San Diego
Fall 2018
November 12-17

Protect Your Business | Advance Your Career

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

See inside for courses and GIAC certifications in:
- Cyber Defense
- Monitoring and Detection
- SIEM
- CISSP® Preparation

PLUS NEW COURSES
- Defensible Security Architecture
- Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses

“SANS provides top-notch, comprehensive training taught by knowledgeable and experienced instructors.”
- Shawn Pray, Accenture

SAVE $400
Register and pay by Sep 19th
Use code EarlyBird18

www.sans.org/san-diego-fall
Our mission at SANS is to deliver cutting-edge information security knowledge and skills to all students in order to protect people and assets. At the heart of everything we do is the SANS Promise: Students will be able to use the new skills they have learned as soon as they return to work. See that promise in action at SANS San Diego Fall 2018.

Take advantage of these opportunities to get the most out of your training:

- Distinguish yourself as an information security leader by preparing for your GIAC Certification.
- Challenge your skills during two nights at Cyber Defense NetWars Tournament (FREE with any 5- to 6-day SANS course registration).
- Network with like-minded security professionals facing similar challenges.
- Attend evening bonus sessions led by SANS instructors and gain insight into the latest cybersecurity topics.
- Extend your SANS course by four months with an OnDemand Bundle.

Don’t miss this opportunity to network with like-minded peers, and dive into timely, effective security training. Gain valuable insight into today’s top cybersecurity threats and be better armed to defend your environment. Choose your course and register now.

### Courses at a Glance

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td>Introduction to Cyber Security</td>
<td>Page 4</td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials Bootcamp Style</td>
<td>Page 5</td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>Page 6</td>
</tr>
<tr>
<td>SEC505</td>
<td>Securing Windows and PowerShell Automation</td>
<td>Page 7</td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td>Page 8</td>
</tr>
<tr>
<td>SEC530</td>
<td>Defensible Security Architecture</td>
<td>Page 9</td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics</td>
<td>Page 10</td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>Page 11</td>
</tr>
<tr>
<td>SEC599</td>
<td>Defeating Advanced Adversaries – Purple Team Tactics &amp; Kill Chain Defenses</td>
<td>Page 12</td>
</tr>
<tr>
<td>MGT414</td>
<td>SANS Training Program for CISSP® Certification</td>
<td>Page 13</td>
</tr>
</tbody>
</table>

Available via Simulcast

### Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 15.

**General Session – Welcome to SANS** – Bryan Simon

**KEYNOTE:** Windows Exploratory Surgery with Process Hacker – Jason Fossen

**Zero Trust Architecture** – Justin Henderson

**CYBER DEFENSE NETWARS TOURNAMENT**

Two nights: November 15th & 16th
Hosted by Seth Misenar
Learn more on page 14.

Save $400 when you register and pay by Sept 19th using code EarlyBird18

Register today for SANS San Diego Fall 2018! www.sans.org/san-diego-fall
SANS Faculty

A revered faculty of cybersecurity specialists author and teach SANS courses, which is why so many professionals choose SANS training again and again, year after year.

Just over 90 individuals are currently qualified to hold the title SANS Certified Instructor. They are the founders of international cybersecurity organizations, the authors of top-selling information security books, developers of the most advanced cyber ranges and CTF challenges, and they are called on to share their expertise with government and commercial organizations around the world regularly.

Whether you will train with us live at an event or online, SANS guarantees that you will be able to apply what you learn from our instructors and training as soon as you return to work.

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

Ron Foupht, Sirius Computer Solutions

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 short memo and/or a few PowerPoint slides).

• Provide all the necessary information in one place, including copies of the Training Roadmap, instructor bio, Why SANS? summary pages, and a list of additional benefits offered at our live events or online.

Be specific

• How does the course relate to the job you need to be doing? Are you establishing baseline skills? Transitioning to a more focused role? Decision makers need to understand the plan and context.

• Highlight the specifics of what you’ll be able to do after training. Each SANS course description includes a section titled “You Will Be Able To.” Be sure to include this in your request to make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Establish longer-term expectations

• Information security is a specialized career path within IT, with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense—not a once-and-done item.

• Take a GIAC Certification exam to prove the training worked. Employers value the validation of skills and knowledge that a GIAC Certification provides. Exams are psychometrically designed to establish competency for related job tasks.

• Consider offering trade-offs for the investment. Many professionals build annual training expenses into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.
Extend and Validate Your Training

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

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

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

“Special Pricing
Bundle OnDemand or GIAC with your course before Oct 1st and save $40!
GIAC and OnDemand Bundle price before Oct 1st: $729
GIAC and OnDemand Bundle price on or after Oct 1st: $769

“The course content and OnDemand delivery method have both exceeded my expectations.”
-Robert Jones, Team Jones, Inc.

“GIAC is the only certification that proves you have hands-on technical skills.”
-Christina Ford, Department of Commerce

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

*GIAC and OnDemand Bundles are only available for certain courses.
To determine if SANS SEC301: Introduction to Cyber Security is right for you, ask yourself five simple questions:

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

If you answer yes to any of these questions, then the SEC301: Introduction to Cyber Security training course is for you. Students with a basic knowledge of computers and technology but no prior cybersecurity experience can jump-start their security education with insight and instruction from real-world security experts in SEC301. This completely revised and comprehensive five-day course covers a wide range of baseline topics, including terminology, the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles. The hands-on, step-by-step learning format will enable you to grasp all the information presented even if some of the topics are new to you. You’ll learn fundamentals of cybersecurity that will serve as the foundation of your security skills and knowledge for years to come. Written by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next SANS course in this progression, SEC401: Security Essentials Bootcamp Style. It also delivers on the SANS promise: You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.

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

-Sandy Baguskas, John Hancock
Who Should Attend
- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic specialists, penetration testers, and auditors who need a solid foundation of security principles to be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

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

Is SEC401: Security Essentials Bootcamp Style the right course for you? STOP and ask yourself the following questions:
- Do you fully understand why some organizations get compromised and others do not?
- If there were compromised systems on your network, are you confident that you would be able to find them?
- Do you know the effectiveness of each security device and are you certain that they are all configured correctly?
- Are proper security metrics set up and communicated to your executives to drive security decisions?

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

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

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

Prevention is ideal but detection is a must.

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

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you will need if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.
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.
SEC505: Securing Windows and PowerShell Automation

Six-Day Program
Mon, Nov 12 - Sat, Nov 17
9:00am - 5:00pm
36 CPEs
Laptop Required

Who Should Attend
- Security Operations personnel
- Blue Team players who were terrified by SEC504
- Windows endpoint and server administrators
- Anyone who wants to learn PowerShell automation
- Anyone implementing the NSA Top 10 Mitigations
- Anyone implementing the CIS Critical Security Controls
- DoD admins applying the NSA/DISA Secure Host Baseline
- Individuals deploying or managing a PKI or smart cards
- Anyone wanting a more rugged Windows architecture

Hackers know how to use PowerShell for evil. Do you know how to use it for good? In SEC505 you will learn PowerShell and Windows security hardening at the same time. SecOps/DevOps requires automation, and Windows automation means PowerShell.

You’ve run a vulnerability scanner and applied patches – now what? A major theme of this course is defensible architecture: we have to assume that there will be a breach, so we need to build in damage control from the beginning. Whack-a-mole incident response cannot be our only defensive strategy – we’ll never win, and we’ll never get ahead of the game. By the time your monitoring system tells you a Domain Admin account has been compromised, IT’S TOO LATE.

For the assume-breach mindset, we must carefully delegate limited administrative powers so that the compromise of one administrator account is not a disaster across the board. Managing administrative privileges and credentials is a tough problem, so this course devotes an entire day to just this one critical task. Perhaps you’ve taken a hacking course at SANS and you now want to learn Windows mitigations: SEC505 is that course. SEC505 is the defense-only mirror image of SEC504 with regard to Windows and Active Directory.

Learning PowerShell is also useful for another kind of security: job security. Employers are looking for people with these skills. You don’t have to know any PowerShell to attend the course, we will learn it together. About half the labs during the week are PowerShell, while the rest use graphical security tools. Many of the PowerShell scripts written by the course author are available to download from GitHub for free.

This course is not a vendor show to convince you to buy another security appliance or to install yet another endpoint agent. The idea is to use built-in or free Windows and Active Directory security tools when we can (especially PowerShell and Group Policy) and then purchase commercial products only when absolutely necessary.

If you are an IT manager or CIO, the aim for this course is to have it pay for itself 10 times over within two years, because automation isn’t just good for SecOps/DevOps; it can save money too.

This course is designed for systems engineers, security architects, and the Security Operations (SecOps) team. The focus of the course is on how to automate the NSA Top 10 Mitigations and the CIS Critical Security Controls related to Windows, especially the ones that are difficult to implement in large environments.

SEC505 will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) certification exam to prove your Windows security expertise. The GCWN certification counts towards a Master’s Degree in Information Security from the SANS Technology Institute (www.sans.edu) and satisfies the Department of Defense 8140 computing environment requirement. The GCWN is also a foundational certification for soldiers in the U.S. Army’s 255-S Information Protection Program. For DoD students, we will see how to apply the NSA/DISA Secure Host Baseline.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. We don’t cover patch management, share permissions, or other such basics – the aim is to go far beyond that. Come have fun learning PowerShell and Windows security at the same time!

Jason Fossen
SANS Faculty Fellow
@JasonFossen

Jason Fossen is a principal security consultant at Enclave Consulting LLC, a published author, and a frequent public speaker on Microsoft security issues. He is the sole author of the SANS week-long Securing Windows course (SEC505), maintains the Windows day of Security Essentials (SEC401.5), and has been involved in numerous other SANS projects since 1998. He graduated from the University of Virginia, received his master’s degree from the University of Texas at Austin, and holds a number of professional certifications. He currently lives in Dallas, Texas.
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)

“The course offers invaluable insight into not only the ‘what’ of monitoring, but also the ‘why’ – highly recommended!”
-Jason Nickola, DTS

Seth Misenar is the founder of and lead consultant for Context Security, a Jackson, Mississippi-based company that provides information security thought leadership, independent research, and security training. Seth’s background includes network and web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as both a physical and network security consultant for Fortune 100 companies, as well as the Health Insurance Portability and Accountability Act, and as information security officer for a state government agency. Prior to becoming a security geek, Seth received a bachelor’s degree in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is no stranger to certifications and thus far has achieved credentials that include the CISSP®, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE.
Architecture is designed to help students build and maintain a truly defensible security architecture. "The perimeter is dead" is a favorite saying in this age of mobile, cloud, and the Internet of Things. We are indeed living in a new world of "de-perimeterization" where the old boundaries of "inside" and "outside" or "trusted" and "untrusted" no longer apply.

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

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

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

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

You Will Learn To:

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

John Hubbard
SANS Instructor @SecHubb

John is a dedicated blue-teamer and is driven to help develop defensive talent around the world. Through his years of experience as the SOC Lead for GlaxoSmithKline, he has real-world, first-hand knowledge of what it takes to defend an organization against advanced cyber-attacks and is eager to share these lessons with his students. As a SANS Cyber Defense curriculum instructor and course author of SEC455, John specializes in threat hunting, network security monitoring, SIEM design and optimization, and constructing defensive postures that allow organizations to protect their most sensitive data. Throughout class, he works with students to explain difficult concepts in relatable and clear language, illustrates important ideas with stories and demonstrations, and encourages students to push themselves beyond the limit of what they thought possible. John holds degrees in electrical and computer engineering and his past research ranges from malware reverse-engineering to car hacking, mobile app security, and IoT devices. In his free time, John enjoys catching every InfoSec conference he can attend, FPV drone racing, coffee roasting, and slowly turning his home into a data center.
Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

As threats evolve, an organization’s security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course that teaches students the Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle. The British government’s Center for the Protection of National Infrastructure describes the Controls as the “baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence.”

SANS in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

The course shows security professionals how to implement the Controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.
Six-Day Program  
Mon, Nov 12 - Sat, Nov 17  
9:00am - 5:00pm  
36 CPEs  
Laptop Required  

Who Should Attend  
- 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

You just got hired to help our virtual organization “SyncTechLabs” build out a cybersecurity capability. On your first day, your manager tells you: “We looked at some recent cybersecurity trend reports and we feel like we’ve lost the plot. Advanced persistent threats, ransomware, denial of service...we’re not even sure where to start!”

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

SEC599 aims to leverage the purple team concept by bringing together red and blue teams for maximum effect. Recognizing that a prevent-only strategy is not sufficient, the course focuses on current attack strategies and how they can be effectively mitigated and detected using a Kill Chain structure.

Throughout the course, the purple team principle will be maintained, where attack techniques are first explained in-depth, after which effective security controls are introduced and implemented.

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

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

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

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

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

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

Erik Van Buggenhout is the lead author of SEC599: Defeating Advanced Adversaries. In addition, Erik teaches SEC560: Network Penetration Testing and Ethical Hacking and SEC442: Web Application Penetration Testing and Ethical Hacking. He has been involved with SANS since 2009, starting as a Mentor, working his way to Community Instructor in 2012, and finally becoming a Certified Instructor in 2016. Erik loves explaining deeply technical concepts by using war stories, adding a few funny anecdotes here and there. As testimony to his technical expertise, he has obtained the GSE, GCIA, GNFA, GPEN, GWAPT, GCIH, and GSEC certifications. In addition to his work with SANS, Erik is the co-founder of the Belgian firm NVISO, which focuses on high-end cybersecurity services, specializing in government, defense and the financial sector. Together with his team of 20+ technical experts, Erik delivers a wide array of technical security services, including penetration testing, security monitoring and incident response. Prior to NVISO, Erik spent five years at Big 4 firm, starting as a junior penetration tester and evolving into a subject-matter expert for the EMEA region.

Erik is a self-confessed speed walker, so if you see him rushing around at a conference, feel free to stop him and say “Hi”

Register at www.sans.org/san-diego-fall | 301-654-SANS (7267)

Erik Van Buggenhout  
SANS Certified Instructor  
@ErikVaBu

SANS Technology Institute  
www.sans.edu

Bundle OnDemand with this course

NEW!

GDAT  
Defending Advanced Threats  
www.giac.org/gdat
David R. Miller has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on information systems security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security programs. He serves as a security lead and forensic investigator on numerous enterprise-wide IT design and implementation projects for Fortune 500 companies, providing compliance, security, technology, and architectural recommendations and guidance. Projects David has worked on include Microsoft Windows Active Directory enterprise designs, security information and event management systems, intrusion detection and protection systems, endpoint protection systems, patch management systems, configuration monitoring systems, and enterprise data encryption for data at rest, in transit, in use, and within email systems. David is an author, lecturer and technical editor of books, curriculum, certification exams, and computer-based training videos.

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

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

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/san-diego-fall-2018/courses
Come and join us for these exciting events to test your skills in a challenging and fun learning environment.

*CYBER DEFENSE NETWARS IS FREE OF CHARGE TO ALL STUDENTS AT SANS SAN DIEGO FALL 2018.*

www.sans.org/san-diego-fall

Two FREE Nights of Cyber Defense NetWars at SANS San Diego Fall 2018!*

NOVEMBER 15 & 16 7:15 – 10:15 PM

The all-new Cyber Defense NetWars challenge is a defense-focused competition that test your ability to solve problems and secure your systems from compromise. It’s a truly unique experience, and an opportunity to prove your skills in Administration, Threat Hunting, Log Analysis, Packet Analysis, Cryptography, and much more.

The SANS Cyber Defense NetWars Experience:

- Takes place in an interactive, Internet-based environment where you’ll secure systems and detect compromises
- Is accessible for a broad range of skill levels
- Is split into separate levels so players may quickly advance through earlier levels to the level of their expertise

Come and join us for these exciting events to test your skills in a challenging and fun learning environment.

*CYBER DEFENSE NETWARS IS FREE OF CHARGE TO ALL STUDENTS AT SANS SAN DIEGO FALL 2018.*
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.

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

Keynote: Windows Exploratory Surgery with Process Hacker
Jason Fossen
In this talk, Jason Fossen, SANS Institute Fellow and SEC505 author, will rummage around inside the guts of Windows while on the lookout for malware, using a free tool named Process Hacker (similar to Process Explorer, but open source). Understanding processes, threads, drivers, handles, and other OS internals is important for analyzing malware, understanding exploits, doing forensics, troubleshooting, and hardening the OS. If you have a laptop, get Process Hacker from http://processhacker.sourceforge.net and together we’ll take a peek under the GUI to learn about Windows internals. This talk also helps to prepare attendees for several of the courses at the conference by presenting key OS concepts like virtual memory, modules, security access tokens, and more.

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

“SANS is by far the best InfoSec training available in the world. Every instructor I have encountered are straight up superstars!”
- Brian Bailey, West Virginia State Treasurer’s Office

“SANS provides a vast amount of knowledge presented by industry professionals who can do the work, and not just hide behind teaching it.”
- Carl Frey, Jockey International
## Future Training Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>San Francisco Summer</td>
<td>San Francisco, CA</td>
<td>Aug 26-31</td>
</tr>
<tr>
<td>Tampa-Clearwater</td>
<td>Tampa, FL</td>
<td>Sep 4-9</td>
</tr>
<tr>
<td>Baltimore Fall</td>
<td>Baltimore, MD</td>
<td>Sep 8-15</td>
</tr>
</tbody>
</table>

### Network Security

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Northern VA Fall – Tysons</td>
<td>McLean, VA</td>
<td>Oct 13-20</td>
</tr>
<tr>
<td>Denver</td>
<td>Denver, CO</td>
<td>Oct 15-20</td>
</tr>
<tr>
<td>Seattle Fall</td>
<td>Seattle, WA</td>
<td>Oct 15-20</td>
</tr>
<tr>
<td>Houston</td>
<td>Houston, TX</td>
<td>Oct 29 - Nov 3</td>
</tr>
<tr>
<td>Dallas Fall</td>
<td>Dallas, TX</td>
<td>Nov 5-10</td>
</tr>
<tr>
<td>DFI RCON Miami</td>
<td>Miami, FL</td>
<td>Nov 5-10</td>
</tr>
<tr>
<td>San Diego Fall</td>
<td>San Diego, CA</td>
<td>Nov 12-17</td>
</tr>
<tr>
<td>Austin</td>
<td>Austin, TX</td>
<td>Nov 26 - Dec 1</td>
</tr>
<tr>
<td>San Francisco Fall</td>
<td>San Francisco, CA</td>
<td>Nov 26 - Dec 1</td>
</tr>
<tr>
<td>Nashville</td>
<td>Nashville, TN</td>
<td>Dec 3-8</td>
</tr>
<tr>
<td>Santa Monica</td>
<td>Santa Monica, CA</td>
<td>Dec 3-8</td>
</tr>
</tbody>
</table>

### Cyber Defense Initiative

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sonoma</td>
<td>Santa Rosa, CA</td>
<td>Jan 14-19, 2019</td>
</tr>
<tr>
<td>Miami</td>
<td>Miami, FL</td>
<td>Jan 21-26</td>
</tr>
<tr>
<td>Las Vegas</td>
<td>Las Vegas, NV</td>
<td>Jan 28 - Feb 2</td>
</tr>
</tbody>
</table>

### Security East

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Breach</td>
<td>New York City, NY</td>
<td>Aug 20-27</td>
</tr>
<tr>
<td>Threat Hunting &amp; Incident Response</td>
<td>New Orleans, LA</td>
<td>Sep 6-13</td>
</tr>
<tr>
<td>Alaska</td>
<td>Anchorage, AK</td>
<td>Sep 10-15</td>
</tr>
<tr>
<td>Oil &amp; Gas Cybersecurity</td>
<td>Houston, TX</td>
<td>Oct 1-6</td>
</tr>
<tr>
<td>Secure DevOps</td>
<td>Denver, CO</td>
<td>Oct 22-29</td>
</tr>
<tr>
<td>Pen Test HackFest</td>
<td>Bethesda, MD</td>
<td>Nov 12-19</td>
</tr>
<tr>
<td>Tactical Detection and Data Analytics</td>
<td>Scottsdale, AZ</td>
<td>Dec 4-11</td>
</tr>
<tr>
<td>Cyber Threat Intelligence</td>
<td>Bethesda, MD</td>
<td>Jan 21-28, 2019</td>
</tr>
</tbody>
</table>

## Future Summit Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Breach</td>
<td>New York City, NY</td>
<td>Aug 20-27</td>
</tr>
<tr>
<td>Threat Hunting &amp; Incident Response</td>
<td>New Orleans, LA</td>
<td>Sep 6-13</td>
</tr>
<tr>
<td>Alaska</td>
<td>Anchorage, AK</td>
<td>Sep 10-15</td>
</tr>
<tr>
<td>Oil &amp; Gas Cybersecurity</td>
<td>Houston, TX</td>
<td>Oct 1-6</td>
</tr>
<tr>
<td>Secure DevOps</td>
<td>Denver, CO</td>
<td>Oct 22-29</td>
</tr>
<tr>
<td>Pen Test HackFest</td>
<td>Bethesda, MD</td>
<td>Nov 12-19</td>
</tr>
<tr>
<td>Tactical Detection and Data Analytics</td>
<td>Scottsdale, AZ</td>
<td>Dec 4-11</td>
</tr>
<tr>
<td>Cyber Threat Intelligence</td>
<td>Bethesda, MD</td>
<td>Jan 21-28, 2019</td>
</tr>
</tbody>
</table>

## Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit [www.sans.org/community](http://www.sans.org/community) for up-to-date Community course information.
Register online at www.sans.org/san-diego-fall
We recommend registering early to get your first choice of courses.
Select your course and indicate whether you plan to test for GIAC certification. If the course is still open, the secure, online server will accept your registration. Sold-out courses will be removed from the online registration. Everyone must complete the online registration form. We do not take registrations by phone.

Cancellation & Access Policy
If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply. All substitution requests must be submitted by email to registration@sans.org.
If an attendee must cancel and no substitute is available, a refund can be issued for any received payments by October 24, 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.

Pay Early and Save*
Use code EarlyBird18 when registering early

<table>
<thead>
<tr>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>9-19-18</td>
<td>$400</td>
<td>10-10-18</td>
<td>$200</td>
</tr>
</tbody>
</table>

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

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

SANS Simulcast
is available from San Diego Fall 2018
To register for a Simulcast course, please visit www.sans.org/event/san-diego-fall-2018/attend-remotely

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

Special Hotel Rates Available
A special discounted rate of $241 S/D will be honored based on space availability.
Government per diem rooms at the prevailing rate are available with proper ID. These rates include high-speed Internet in your room and are only available through October 12, 2018.

Top 3 reasons to stay at the Hard Rock Hotel San Diego
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Hard Rock Hotel San Diego, you can further network with your industry peers and remain in the center of the activity surrounding the training event.
3. SANS schedules morning and evening events at the Hard Rock Hotel San Diego that you won’t want to miss!

There’s something electric about being in the middle of it all. Hard Rock Hotel San Diego puts you in the limelight with chic accommodations in the heart of downtown and the famed nightlife of the Gaslamp Quarter. And you can live it up without ever leaving the hotel – try a jam session in your suite with our complimentary Sound- of-Your-Stay service, or mouthwatering sushi at world-famous Nobu and rooftop cocktails at Float rooftop lounge or 207 Bar.

Hotel Information
Hard Rock Hotel San Diego
207 Fifth Avenue
San Diego, CA  92101
619-702-3000
www.sans.org/event/san-diego-fall-2018/location

There’s something electric about being in the middle of it all. Hard Rock Hotel San Diego puts you in the limelight with chic accommodations in the heart of downtown and the famed nightlife of the Gaslamp Quarter. And you can live it up without ever leaving the hotel – try a jam session in your suite with our complimentary Sound- of-Your-Stay service, or mouthwatering sushi at world-famous Nobu and rooftop cocktails at Float rooftop lounge or 207 Bar.

Special Hotel Rates Available
A special discounted rate of $241 S/D will be honored based on space availability.
Government per diem rooms at the prevailing rate are available with proper ID. These rates include high-speed Internet in your room and are only available through October 12, 2018.

Top 3 reasons to stay at the Hard Rock Hotel San Diego
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Hard Rock Hotel San Diego, you can further network with your industry peers and remain in the center of the activity surrounding the training event.
3. SANS schedules morning and evening events at the Hard Rock Hotel San Diego that you won’t want to miss!

There’s something electric about being in the middle of it all. Hard Rock Hotel San Diego puts you in the limelight with chic accommodations in the heart of downtown and the famed nightlife of the Gaslamp Quarter. And you can live it up without ever leaving the hotel – try a jam session in your suite with our complimentary Sound-of-Your-Stay service, or mouthwatering sushi at world-famous Nobu and rooftop cocktails at Float rooftop lounge or 207 Bar.

Special Hotel Rates Available
A special discounted rate of $241 S/D will be honored based on space availability.
Government per diem rooms at the prevailing rate are available with proper ID. These rates include high-speed Internet in your room and are only available through October 12, 2018.

Top 3 reasons to stay at the Hard Rock Hotel San Diego
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Hard Rock Hotel San Diego, you can further network with your industry peers and remain in the center of the activity surrounding the training event.
3. SANS schedules morning and evening events at the Hard Rock Hotel San Diego that you won’t want to miss!

There’s something electric about being in the middle of it all. Hard Rock Hotel San Diego puts you in the limelight with chic accommodations in the heart of downtown and the famed nightlife of the Gaslamp Quarter. And you can live it up without ever leaving the hotel – try a jam session in your suite with our complimentary Sound-of-Your-Stay service, or mouthwatering sushi at world-famous Nobu and rooftop cocktails at Float rooftop lounge or 207 Bar.

Special Hotel Rates Available
A special discounted rate of $241 S/D will be honored based on space availability.
Government per diem rooms at the prevailing rate are available with proper ID. These rates include high-speed Internet in your room and are only available through October 12, 2018.

Top 3 reasons to stay at the Hard Rock Hotel San Diego
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Hard Rock Hotel San Diego, you can further network with your industry peers and remain in the center of the activity surrounding the training event.
3. SANS schedules morning and evening events at the Hard Rock Hotel San Diego that you won’t want to miss!

There’s something electric about being in the middle of it all. Hard Rock Hotel San Diego puts you in the limelight with chic accommodations in the heart of downtown and the famed nightlife of the Gaslamp Quarter. And you can live it up without ever leaving the hotel – try a jam session in your suite with our complimentary Sound-of-Your-Stay service, or mouthwatering sushi at world-famous Nobu and rooftop cocktails at Float rooftop lounge or 207 Bar.

Special Hotel Rates Available
A special discounted rate of $241 S/D will be honored based on space availability.
Government per diem rooms at the prevailing rate are available with proper ID. These rates include high-speed Internet in your room and are only available through October 12, 2018.

Top 3 reasons to stay at the Hard Rock Hotel San Diego
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Hard Rock Hotel San Diego, you can further network with your industry peers and remain in the center of the activity surrounding the training event.
3. SANS schedules morning and evening events at the Hard Rock Hotel San Diego that you won’t want to miss!
Newsletters

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

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

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

Webcasts

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

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

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

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

Other Free Resources (SANS.org account not required)

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

Save $400 when you pay for any 4-, 5-, or 6-day course and enter the code “EarlyBird18” by September 19th. Register today at www.sans.org/san-diego-fall