Discover your hidden talents,
sharpen your cybersecurity skills,
and challenge yourself
by training at

SANS CYBER DEFENSE

SAN DIEGO 2015

October 19-24

```
4500 0054 0000 4000 4001 3ca7 7f00 0001
7f00 0001 0800 e263 5107 0cdd 0473 524f
73f2 0200 0809 0a0b 0c0d 0eof 1011 1213
1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
3435 3637
```

...and become
EXTRAORDINARY!

sans.org/event/cyber-defense-san-diego-2015

NEW THIS YEAR!

SANS CYBER DEFENSE

Challenge 2015

SEE CENTER BIND-IN CARD
FOR MORE DETAILS

THE CYBER DEFENSE CURRICULUM AT SANS IS NOT YOUR ORDINARY CYBER DEFENSE TRAINING PROGRAM

And it shouldn't be, because your job, as a Cyber Defender, is NOT ordinary.

You are on the front lines. You protect your family, your organization, and your country from those who would do harm. Defending networks isn't just your job, it's your passion. It flows through your veins and is your primary focus every waking moment.

While there are many aspects to cybersecurity, you know that cyber defense is what protects lives, businesses, and governments. You realize that you are an unsung hero. If an attack gets through, everyone hears about it, but no one hears about the hundreds of attacks you prevent every day.

Enemies will continually try to cause harm, but you will fight back by taking each threat seriously and building your skills to thwart the full range of attacks. You are the first and last line of defense and the work you do is extraordinary. Each day you'll make a bold commitment to:

- **Vigilantly defend networks against attacks**
- **Expose vulnerabilities**
- **Always provide competent service**
- **Continuously hone your skills**
- **Immediately respond to breaches**
- **Secure data and infrastructure**
- **Stay up to date on the latest attacks and breaches**
- **Create new solutions**
- **Diligently keep your knowledge current**

How is this cyber defense training different? SANS training has been described by students as rigorous, in-depth, defense-focused, strategic, and leading-edge. The Cyber Defense curriculum can best be described as the most effective training available to keep you ahead of the adversary at all times.

Investigate the SANS Cyber Defense Curriculum and join the ranks of thousands of distinguished unsung heroes who sharpen their cybersecurity skills at SANS.

A SPECIAL MESSAGE FROM DR. ERIC COLE

Each year thousands of cybersecurity professionals across the world take Cyber Defense training at SANS Institute. Here's why…

"The threat level remains high. High-profile cybersecurity breaches have become an all too common occurrence in recent years and show no sign of abating. Even more alarming is the fact that, in most organizations, security breaches are going undetected for several months. Surprisingly and worst of all, the organizations compromised are usually made aware of the attack by someone outside of the organization. The impact is costly, resulting in business disruptions and serious reputational damage.

"I invite and encourage you to join the ranks of your peers and colleagues who come to San Diego each year to improve their skills and their organization's security posture. The best defense against a cyber-attack or threat is education. Join us in San Diego and challenge the adversary."

-Dr. Eric Cole, world-renowned Cybersecurity Expert,
SANS Fellow and Author of *Advanced Persistent Threat:*
Understanding the Danger and How to Protect Your Organization

THE CYBER DEFENSE CURRICULUM

EXTRAORDINARY TRAINING FOR CHALLENGING MOMENTS

As a cybersecurity professional, you know that cyber dangers, vulnerabilities, and threats occur at the speed of a click –
AND SOMETIMES YOU ONLY HAVE A MOMENT TO TAKE ACTION.
It takes lightning speed and the ninja-like skills of a SANS Cyber Defender to thwart those attacks.

At SANS Institute you'll acquire the skills and tactics you need to seize these moments. The courses in the SANS Cyber Defense curriculum will teach you the essential skills required to defend your organization against cyber-attacks and improve its overall security posture.

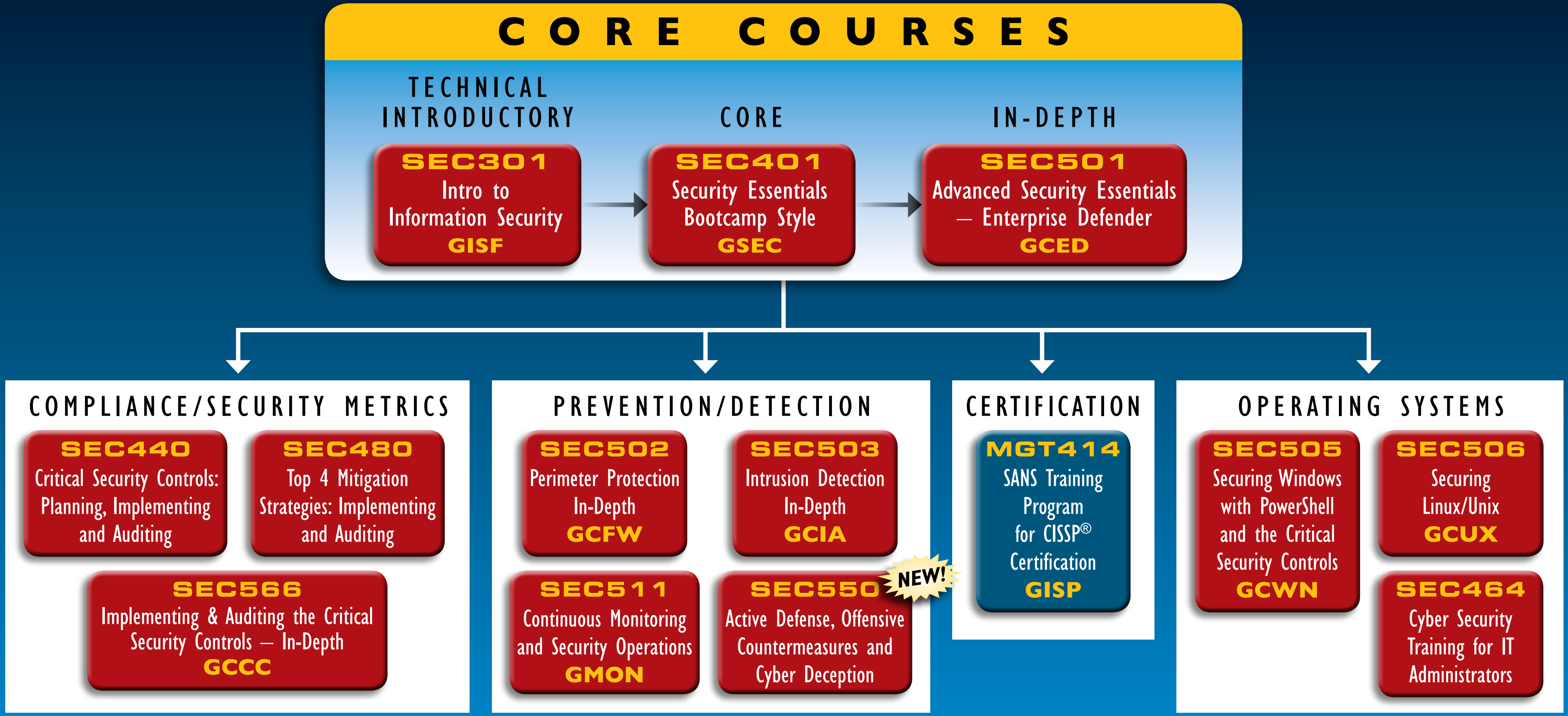
As a SANS Cyber Defender, you'll be fully equipped to:

- **Prevent, detect, and respond to incidents**
- **Build and design secure business processes**
- **Assess, understand, and fix exposures in existing networks**
- **Understand the threat and how to defend against it**
- **Communicate cybersecurity throughout the organization**
- **Create security solutions that can scale across any organization**
- **Protect and secure critical intellectual property**

SANS Institute has a proven track record for delivering world-class cyber defense training since 1989. Join the ranks of thousands of cybersecurity professionals who have earned over 58,000 certifications by taking SANS courses at live events in cities across the world from Orlando to San Diego, London, Dubai, Singapore, and Sydney.

If you are unable to travel, SANS offers a vast selection of other options. You can attend courses online via web simulcast, OnDemand, at live evening classes, or at classes in person in your local community.

SANS CYBER DEFENSE CURRICULUM



CORE COURSES

TECHNICAL INTRODUCTORY

SEC301
Intro to Information Security
GISF

CORE

SEC401
Security Essentials Bootcamp Style
GSEC

IN-DEPTH

SEC501
Advanced Security Essentials — Enterprise Defender
GCED

COMPLIANCE/SECURITY METRICS

SEC440
Critical Security Controls: Planning, Implementing and Auditing

SEC480
Top 4 Mitigation Strategies: Implementing and Auditing

SEC566
Implementing & Auditing the Critical Security Controls — In-Depth
GCCC

PREVENTION/DETECTION

SEC502
Perimeter Protection In-Depth
GCFW

SEC503
Intrusion Detection In-Depth
GCIA

SEC511
Continuous Monitoring and Security Operations
GMON

SEC550
Active Defense, Offensive Countermeasures and Cyber Deception

NEW!

CERTIFICATION

MGT414
SANS Training Program for CISSP® Certification
GISP

OPERATING SYSTEMS

SEC505
Securing Windows with PowerShell and the Critical Security Controls
GCWN

SEC506
Securing Linux/Unix
GCUX

SEC464
Cyber Security Training for IT Administrators

THIS IS YOUR LIFE, SEIZE THE MOMENT

CHALLENGE YOURSELF

THIS IS YOUR CYBER DEFENSE COMMUNITY

Whether you attend a live training class or take a course via OnDemand or within your local community, you'll become a part of a vast Cyber Defense community that is leading the way and breaking new ground in the fight against cyber-attacks. You'll join a network of distinguished professionals just like you who care about cybersecurity.

THIS IS YOUR CYBER DEFENSE CAREER

The SANS Cyber Defense curriculum has all the advantages you'd expect from a leading institute. Taking SANS Cyber Defense courses is invaluable to advance your career. Through these cutting-edge courses, you'll discover little-known techniques and tips to help you defend your organization against attacks and security breaches.

You'll gain a real-world perspective and be able to apply the skills you've learned immediately when you return to work.

That's the SANS promise.

As you learn more, the opportunities to advance your career will increase exponentially alongside your new skill sets. The Cyber Defense network can open doors to new opportunities for you. Not only will you get to swap stories and best practices with your peers, you'll also be exposed to unadvertised career opportunities and job leads. You'll gain unparalleled insider access to industry news, business trends, training events, and savings opportunities that are not readily available outside of this network.

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 here 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 manager**
- **Security analyst**
- **Security engineer**
- **System/security administrator**

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

THIS IS YOUR CYBER DEFENSE FACULTY

World-class instruction doesn't just happen anywhere. But it does happen at SANS Institute. SANS invests heavily in its faculty and takes your education seriously. Potential instructors undergo a rigorous background screening and training process before they're allowed to teach. The commitment to excellence continues by requiring all approved instructors to maintain the SANS standard of excellence throughout the course. Each day you will get an opportunity to evaluate the course and the instructor, which gives you as the student control over the process of evaluating the materials and instructors. ***We will not compromise on quality.***

Dr. Eric Cole *SANS Faculty Fellow*

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. He currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Dr. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. He has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. Dr. Cole is the author of several books, including *Hackers Beware*, *Hiding in Plain Site*, *Network Security Bible*, 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 Cybersecurity for the 44th President and several executive advisory boards. Dr. Cole is founder of Secure Anchor Consulting, where he provides state-of-the-art security services and expert witness work. He also served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is actively involved with the SANS Technology Institute (STI) and SANS, working with students, teaching, and maintaining and developing courseware. @drericcole

Eric Conrad *SANS Senior 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 ericconrad.com. @eric_conrad

Mick Douglas *SANS Instructor*

Even when his job title indicated otherwise, Mick Douglas has been doing information security work for over ten years. He received a bachelor's degree in Communications from the Ohio State University and holds the CISSP, GCIH, GPEN, GCUX, GWEB, and GSNA certifications. He currently works at Binary Defense Systems as the DFIR Practice Lead. He is always excited for the opportunity to share with others so they do not have to learn the hard way! When Mick is not "geeking out" you'll likely find him indulging in one of his numerous hobbies: photography, scuba diving, or hanging around in the great outdoors.

Paul A. Henry *SANS Senior Instructor*

Paul Henry is one of the world's foremost global information security and computer forensic experts, with more than 20 years of experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a strategic role in launching network security initiatives to meet our ever-changing threat landscape. Paul also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the U.S. Department of Defense's Satellite Data Project, and both government as well as telecommunications projects throughout Southeast Asia. Paul is frequently cited by major publications as an expert in computer forensics, technical security topics, and general security trends and serves as an expert commentator for network broadcast outlets such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications, such as the Information Security Management Handbook, to which he is a consistent contributor. Paul serves as a featured and keynote speaker at seminars and conferences worldwide, delivering presentations on diverse topics including anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, firewall architectures, security architectures, and managed security services. @phenrycissp

John Strand *SANS Senior Instructor*

John Strand teaches SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling; SEC550: Active Defense, Offensive Countermeasures and Cyber Deception; SEC560: Network Penetration Testing and Ethical Hacking; and SEC580: Metasploit Kung Fu for Enterprise Pen Testing. John is the course author for SEC550 and the co-author for SEC580. When not teaching for SANS, John co-hosts PaulDotCom Security Weekly, the world's largest computer security podcast. He also is the owner of Black Hills Information Security, specializing in penetration testing and security architecture services. He has presented for the FBI, NASA, the NSA, and at DefCon. In his spare time he writes loud rock music and makes various futile attempts at fly-fishing. @strandjs

Seth Misenar *SANS Senior Instructor*

Seth Misenar serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security thought 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 as 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 following: CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. Seth also is the course author of the SEC511: Continuous Monitoring and Security Operations; and co-author of MGT414: SANS Training Program for CISSP® Certification @sethmisenar

Mike Poor *SANS Senior Instructor*

Mike Poor is a founder and senior security analyst for the Washington, DC firm InGuardians, Inc. In the past he has worked for Sourcefire as a research engineer and for SANS leading its 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

Active Defense, Offensive Countermeasures and Cyber Deception

Instructor: Mick Douglas

SEC550

NEW

Change the Way You Think… Annoy and Frustrate Attackers with Unexpected Defenses!

01010001

You will learn how to:

- Track bad guys with callback Word documents
- Use Honeybadger to track web attackers
- Block attackers from successfully attacking servers with honeyports
- Block web attackers from automatically discovering pages and input fields
- Understand the legal limits and restrictions of Active Defense
- Obfuscate DNS entries
- Create non-attributable Active Defense Servers
- Combine geolocation with existing Java applications
- Create online social media profiles for cyber deception
- Easily create and deploy honeypots

sans.org/sec550

In this course, you will learn how to force an attacker to take more moves to attack your network. These moves can increase your ability to detect those attackers. You will learn how to gain better attribution as to who is attacking you and why. You will also learn how to get access to a bad guy's system. And most importantly, you will learn how to do the above legally. This course is very heavy with hands-on labs. We will not just talk about active defenses, we will be working with them in hands-on labs in a way that will enable you to quickly and implement those defenses in your environment as soon as you return to work.

Security Essentials Bootcamp Style

Instructor: Dr. Eric Cole

Prevention Is Ideal but Detection Is a Must!

01001100

> *"SEC401 answers the why of a lot of my work practices, and asks why not for the practices my company doesn't follow."*
>
> -Thomas Petro, Southern California Edison

You will learn how to:

- Design and build a network architecture
- 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

sans.org/sec401

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, 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!

Advanced Security Essentials – Enterprise Defender

Instructor: Paul A. Henry

SEC501

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

01010001

> *"The quality of instructors and students at SANS training provides an excellent learning environment and gives you a chance to talk security tech with your peers."*
>
> -Michael Lammerding, Young's Market

You will learn how to:

- Identify threats against network infrastructure
- Build a defensible network
- Decode and analyze packets using various tools
- Perform penetration testing to determine vulnerabilities
- Carry out the six-step incident handling process
- Identify and remediate malware
- Deploy data loss prevention solutions

sans.org/sec501

GIAC CERTIFIED ENTERPRISE DEFENDER GCED

This comprehensive course focuses 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.

Intrusion Detection In-Depth

Instructor: Mike Poor

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

01001101

> "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

You will learn how to:

- 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
- Capture full-packet payload for examination
- Identify network behavioral anomalies
- Synthesize log data to expose a trail of evidence
- 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.

Hacker Tools, Techniques, Exploits, and Incident Handling

Instructor: John Strand

Know Your Enemy

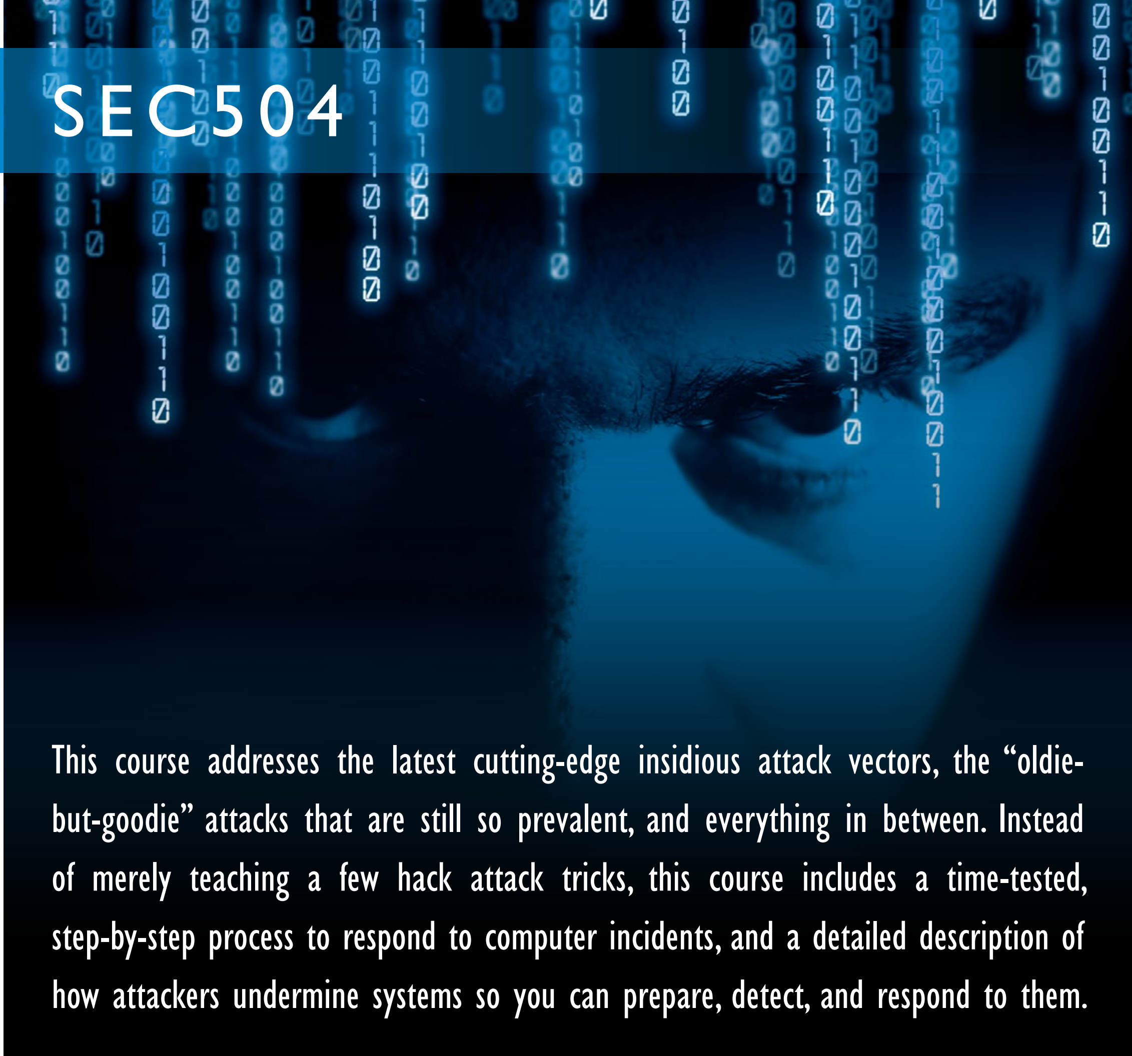
> *"My first SANS training experience was great. I will definitely take another SANS class."*
>
> -Stephanie Padilla, Intel Security

You will learn how to:

- Apply incident handling processes in-depth
- Analyze the structure of common attack techniques
- Accomplish operating system and application-level attacks
- Crack passwords
- Break into web applications
- Maintain access on a target

sans.org/SEC504

GIAC CERTIFIED INCIDENT HANDLER GCIH



SEC504

This course addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process to respond to computer incidents, and a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them.

Continuous Monitoring and Security Operations

Instructor: Seth Misenar

SEC511

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

01000100

"This is my sixth SANS training event and SANS continues to deliver. They offer relevant, practical, and highly informative courses taught by instructors who truly understand the content."

-Tyler Leet, Computer Services Inc.

COMING SOON!

GIAC CONTINUOUS MONITORING CERTIFICATION
GMON

- 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

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 Training Program for CISSP® Certification

Instructor: Eric Conrad

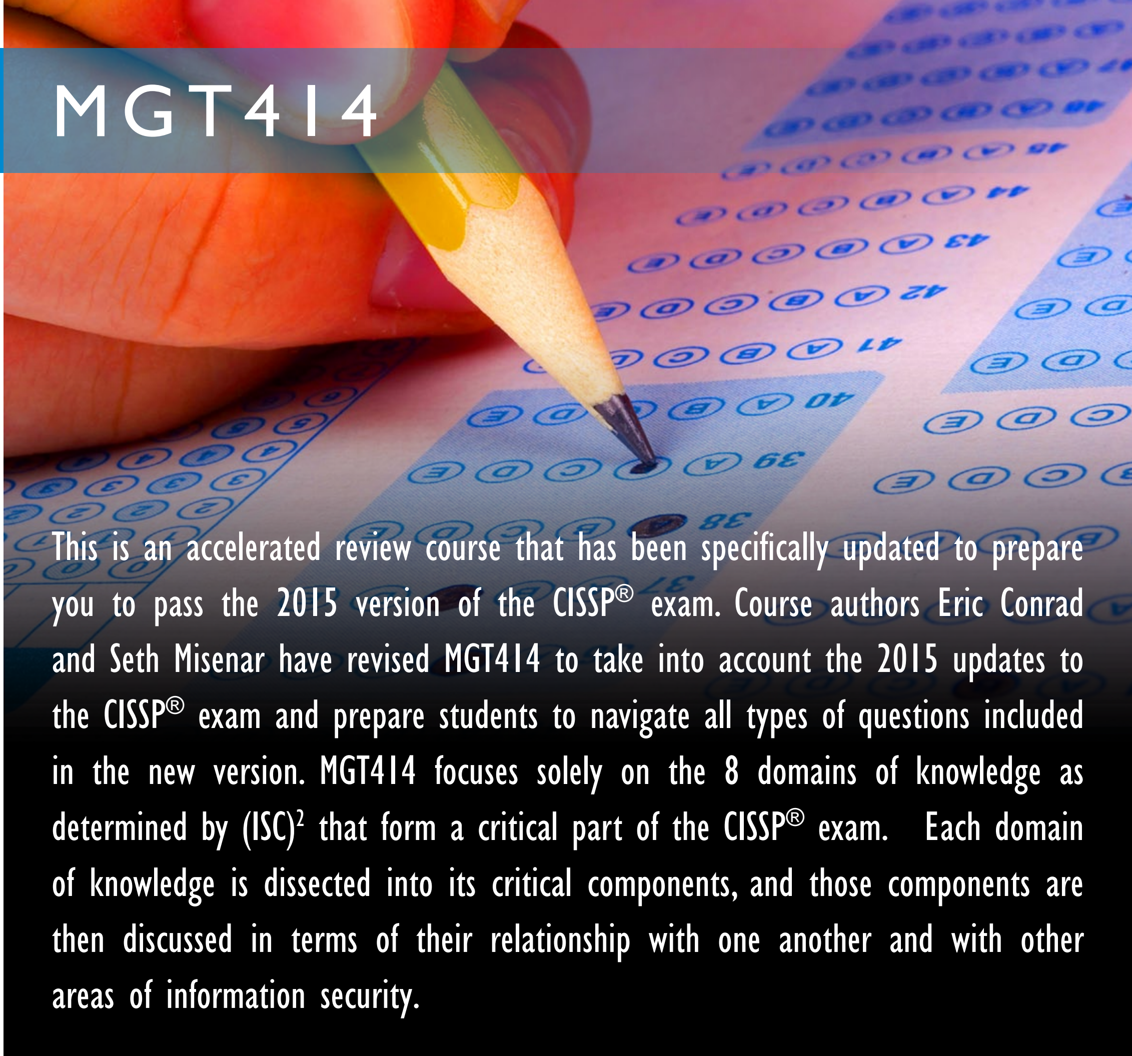
Do You Want to Advance Your Career? Yes!
Do You Need Training for the CISSP Exam? Yes!
Do You Want To Pass The First Time? Yes!

> *"This class focuses like a laser on the key concepts you will need to understand for the CISSP exam. Do not struggle with thousand-page textbooks. Let this course be your guide!"*
>
> -Carl Williams, Harris Corporation

You will learn how to:

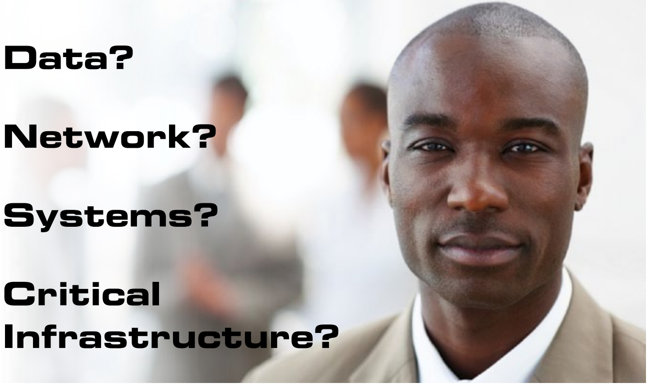
- Understand the 8 domains of knowledge that are covered on the CISSP® exam
- Analyze questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the 8 domains of knowledge
- Apply the skills learned across the 8 domains to solve security problems when you return to work

sans.org/MGT414



MGT414

This is an accelerated review course that has been specifically updated to prepare you to pass the 2015 version of the CISSP® exam. Course authors Eric Conrad and Seth Misenar have revised MGT414 to take into account the 2015 updates to the CISSP® exam and prepare students to navigate all types of questions included in the new version. MGT414 focuses solely on the 8 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.



OnDemand Bundles

sans.org/ondemand/bundles

Bundle four months of online study with your live course for just $629 with an OnDemand Bundle. The additional study will reinforce your learning through quizzes, labs, access to subject-matter experts and more.

Cyber Defense San Diego courses that can be bundled:

SEC401
SEC501
SEC503
SEC504
SEC511
MGT414

DoDD 8570

sans.org/8570

Department of Defense Directive 8570 (DoDD 8570) provides guidance and procedures for the training, certification, and management of all government employees who conduct Information Assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. GIAC has the most certifications that meet the requirements for Technical, Management, CND, and IASAE classifications. SANS courses prepare you to take a GIAC exam.

DoDD 8570 courses at Cyber Defense San Diego:

SEC401 | SEC501 | SEC503
SEC504 | MGT414

For more information about DoDD 8570:

Contact the DoDD 8570 Information Assurance Workforce Improvement Program Office at **http://iase.disa.mil/iawip/Pages/index.aspx**

Contact **8570@sans.org**
or call customer support at **301-654-7267**.

SANS CYBER GUARDIAN PROGRAM

sans.org/cyber-guardian

This program begins with hands-on core courses that will build and increase your knowledge and skills. These skills will be reinforced by taking and passing the associated GIAC certification exam. After completing the core courses, you will choose a course and certification from either the Red or Blue Team. The program concludes with participants taking and passing the GIAC Security Expert (GSE) certification.

Cyber Guardian courses at Cyber Defense San Diego:

SEC503 | SEC504

Contact us at onsite@sans.org to get started!

SANS CYBER DEFENSE SAN DIEGO 2015

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. The hotel is confident you will have a truly memorable experience.

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 Sept. 25, 2015.

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!

SANS CYBER DEFENSE SAN DIEGO 2015

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-2015/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.

Use code **EarlyBird15** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**8/26/15**	**$400.00**	**9/23/15**	**$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.

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 September 30, 2015 – processing fees may apply.

SANS CYBER DEFENSE

Challenge 2015

**PLAY ONLINE
OR AT
LIVE EVENTS**

PRIZES AWARDED WEEKLY

SEE BACK FOR DETAILS

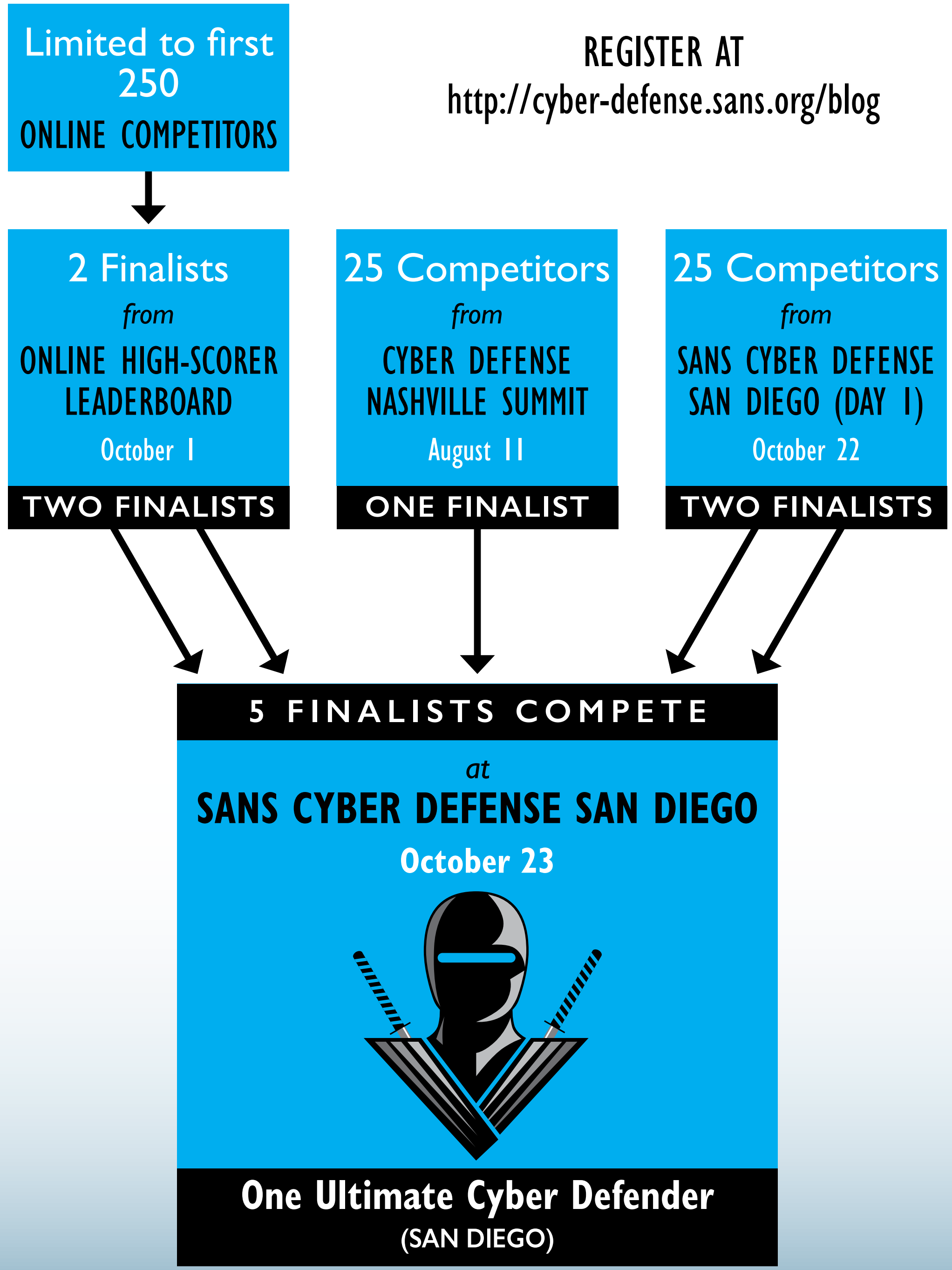
The Cyber Defense curriculum at SANS Institute announces the "battle royale" of cybersecurity competitions. Cybersecurity and Infosec practitioners from across the world will compete to be crowned the

2015 Ultimate Cyber Defender (SAN DIEGO)

at one of SANS' most popular training events:

SANS Cyber Defense San Diego 2015

Register at http://cyber-defense.sans.org/blog


Limited to first 250 ONLINE COMPETITORS

REGISTER AT
http://cyber-defense.sans.org/blog

2 Finalists *from* ONLINE HIGH-SCORER LEADERBOARD October 1 — TWO FINALISTS

25 Competitors *from* CYBER DEFENSE NASHVILLE SUMMIT August 11 — ONE FINALIST

25 Competitors *from* SANS CYBER DEFENSE SAN DIEGO (DAY 1) October 22 — TWO FINALISTS

5 FINALISTS COMPETE *at* SANS CYBER DEFENSE SAN DIEGO October 23

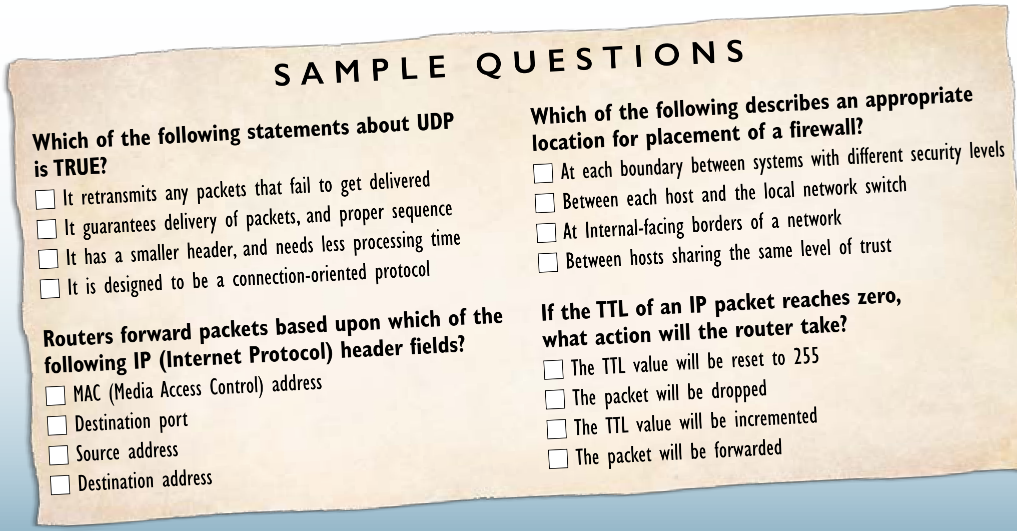
One Ultimate Cyber Defender (SAN DIEGO)

The Cyber Defense program at SANS Institute is on a mission to find the 2015 Ultimate Cyber Defender. This engaging and exciting challenge will allow participants to compete via online, summit, or regional training events. The final "battle royale" will take place in San Diego (Oct. 23) and will pit security professionals against each other in a quest to answer a series of cybersecurity questions every defender should know. Competitions to qualify for the event will be held online and at live events.

One Ultimate Cyber Defender will emerge from a group of contestants from the online and regional events.

The Benefits of Competing

When you participate in the SANS Cyber Defense Challenge you immediately become a standout among your peers. Everyone who participates has the potential to become the winner—but in a way, participating in itself makes you a winner because you get to test your skills and showcase them to existing and potential employers, as well as to friends, colleagues, and family. Each week we will award cool prizes to high-scoring participants via social media. Check the leaderboard every week to see where you stand.


SAMPLE QUESTIONS

Which of the following statements about UDP is TRUE?

□ It retransmits any packets that fail to get delivered
□ It guarantees delivery of packets, and proper sequence
□ It has a smaller header, and needs less processing time
□ It is designed to be a connection-oriented protocol

Routers forward packets based upon which of the following IP (Internet Protocol) header fields?

□ MAC (Media Access Control) address
□ Destination port
□ Source address
□ Destination address

Which of the following describes an appropriate location for placement of a firewall?

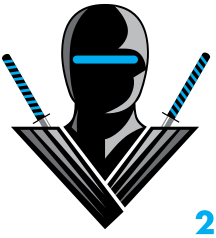
□ At each boundary between systems with different security levels
□ Between each host and the local network switch
□ At Internal-facing borders of a network
□ Between hosts sharing the same level of trust

If the TTL of an IP packet reaches zero, what action will the router take?

□ The TTL value will be reset to 255
□ The packet will be dropped
□ The TTL value will be incremented
□ The packet will be forwarded

All roads lead to SANS Cyber Defense San Diego 2015

Apply now to become the Ultimate Cyber Defender (SAN DIEGO)



REGIONAL COMPETITIONS (2 CITIES)

From 25 competitors at the Nashville Summit, one finalist will be chosen (Aug. 11)
and from 25 competitors at San Diego, two finalists will be chosen (Oct. 22)

Cyber Defense Summit 2015
Nashville, TN | August 11-18
(Cyber Defense Challenge held on August 11)
sans.org/event/cyber-defense-summit-and-training-2015

SANS Cyber Defense San Diego 2015
San Diego, CA | October 19-23
(Cyber Defense Challenge held on October 22)
sans.org/cyberdefense

1 Finalist (Nashville)
2 Finalists (San Diego)
+ 2 Virtual Finalists (High Scorers)

1 Ultimate Cyber Defender
(Crowned in San Diego)

VIRTUAL CONTEST

From 250 online competitors, two finalists with the highest scores will be chosen (Oct. 1) to compete in the finals at San Diego (Oct. 23).

FINALS (ULTIMATE CYBER DEFENDER)

Five finalists (one from Nashville, two from San Diego, and the two highest scorers from Virtual) will compete in San Diego in the Defender Challenge (Oct. 23).

PRIZES

At **SANS Cyber Defense San Diego 2015**, one talented competitor will become the Grand Prize Winner and be named Ultimate Cyber Defender 2015 (SAN DIEGO). Here's a list of the top prizes:

Grand-Prize Winner

- Your choice of a SANS Cyber Defense training course and GIAC Certification Attempt at next year's Cyber Defense San Diego (2016) – Value $6,000
- 1st-place Ultimate Cyber Defender 2015 (SAN DIEGO) trophy
- Certificate of participation
- Bragging rights – *PRICELESS!*

2nd-Place Winner

- Free GIAC Certification attempt – Value $1,099
- 2nd-place Cyber Defender 2015 (SAN DIEGO) trophy
- Certificate of participation

3rd-Place Winner

- $250 gift card
- 3rd-place Cyber Defender 2015 (SAN DIEGO) trophy
- Certificate of participation

Regional Winner (Nashville)

The winner of the competition at Nashville (Aug. 11) will qualify for the finals in San Diego (Oct. 23). As a finalist in San Diego, you will receive an all-expense-paid trip (air, lodging, and meals per diem)* to **SANS Cyber Defense San Diego 2015** to compete in the finals.

Online Winners (2)

On October 1, the two highest scoring virtual competitors will be declared the winners and will be eligible to compete in the finals in San Diego (Oct. 23). As a finalist in San Diego, you will receive an all-expense-paid trip (air, lodging, and meals per diem)* to **SANS Cyber Defense San Diego 2015** to compete in the finals.

Weekly Winners via Social Media

We'll also award prizes each week to the top competitors who participate via social media. The prizes will include gift cards for Amazon.com, Restaurant.com, Subway, Home Depot, and Staples.com, and other retailers. The weekly winners will be announced via the leaderboard.

**Lodging is for two nights (October 22 & 23); airfare is limited to coach and the ticket should not exceed $800*

QUESTIONING

In the Regionals, contestants will be asked questions that are similar to what you might find on a Global Information Assurance Certification (GIAC) exam.

The Finals (Defender Challenge) will feature tougher questions, similar to what you might find on the GIAC-GSE Exam. World-class SANS instructors and well-known industry experts will serve as judges and preside over the competition.

The Cyber Defense Curriculum is pleased to partner with GIAC because GIAC certification ensures that certified security professionals have hands-on technical skills based on the most up-to-date security information. Certification helps to ensure that professionals can actually perform the tasks necessary to defend and protect computer network systems and the critical informational assets that reside on them. Learn more about GIAC at www.giac.org.

POINT SYSTEM

Competitors earn points when they register, answer GIAC questions, and participate and engage via social media. More participation will lead to more points and increase the chance of becoming a semifinalist. Anyone who registers to compete will receive an initial 100 points. Registered participants will receive an email with instructions on how to earn additional points.

Competitors will earn points online when they answer the monthly survey questions. Each question is worth 50 points. One competitor may earn up to 500 points per quiz. Competitors also may earn bonus points through any of the following:

- Creating high-quality content to engage the cybersecurity community
- Sharing interesting topics or information they've learned about or from a SANS course
- Participating in an online forum

Each week competitors will have the opportunity to earn weekly prizes on social media. Postings will be sent via email, twitter, and blogs. Follow these accounts to stay in the know: @SANSInstitute, @SANSdefense, and @DrEricCole.

REGISTRATION

Enter Early and Stay Up-To-Date

The SANS Cyber Defense Challenge 2015 competition will be launched virtually via social media. Participants can enter online beginning this July. The deadline to enter is September 1, 2015. The earlier you enter, the better your chance to compete because there are only 25 slots per venue. Although there is no purchase necessary to enter, participants who wish to compete at a Regional Competition must register at http://cyber-defense.sans.org/blog prior to the event. Students who have registered and paid to attend (Nashville and San Diego) can also register to participate in the competition at the event. Check twitter and follow @SANSDefense or visit http://cyber-defense.sans.org/blog for updates.

You need to be knowledgeable, and you need to be fast.

REGISTER AT
http://cyber-defense.sans.org/blog

RESTRICTIONS: SANS Cyber Defense Challenge 2015 (the Challenge) is open to legal residents of the fifty (50) United States and the District of Columbia who are at least eighteen (18) years old at the time of entry. Employees of SANS and other companies associated with the promotion of the Challenge, and their respective parents, subsidiaries, affiliates and advertising and promotion agencies as well as the immediate family (spouse, parents, siblings, and children) and household members of each such employee are not eligible. The Challenge is subject to federal, state, and local laws and regulations.