SANS

CYBER DEFENSE

SAN DIEGO

2014

Prevent

Detect

Respond

Nov 3-8, 2014 | San Diego, CA

sans.org/event/cyber-defense-san-diego-2014

> ***“SANS courses have expanded my security knowledge and made me more valuable to my organization.”***
>
> -Lance Grover, Consolidated Graphic

COURSES OFFERED

CORE

SEC401
Security Essentials Bootcamp Style
GSEC

MGT512
SANS Security Leadership Essentials For Managers with Knowledge Compression™
GSLC

ADVANCED

SEC501
Advanced Security Essentials – Enterprise Defender
GCED

SEC503
Intrusion Detection In-Depth
GCIA

SPECIALIZATION

SEC566
Implementing and Auditing the Critical Security Controls – In-Depth
GCCC

MGT414
SANS® +S™ Training Program for the CISSP® Certification Exam
GISP

SEC511
Continuous Monitoring and Security Operations
New!

SANS CYBER DEFENSE
SAN DIEGO 2014

Nov 3-8, 2014 | San Diego, CA

Join us at this premier Cyber Defense-focused event that will feature SANS' top-notch instructors. We are offering seven of our most popular defensive courses that will teach you how to stay on top of today's threats and ahead of tomorrow's. You will experience deep-immersion technical training full of practical tools and techniques for defending against attacks. Bonus evening sessions will accelerate your pace of learning while numerous labs and exercises provide a comprehensive hands-on training experience.This unique blend of expertise and real-world practice is what drives SANS' unparalleled reputation and will turbo-charge your career as well.

Top five reasons to attend:

1. **Defense-Focused Training** – SANS' first-ever offering of training dedicated solely to teaching security professionals how to excel at defending. Threats evolve and your security program should too!
2. **SANS Instructors** – World-class expert instructors foster an environment of excellence.
3. **NEW Content** – *Continuous Monitoring and Security Operations* (SEC511) written by two of SANS' top instructors, Eric Conrad (GSE#13) & Seth Misenar (GSE#28). Learn how to monitor, detect, and react to changing threat vectors.
4. **Bonus Talks** – SANS' top instructors and industry-leading experts offer free bonus sessions on ground-breaking topics that will enable you to stay ahead of the attackers and increase your value within your organization.
5. **Networking** – Learn, dine, and socialize with other leading security professionals in a world-class city.

Register today at sans.org/event/cyber-defense-san-diego-2014 – Don't wait too long because the threats are not slowing down! ***The sooner you register, the BIGGER the savings!***

Security Essentials Bootcamp Style

Instructor: Dr. Eric Cole

SEC401

Prevention Is Ideal but Detection Is a Must!

> *"SEC401 is the best class I have ever taken.*
> *Dr. Cole is also the most knowledgeable and best instructor.*
> *I have over 2,800 hours of training.*
> *I would highly recommend SANS and especially Dr. Cole."*
>
> -Nicholas Christian, Tennessee Bureau of Investigation

- Design and build a network architecture
- Learn how to create a security roadmap
- Build a network visibility map to harden a network
- Develop effective security metrics
- Analyze systems using Linux and Windows command-line tools
- Identify vulnerabilities in a system & configure the system to be more secure
- Utilize sniffers to analyze protocols to determine content and passwords

GIAC SECURITY ESSENTIALS CERTIFICATION GSEC

sans.org/sec401

SANS' flagship and most popular course! Written by renowned industry expert and SANS Instructor Dr. Eric Cole, this intensive six-day course focuses on the essential skills needed to protect and secure an organization's critical information assets and business systems. Key concepts covered include Networking Concepts, Defense-In-Depth, O/S Security, Secure Communications, and much more. Extended hours in a bootcamp format reinforce key concepts with hands-on labs. This course will challenge you!

SEC501

Advanced Security Essentials – Enterprise Defender

Instructor: Bryce Galbraith

Attacks and Threats Are Relentless... Your Defense Should Be Too!

This comprehensive course is focused on preventing, detecting, and reacting to attacks in a timely fashion. These actions must be seamlessly integrated so that once an attack is detected, defensive measures can be adapted, proactive forensics implemented, and the organization can continue to operate. Learn how to design and implement a robust network infrastructure that will enable you to protect your network through timely detection. Penetration testing will teach you how to identify an organization's exposure points. A proven six-step process to follow in response to an attack will teach you how to mitigate and recover from incidents. Finally, the course will cover malware and data loss prevention.

> *"SEC501 is the best technical training course I have ever taken.*
> *It exposed me to many valuable concepts and tools,*
> *but it also gave me a solid introduction to those tools*
> *so that I can continue to study and improve on my own."*
>
> -Curt Smith, Hidalgo Medical Services

- Learn how to identify threats against network infrastructure
- Learn how to build a defensible network
- Learn how to decode and analyze packets using various tools
- Learn how to perform penetration testing to determine vulnerabilities
- Learn the six-step incident handling process
- Identify and remediate malware
- Deploy data loss prevent solutions

sans.org/sec501

Intrusion Detection In-Depth

Instructor: Mike Poor

All Packets Are Not Created Equal... Some Are Evil!

> *"SEC503 is a great eye-opener and I'm excited to bring the knowledge I learned back to my organization."*
>
> -John Neff, Sotera Defense Solutions

- Utilize open-source tools in all phases of network detection to bolster defense
- Understand different phases of an attack and identify them in several ways
- Learn to capture full-packet payload for examination
- Identify network behavioral anomalies
- Learn to synthesize log data to expose a trail of evidence
- Learn to place, customize, and tune IDS/IPS for maximum detection

GIAC CERTIFIED INTRUSION ANALYST GCIA

sans.org/sec503

SEC503

This course will teach you how to identify those evil packets! Time is of the essence in detecting and responding to attacks, and organizations are not doing enough to hone and support the detection capability of their security analysts. This course was specifically developed to teach individuals the essential skills and techniques needed to recognize and react to indicators of a cyber attack before it becomes a large-scale data breach and headline news.

SEC511

Continuous Operations and Security Operations

Instructor: Eric Conrad

The Threat Landscape Is Constantly Changing! How Quickly Can You Adapt?

No network is impenetrable, a reality that business executives and security professionals alike have to accept. This course focuses on the current principles of a modern security architecture and Security Operations Center (SOC) in direct response to the current tactics and techniques used by adversaries to penetrate seemingly secure organizations. The Defensible Security Architecture, Continuous Diagnostics and Mitigation, and Continuous Security Monitoring taught in this course will best position your organization or SOC to analyze threats and detect anomalies that could indicate cybercriminal behavior.

> *"SANS courses provide practical knowledge and skills that can be immediately applied on the job."*
>
> -Martin Hristov, Sony

- Understand the principles of a defensible security architecture
- Analyze a security architecture for deficiencies
- Apply the principles to design a defensible architecture
- Implement a robust and continuous security monitoring program
- Correlate security monitoring data for actionable intelligence
- Write scripts to reduce the total cost of ownership of continuous security monitoring

sans.org/sec511

Implementing and Auditing the Critical Security Controls – In-Depth

Instructor: Randy Marchany

As Threats Evolve, an Organization's Security Should Evolve as well!

> *"These controls should be in every security professional playbook. SEC566 provides the necessary insight to make implementation manageable."*
>
> -Randy Pauli, Chelan County PUD

- Learn to apply a security framework based on actuals threats to defend against attacks
- Use tools that implement the Controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each Control
- Employ specific metrics to establish a baseline and measure the effectiveness of the Controls
- Understand how the Critical Controls map to standards such as NIST 800-53
- Learn to audit each Control

sans.org/sec566

SEC566

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

MGT414

FREE RETAKE OFFER: sans.org/special/cissp-get-certified-program

This course provides you with the expert instruction, case studies, CISSP® study guide, supplemental test questions, and the hands-on training and knowledge you need to pass the CISSP® exam. MGT414 is absolutely the best way to earn your CISSP® certification and to learn the core principles of the Ten CISSP® Domains of Knowledge.

SANS® +S™ Training Program for the CISSP® Certification Exam

Instructor: Seth Misenar

CISSP® Exam – Rigorous and Challenging! We will Prepare You... One Domain at a Time!

> *"MGT414 is simply the best way to prepare for the CISSP. Great test-taking tips, relevant examples, and real-life meaningful illustrations."*
>
> -Thomas Cook, U.S. Marine Corps

- In-depth study of the 10 domains of knowledge covered on the exam
- Learn to analyze exam questions and select the correct answer
- Learn and apply knowledge and testing skills in class that will help you pass the exam
- Apply skills learned across 10 domains to solve security issues in the workplace
- Learn from the best security professionals in the industry

sans.org/mgt414

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Instructor: Stephen Northcutt

Security Is about Managing Risks... What Managers Should Know!

> *"Tremendously valuable experience! Learned a lot and also validated a lot of current practices. Thank You!!"*
>
> -Chad Gray, Booz Allen Hamilton

- 〉Learn what IT security managers must know to function in today's environment
- 〉Learn the methods of attacks against an enterprise
- 〉Learn to secure communication techniques to secure a company's assets
- 〉Learn how to better protect intellectual property
- 〉Learn how to brief management on risk architecture
- 〉Learn proven incident-handling techniques

sans.org/mgt512

GIAC Security Leadership Certification GSLC

MGT512

This course covers the essential security topics and teaches managers the vital skills required to effectively supervise the security component of any information technology project. You won't just learn how to manage security—we will show how to apply the technical knowledge you learned to the art of management. We'll explore proven techniques for successful and effective management, empowering you to immediately apply what you have learned upon returning to the office.

BONUS SESSIONS

EVENING KEYNOTE

Understanding the Offense to Build a Better Defense

Dr. Eric Cole

Many organizations do not perform proper threat modeling. Nor do they understand what the adversary is capable of. The only way to ensure good defense is to understand the offense. Unfortunately how the threat targets and attacks a system can provide insight into implementing a proper security program. This talk will examine attackers' capabilities and methods, and outline specific steps organizations can take to properly defend themselves.

MORNING KEYNOTE

Moving Forward to a Secure Future

Stephen Northcutt

Everyone loves talking about the different types of attacks and the adversary's formidable capabilities. Information about the threat is indeed important, but organizations also need to focus on properly securing their organization. In this talk we will review what organizations need to do to properly defend themselves going forward. It is critical that organizations have a solid defensive foundation built on asset identification, configuration management, and change control. As will be discussed, once the foundation is in place, organizations can turn to more focused and complex defensive solutions.

Continuous Monitoring: Making a SOC a Reality

Panel discussion lead by Eric Conrad

Security Operations Centers (SOC) are the control point for monitoring and protecting an organization. In this panel discussion led by Eric Conrad, participants will have an opportunity to ask top experts in the field about the best way to build out a SOC. Several panelists with extensive and ongoing experience in monitoring and analysis will discuss the best practices in the industry.

Moving Past Prevention and Focusing on Detection

Bryce Galbraith

SANS Faculty Fellow Dr. Eric Cole, an industry-recognized security expert with over 20 years of hands-on experience, often says that "Prevention is ideal but detection is a must." Ideally an organization wants to prevent all attacks. But in reality, considering the capability of some adversaries, all attacks cannot be prevented—some will have to be detected. Therefore organizations need to put more and more focus on detection. If an adversary successfully bypasses preventive measures, it is critical that the attack be detected in a timely manner and the damage controlled and limited.

SANS CYBER DEFENSE CURRICULUM

Targeted attacks are on the rise, organizations are being compromised, and attacks can go undetected for months. Smart organizations know that risk management is a key part of all security decisions, but many don't know where to start. The five-step Cyber Defense process outlined below will enable you to identify risk, determine the highest priorities, focus in on the areas that really matter, and measure progress against established baselines to improve your overall security posture.

Five Key Steps to Cyber Defense

STEP 1: Identify Critical Data

Align critical assets with threats and vulnerabilities to focus on risk

1 What is the risk?

2 Is it the highest priority risk?

3 What is the most cost-effective way to reduce the risk?

STEP 2: Align the Defense with the Offense

1 Reconnaissance

2 Scanning

3 Exploitation

4 Creating backdoors

5 Covering tracks

STEP 3: Know Thy Organization

If the offense knows more than the defense, you will lose

Requirements:

1 Accurate and up-to-date network diagram

2 Network visibility map

3 Configuration management and change control

STEP 4: Defense in Depth

There is no such thing as an unstoppable adversary

Requirements:

1 Inbound prevention

2 Outbound detection

3 Log correlation

4 Anomaly detection

STEP 5: Common Metrics

Requirements:

Utilize the Critical Controls:

1 Offense informing the defense

2 Automation and continuous monitoring of security

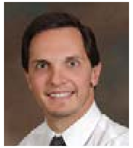
3 Metrics to drive measurement and compliance

Providing curriculum options by job role for the following positions:

- **Cybersecurity manager/officer**
- **Intrusion analyst/Security Operations Center monitor**
- **Operations management**
- **Security analyst**
- **Security engineer**
- **System/security administrator**

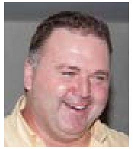
Download your free roadmap brochure at cyber-defense.sans.org/training/roadmap

CYBER DEFENSE SAN DIEGO INSTRUCTORS



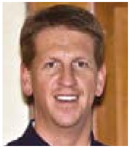
Dr. Eric Cole

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole has experience in information technology with a focus on helping customers focus on the right areas of security by building out a dynamic defense. Dr. Cole has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. He served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is the author of several books, including *Advanced Persistent Threat*, *Hackers Beware*, *Hiding in Plain Sight*, *Network Security Bible 2nd Edition*, and *Insider Threat*. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is the founder and an executive leader at Secure Anchor Consulting, where he provides leading-edge cybersecurity consulting services and expert witness work, and leads research and development initiatives to advance the state of the art in information systems security. Dr. Cole was the lone inductee into the InfoSec European Hall of Fame in 2014. Dr. Cole is actively involved with the SANS Technology Institute (STI) and is a SANS faculty Fellow and course author who works with students, teaches, and develops and maintains courseware. @drericcole



Eric Conrad

SANS Principal Instructor Eric Conrad is lead author of the book *The CISSP Study Guide*. Eric's career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and health care. He is now president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing. He is a graduate of the SANS Technology Institute with a Master of Science degree in information security engineering. In addition to the CISSP, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at www.ericconrad.com. @eric_conrad



Bryce Galbraith

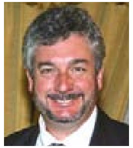
Bryce is a contributing author to the internationally bestselling book *Hacking Exposed: Network Security Secrets & Solutions*. He helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, and he was a member of Foundstone's renowned penetration testing team and served as a senior instructor and co-author of its Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security, where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS Institute's most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, holds several security certifications, and speaks at conferences around the world. @brycegalbraith

Randy Marchany

Randy is the Chief Information Security Officer to Virginia Tech University and the Director of its IT Security Laboratory. He is a co-author of the original SANS Top 10 Internet Threats, the SANS Top 20 Internet Threats, the SANS Consensus Roadmap for Defeating DDoS Attacks, and the SANS Incident Response: Step-by-Step guides. Randy is currently a certified instructor for the SANS Institute. He is a member of the Center for Internet Security development team that produced and tested the CIS Solaris, HPUX, AIX, Linux and Windows2000/XP security benchmarks and scoring tools. He was a member of the White House Partnership for Critical Infrastructure Security working group that developed a Consensus Roadmap for responding to the DDoS attacks of 2000. @randymarchany

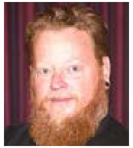
Seth Misenar

Seth Misenar is a SANS Principal Instructor and also serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security through leadership, independent research, and security training. Seth's background includes network and Web application penetration testing, vulnerability assessment, regulatory compliance, security architecture design, and general security consulting. He has previously served as both physical and network security consultant for Fortune 100 companies as well as the HIPAA and information security officer for a state government agency. Prior to becoming a security geek, Seth received a BS 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, but are not limited to, the CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. @sethmisenar



Stephen Northcutt

Stephen Northcutt founded the GIAC certification and served as president of the SANS Technology Institute. Stephen is author/coauthor of *Incident Handling Step-by-Step*, *Intrusion Signatures and Analysis*, *Inside Network Perimeter Security 2nd Edition*, *IT Ethics Handbook*, *SANS Security Essentials*, *SANS Security Leadership Essentials*, and *Network Intrusion Detection 3rd Edition*. He was the original author of the Shadow Intrusion Detection system before accepting the position of Chief for Information Warfare at the Ballistic Missile Defense Organization. Stephen is a graduate of Mary Washington College. Before entering the field of computer security, he worked as a Navy helicopter search and rescue crewman, white water raft guide, chef, martial arts instructor, cartographer, and network designer. Since 2007 Stephen has conducted over 40 in-depth interviews with leaders in the security industry, from CEOs of security product companies to the most well-known practitioners, in order to research the competencies required to be a successful leader in the security field. He maintains the SANS Leadership Laboratory, where research on these competencies is posted, as well as SANS Security Musings. He leads the Management 512 Alumni Forum, where hundreds of security managers post questions. @StephenNorthcut



Mike Poor

Mike is a founder and senior security analyst for the Washington firm InGuardians, Inc. In the past he worked for Sourcefire as a research engineer and for SANS leading their intrusion analysis team. As a consultant, Mike conducts incident response, breach analysis, penetration tests, vulnerability assessments, security audits, and architecture reviews. His primary job focus, however, is on intrusion detection, response, and mitigation. Mike currently holds the GCIA certification and is an expert in network engineering and systems and network and web administration. Mike is an author of the international best-selling *Snort* series of books from Syngress, a member of the Honeynet Project, and a handler for the SANS Internet Storm Center. @Mike_Poor

The information security field is growing and maturing rapidly. Are you positioned to grow with it? A Master's Degree in Information Security from the SANS Technology Institute (STI) will help you build knowledge and skills in management or technical engineering.

Master's Degree Programs:

- ▸ **M.S. in Information Security Engineering**
- ▸ **M.S. in Information Security Management**

Specialized Graduate Certificates:

- ▸ **Penetration Testing & Ethical Hacking**
- ▸ **Incident Response**
- ▸ **Cybersecurity Engineering (Core)**

The SANS Technology Institute, a subsidiary of the SANS Institute, is accredited by the Middle States Commission on Higher Education (3624 Market Street, Philadelphia, PA 19104 – Tel: 267.284.5000), an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

Learn more at
www.sans.edu | info@sans.edu

How Are You Protecting Your

Get GIAC certified!

GIAC offers over 26 specialized certifications in security, digital forensics, penetration testing, web application security, IT audit, management, and IT security law.

GSEC — **SEC401:** GIAC Security Essentials
giac.org/certification/security-essentials-gsec

GCED — **SEC501:** GIAC Certified Enterprise Defender
giac.org/certification/certified-intrusion-analyst-gcia

GCIA — **SEC503:** GIAC Certified Intrusion Analyst
giac.org/certification/intrusion-detection-in-depth

GCCC — **SEC566:** GIAC Critical Controls Certification
giac.org/certification/critical-controls-certification-gccc

GISP — **MGT414:** GIAC Information Security Professional
giac.org/certification/information-security-professional-gisp

GSLC — **MGT512:** GIAC Security Leadership
giac.org/certification/security-leadership-gslc

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

FUTURE SANS SUMMIT & TRAINING EVENTS

SANS Crystal City 2014

Crystal City, VA | September 8-13

SANS Baltimore 2014

Baltimore, MD | September 22-27

Retail Cyber Security

SUMMIT & TRAINING

Dallas, TX | September 8-17

SANS Seattle 2014

Seattle, WA | September 29 - October 6

Security Awareness

SUMMIT & TRAINING

Dallas, TX | September 8-17

SANS Network Security 2014

Las Vegas, NV | October 19-27

SANS Albuquerque 2014

Albuquerque, NM | September 15-20

SANS DFIRCON EAST

SANS DFIRCON East 2014

Fort Lauderdale, FL | November 3-8

See a complete list of all future SANS training events at sans.org/security-training/by-location/all

Hotel Information

Training Campus
Hard Rock Hotel San Diego

207 Fifth Avenue
San Diego, CA
sans.org/event/cyber-defense-san-diego-2014/location

The Hard Rock Hotel San Diego is centrally located in the city's lively Gaslamp Quarter. The hotel's unconventionally sleek and contemporary design will wow you, and the unique amenities and expectation-exceeding service will provide you with an authentic experience that simply rocks.

Special Hotel Rates Available

A special discounted rate of $210.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through October 10, 2014. To make reservations please call (866) 751-7625 and ask for the SANS November 2014 group rate.

Top 5 reasons to stay at the Hard Rock Hotel San Diego

1 All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.

2 No need to factor in daily cab fees and the time associated with travel to alternate hotels.

3 By staying at the Hard Rock Hotel San Diego, you gain the opportunity to further network with your industry peers and remain at the center of activities surrounding the training event.

4 SANS schedules morning and evening events at the Hard Rock Hotel San Diego that you won't want to miss!

5 Everything is in one convenient location!

Registration Information

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

Register online at sans.org/event/cyber-defense-san-diego-2014/courses

Select your course or courses 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.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**9/17/14**	**$400.00**	**10/1/14**	**$200.00**

Some restrictions apply.

Group Savings (Applies to tuition only)*

10% discount if 10 or more people from the same organization register at the same time
5% discount if 5 - 9 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

**Early-bird rates and/or other discounts cannot be combined with the group discount.*

Cancellation

You may substitute another person in your place at any time, at no charge, by email: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by October 15, 2014 – processing fees may apply.

DON'T MISS IT!

- **Hands-On Immersion Training Taught by Real-World Practitioners**

  Our hands-on, immersion-style security training courses are taught by top experts active in the field.

- **SANS Bonus Sessions**

  Enrich your SANS training experience! Evening talks by our instructors and selected subject-matter experts help you broaden your knowledge, hear the voices that matter in computer security, and get the most for your training dollar.

- **Get Certified!**

  Six of the courses offered have associated GIAC certifications with them.

Register at
sans.org/event/cyber-defense-san-diego-2014

Register and pay by
September 17TH and
SAVE $400
on San Diego courses.

sans.org/info/161405

5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

Save $400 when you register and pay by September 17th
sans.org/event/cyber-defense-san-diego-2014