speaker who has presented at over 250 events world-wide. He provides consulting services as a virtual CISO, expert witness testimony, and domain expertise in blockchain and cryptocurrency. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. He is a retired U.S. Navy captain who was entrusted with nine command assignments, including responsibility for leadership training for 70,000 sailors. A graduate of Northwestern University, he holds a B.S. in computer science, a B.A. in mathematics, a master’s degree in business administration, and a master’s degree in strategic studies, and holds the GSLC, CISSP®, CISM and CISA certifications.

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/virginia-beach-2018/courses
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.

MGT514 uses case studies from Harvard Business School, case scenarios, team-based exercises, and discussions that put students in real-world situations. You will be able to use these same activities with your own team members at 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.

Ted Demopoulos’ first significant exposure to computers was in 1977 when he had unlimited access to his high school’s PDP-11 and hacked at it incessantly. He consequently almost flunked out but learned he liked playing with computers a lot. His business pursuits began in college and have been continuous ever since. His background includes over 25 years of experience in information security and business, including 20+ years as an independent consultant. Ted helped start a successful information security company, was the CTO at a “textbook failure” of a software startup, and has advised several other businesses. Ted is a frequent speaker at conferences and other events, quoted often by the press, the recipient of a Department of Defense Award of Excellence, and the author of several books including the recent *Infosec Rock Star: How to Accelerate Your Career Because Geek Will Only Get You So Far*. In his spare time, he is also a food and wine geek, enjoys flyfishing and playing with his children.
This course covers how developers and security professionals can build and deliver secure software using DevOps and cloud services, specifically Amazon Web Services (AWS). It explains how principles, practices, and tools in DevOps and AWS can be leveraged to improve the reliability, integrity, and security of applications.

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

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

The course makes extensive use of open-source materials and tooling for automated configuration management (“Infrastructure as Code”), Continuous Integration, Continuous Delivery, Continuous Deployment, containerization, micro-segmentation, automated compliance (“Compliance as Code”), and Continuous Monitoring. This course also makes extensive use of AWS and associated developer tools such as CloudFormation, CodeCommit, CodeBuild, CodePipeline, and other cloud application services so students can experience how these services can be utilized in their applications.

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

-Devika Y., Bloomberg

Eric Johnson is a Principal Security Consultant at Cypress Data Defense, where he leads secure software development lifecycle consulting, web and mobile application penetration testing, secure code review assessments, static source code analysis, security research, and security tools development. He also founded the Puma Scan static analysis open-source project, which allows software engineers to run security-focused .NET static analysis rules during development and in continuous integration pipelines. For SANS, Eric authors application security courses on DevOps, cloud security, secure coding, and defending mobile apps. He serves on the advisory board for the SANS Securing the Human Developer awareness training program, delivers security training around the world, and has presented his security research at such conferences as BlackHat, OWASP, BSides, JavaOne, UberConf, and ISSA. Eric has a bachelor of science degree in computer engineering and a master of science degree in information assurance from Iowa State University, and currently holds the CISSP®, GWAPT, GSSP-.NET, and GSSP-Java certifications.
Enrich your SANS training experience! Evening talks by our instructors and selected subject-matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.

KEYNOTE (WEEK 1): **InfoSec State of the Union**
Jake Williams
In this presentation Jake will address current topics in cybersecurity discussing the intersection of tech, policy, and ethics. Because it’s impossible to know what will be in the news as we go to print with these abstracts, talk to Jake for an up-to-date list of what he’ll be discussing in this session. Past sessions have addressed hacking cases, data breaches, impact of nation-state malware leaks, hacking the voting system, and state-sponsored cyber espionage.

(WEEK 1): **Continuous Security: Monitoring & Active Defense in the Cloud**
Eric Johnson
Monitoring and feedback loops from production is a critical tenant in DevOps for measuring performance, runtime errors, statistics, and changes. In the SecDevOps world, security teams can take advantage of DevOps monitoring tools to increase security visibility, identify anomalies, and respond swiftly to real-time attacks. Cloud providers are offering powerful infrastructure, development, and application continuous monitoring services that generate a wealth of data. But, building continuous security monitoring on top of the data can be challenging. Where are the log files? What is the log file format? What security events are captured? How do we display meaningful metrics? Can we detect and defend in real time? This talk will introduce attendees to a realistic Amazon Web Service environment’s monitoring and active defense system and discuss real data collected during a war game exercise. Afterwards, we will walk through the postmortem, review the alerts raised during the incident, determine if there were any surprises, and identify opportunities to improve the system. Attendees will walk away with actionable techniques for building an active defense framework to help protect your organization’s cloud resources.

(WEEK 1): **Automating NIST Risk Management Framework (RMF)/800-53**
Peter Szczepankiewicz
Doing good Cybersecurity is so much more than inspection compliance. We’ve all seen it. You’re 100% compliant and can still get hacked! But after decades of gathering security information from your global enterprise, measured in gross tonnage, the converse is also true. Weighed down with lakes of data, very interesting things start to happen when you view portions of your data through the lens of the NIST Risk Management Framework. You realize that there are phantom scripts running around in your network, written by our own staff. People on vacation have accounts that are somehow still actively logging in and out, from many VPNs! Your vulnerabilities, coupled with your outbound packets reveal file-less malware that doesn’t use command and control. As a standard course of action, one should be detecting violations in real time, as well as searching with this lens. Come learn about specific real-time correlation rules that your peers are using for NIST RMF and join in this discussion about what is working in the field. While not all of NIST RMF can be automated, what can be automated should be automated.

(WEEK 1): **Blockchain: The New Digital Swiss Army Knife?**
G. Mark Hardy
Blockchain as a technology has been proposed as a solution to everything from frictionless currency transfer to tracking cargo on ships. With over $1 billion in venture funds invested and several hundred patents filed, every security professional must know the impact on organizations in terms of risk, volatility, and competitiveness. This talk will explore alternative uses for blockchain technology other than cryptocurrency, and provide a framework for utilizing and securing a technology considered as disruptive as the Internet was in the 1990s.
KEYNOTE (WEEK 2): Actionable Detects: Blue Team Cyber Defense Tactics
Seth Misenar
Organizations relying on third parties to detect breaches can go almost a full year before finding out they have been compromised. Detect the breach yourself, and on average you will find it within about a month of the initial occurrence. Considering detection and defense against modern adversaries too costly to perform yourself can be a very expensive miscalculation considering the substantially increased price of response and recovery with breach duration. Seth Misenar’s ever-evolving, Actionable Detects presentation, provides you with thoughts, tactics, techniques, and procedures to once again take pride in your Blue Team Cyber capabilities. Not applying these lessons learned could prove costly in the face of adapting threat actors. Dig in and learn to hold your head high when talking about your defensive cyber operations capabilities.

(WEEK 2): Stuck in the Box, a SIEM’s Tale
Justin Henderson
Organizations often spend excessive amounts of money on SIEM products only to end up with a log collection box when they thought they purchased a tactical detection system. Most organizations find themselves with a SIEM but unsure how to use its capabilities. Point solutions are quick to defend deficiencies by stating each environment is different so you, the customer, must tell them what you want the SIEM to do and then they’ll help with professional services or by replacing your current SIEM with something “better and more advanced.” This is complete hogwash. Organizations tend to have a lot of overlap such as the use of Windows systems or network protocols such as DNS. As such there are high fidelity detects that can be implemented in every organization. Enough is enough. If you are looking for techniques and methods to get value out of your current SIEM or are interested in seeing how a new open-source big data solution such as the Elastic Stack (formerly ELK) most likely can beat what you have today, then this talk is for you. Fact is that it is time to think outside the box. Come find out how one organization spent 14 months deploying a top magic quadrant SIEM solution only to have it beaten by ELK in two weeks.

(WEEK 2): So, You Want To Be An Infosec Consultant?
Ted Demopoulos
Becoming a successful consultant seems like a dream: high pay, freedom, and fascinating work. These can all be true yet there is more to the reality: as a consultant you are running a business and you need clients! This session covers what those considering consulting need to know, including starting the business, getting clients, pricing, and much more. Whether you as aspire to consulting full time or you want to keep your job and consult on the side, we cover the basics you need to know to get started.

(WEEK 2): OODA Security: Taking Back the Advantage
Kevin Fiscus
OODA, or Observe, Orient, Decide and Act, is a concept first developed for fighter pilots. The concept states that the adversary who can effectively complete the OODA cycle first will go home while the adversary who takes longer enjoys, at best, a long, slow parachute ride to the ground. This concept can be applied to information security. In theory, we defenders should have the advantage as it is our “house” the attackers are attacking. Unfortunately, that is rarely the case. Over 50% of organizations find out they have been compromised via notification by a third party, meaning that all too often defenders don’t even start their OODA loop until after the attacker has completed the compromise. Making things worse, traditional security controls are failing us because attackers already know how to circumvent or evade them. Fortunately, there is a solution. By making better use of our existing technology and by using some of the attackers’ tools and techniques against them, we can deter, distract, delay, disrupt and detect them. Come learn how we can turn the tables on the bad guys and reclaim the OODA loop initiative.

Register at www.sans.org/virginia-beach | 301-654-SANS (7267)
Future Training Events

Rocky Mountain Denver, CO Jun 4-9
Crystal City Arlington, VA Jun 18-23
Minneapolis Minneapolis, MN Jun 25-30
Vancouver Vancouver, BC Jun 25-30
Charlotte Charlotte, NC Jul 9-14

SANSFIRE Washington, DC Jul 14-21

Boston Summer Boston, MA Aug 6-11
San Antonio San Antonio, TX Aug 6-11
New York City Summer New York, NY Aug 13-18
Northern VA – Alexandria Alexandria, VA Aug 13-18
Virginia Beach Virginia Beach, VA Aug 20-31
Chicago Chicago, IL Aug 20-25
San Francisco Summer San Francisco, CA Aug 26-31
Tampa-Clearwater Tampa, FL Sep 4-9
Baltimore Fall Baltimore, MD Sep 10-15

Network Security Las Vegas, NV Sep 23-28

Northern VA Fall – Tysons Tysons, VA Oct 13-20
Denver Denver, CO Oct 15-20
Seattle Fall Seattle, WA Oct 15-20
Houston Houston, TX Oct 29 - Nov 3
Dallas Fall Dallas, TX Nov 5-10
San Diego Fall San Diego, CA Nov 12-17
Austin Austin, TX Nov 26 - Dec 1

Future Summit Events

DFIR Austin, TX Jun 7-14
Security Awareness Charleston, SC Aug 6-15
Data Breach New York City, NY Aug 20-27
Threat Hunting & Incident Response New Orleans, LA Sep 6-13
Alaska Anchorage, AK Sep 10-15
Oil & Gas Cybersecurity Houston, TX Oct 1-6
Secure DevOps Denver, CO Oct 22-29
Pen Test HackFest Bethesda, MD Nov 12-19

Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit www.sans.org/community for up-to-date Community course information.
Due to a high demand for security training at SANS Virginia Beach 2018, courses will be held at both the Hilton Virginia Beach Oceanfront and Hilton Garden Inn Virginia Beach Oceanfront. The hotels are less than a five minute walk from one another, and are accessible from both the Boardwalk and Atlantic Avenue. In order to maximize the availability of training, SANS will announce specific course locations closer to the start of the event.

www.sans.org/event/virginia-beach-2018/location

Hilton Virginia Beach Oceanfront
3001 Atlantic Avenue
Virginia Beach, VA 23451
757-213-3000

Hilton Garden Inn Virginia Beach
Oceanfront
3315 Atlantic Avenue
Virginia Beach, VA 23451
855-618-4697

Special Hotel Rates Available
A special discounted rate of $207.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. These rates include high-speed Internet in your room and are only available through 5pm EST on July 20, 2018.

Register online at www.sans.org/virginia-beach

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

Select your course and indicate whether you plan to test for GIAC certification. If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Use code EarlyBird18 when registering early

Pay Early and Save*

Pay & enter code by
DATE  DISCOUNT
7-4-18  $400.00
7-25-18  $200.00

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

SANS Voucher Program
Expand your training budget!
Extend your fiscal year. The SANS Voucher Program provides flexibility and may earn you bonus funds for training.

www.sans.org/vouchers

Cancellation & Access Policy
If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply. All substitution requests must be submitted by email to registration@sans.org.

If an attendee must cancel and no substitute is available, a refund can be issued for any received payments by August 1, 2018. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.
Join the SANS.org community today to enjoy these free resources at www.sans.org/account

Newsletters

NewsBites
Twice-weekly, high-level executive summaries of the most important news relevant to cybersecurity professionals.

OUCH!
The world’s leading monthly free security awareness newsletter designed for the common computer user.

@RISK: The Consensus Security Alert
A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data.

Webcasts

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

Analyst Webcasts
A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

WhatWorks Webcasts
The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT security issues.

Tool Talks
Tool Talks are designed to give you a solid understanding of a problem, and how a vendor’s commercial tool can be used to solve or mitigate that problem.

Other Free Resources (No SANS account is necessary)

- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQs
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

Save $400 when you pay for any 4-, 5-, or 6-day course and enter the code “EarlyBird18” by June 13th. www.sans.org/boston-summer

5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

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

To be removed from future mailings, please contact unsubscribe@sans.org or (301) 654-SANS (7267). Please include name and complete address. NALT-BRO-Boston-2018