**Simulcast training from SANS Institute** allows you to attend a live training event from the convenience of your own computer. SANS Simulcast courses let you experience the energy of a live SANS classroom, while benefiting from the features of remote training, which include:

- A full five/six days of interactive online real-time training
- Four months of online access to your course
- Archived labs and lectures
- All printed books and required materials

**SANS Simulcast** was designed to give you all of the benefits of both a live event and remote learning. Students who use Simulcast are able to avoid travel, learn from the best in the industry, and interact with their classroom and review their course afterwards at their own pace.

**Join these classes via Simulcast from upcoming SANS APAC events!**

Register by September 30 and receive a **USD 500 discount** using the discount code '**SIM2016APAC**' *(Please note that this discount cannot be combined with other offers, including early registration discount rates.)*

---

**@ SANS October Singapore 2016**
SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling
31 Oct - 5 Nov | Instructor: Kevin Fiscus

**Learn More**

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), 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.

By helping you understand attackers' 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, this course helps you turn the tables on computer attackers. 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, 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 for, exploiting, and defending systems. It will enable you to discover the holes in your system before the bad guys do!

---

**@ SANS Sydney 2016**
SEC301: Intro to Information Security
7-11 Nov | Instructor: My-Ngoc Nguyen

**Learn More**

To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

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

If you answer yes to any of these questions, the **SEC301: Introduction to Information Security** training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised five-day comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

This course is designed for students who have a basic knowledge of computers and technology but no prior knowledge of cyber security. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you.

You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

---

**@ SANS Sydney 2016**
SEC511: Continuous Monitoring and Security Operations
14-19 Nov | Instructor: Bryan Simon

**Learn More**

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying 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, 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. **SEC511: Continuous Monitoring and Security Operations** will teach you how to strengthen your skills to undertake that proactive approach.

SANS is uniquely qualified to offer this course. Course authors, Eric Conrad (GSE #13) and Seth Misenar (GSE #28), hold the distinguished GIAC Security Expert Certification, and both are experienced, real-world, practitioners who apply the concepts and techniques they teach in this course on a daily basis. SEC511, taught here by Bryan Simon, 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.

---

To learn more about completing one of the above SANS courses via Simulcast, visit Simulcast FAQ or email us at asiapacific@sans.org.