Discover the SANS Cyber Defense Difference.

Download a free Cyber Defense curriculum roadmap at

cyber-defense.sans.org/training/roadmap
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.
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 participate in SANS events and programs 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 to challenge the adversary.”

-Dr. Eric Cole, is a cybersecurity expert, SANS Fellow and author of Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization
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 the 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.
SEC301 is an introductory course that provides the fastest path to get up to speed in information security. Written and taught by battle-scarred security veterans, this entry-level five-day course covers a broad spectrum of security topics, and is liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security and the basics of risk management.
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

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 areas 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!

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
This comprehensive six-day 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.
Build a Defensive Network that Can Withstand Attacks!

“SEC502 opened my eyes so wide, it scared me.”
—GEORGE SCARBOROUGH, DEFENSE LOGISTICS AGENCY

You will learn how to:
- Perform packet-level analysis to understand traffic on the wire
- Conduct firewall protection hands-on by configuring and testing a network firewall
- Perform perimeter assessment
- Lock down routers
- Understand authentication, encryption, and VPN basics
- Understand cloud security implications
- Use network mapping and monitoring tools

sans.org/sec502

SEC502 is a comprehensive analysis of a wide breadth of technologies covering multiple security techniques to help you defend your network from remote attacks. A proper security posture must be comprised of multiple layers. The six-day course starts by looking at common problems we need to resolve. Is there traffic passing by my firewall I didn’t expect? How did my system get compromised when no one can connect to it from the Internet? Is there a better solution than anti-virus for controlling malware? We’ll dig into these questions and more and answer them.
Intrusion Detection
In-Depth

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

“Today has been brilliant, bringing all of our skills together to achieve the challenge.
-Hayley Roberts, MOD

This six-day 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.

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

sans.org/sec503
Windows Is on the Front Line in the APT Malware Battlefield. We Will Teach You How to Win!

“They is by far the best class I’ve ever taken for Windows.”

- ROB TRUJILLO, U.S. COURTS

How can we deal with pass-the-hash attacks, token abuse, administrator account compromise, and the lateral movement of hackers inside our networks? How do we actually implement the Critical Security Controls on Windows in a large environment? How can we significantly reduce the client-side exploits that lead to malware infections? These are tough problems, but we tackle them in SEC505. This six-day course will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) certification exam.
Securing Linux/Unix

Some of the Most Critical Systems in Your Organizations are Unix. Learn How To Protect Them!

“\textit{I’ve been a Unix systems administrator for a couple of decades, but in SEC506 I learned something new every day.}”

-Martin Hristov, Sony

You will learn how to:
\begin{itemize}
  \item Reduce the attack surface of Linux/Unix and disable unnecessary services
  \item Protect your systems from buffer overflows and DoS
  \item Deploy SSH to protect administrative sessions and leverage functionality
  \item Use sudo to control and monitor administrative access
  \item Create a centralized logging infrastructure with Syslog-NG
  \item Deploy log monitoring tools to scan for significant events
  \item Securely configure Apache, BIND, and Sendmail
\end{itemize}

sans.org/sec506

Learn in-depth coverage of Linux and Unix security issues. Examine how to mitigate or eliminate general problems that apply to all Unix-like operating systems, including vulnerabilities in the password authentication system, file system, virtual memory system, and applications that commonly run on Linux and Unix. Throughout this six-day course you will become skilled at utilizing freely available tools to handle security issues, including SSH, AIDE, sudo, Isof, and many others.
Continuous Monitoring and Security Operations

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

“No other training has provided such good, in-depth coverage of the real defensive techniques that can work.”

-Roderick Nixon, BPMI

You will learn how to:

- 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.
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 a way that will enable you to quickly implement those defenses in your environment as soon as you return to work.
Implementing and Auditing the Critical Security Controls – In-Depth

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 Public Utility District

You will learn how to:

› Apply a security framework based on actuals threats to defend against attacks
› Use tools that implement the Controls through automation
› 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
› Audit each Control

This in-depth five-day 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.

sans.org/sec566
This six-day course provides you with the expert instruction, case studies, CISSP® study guide, supplemental test questions, and hands-on training and knowledge you need to pass the CISSP® exam. MGT414 is absolutely the best way to prepare for your CISSP® certification and to learn the core principles of the Ten CISSP® Domains of Knowledge.
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.

**Why Is Cyber Defense Critical?**

Whether an attacker is successful penetrating an organization’s network depends on how well that organization can defend itself. While defending against attacks is an ongoing challenge, with new threats emerging all the time and the advanced persistent threat (APT) on everyone’s mind, organizations need to understand what 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 budget or allocates any resources or time on anything in the name of cybersecurity, three questions must be answered:

1. **What is the risk?**
2. **Is it the highest priority risk?**
3. **What is the most cost-effective way to reduce the risk?**

Security is all about making sure you are focusing in on the right areas of defense.

---

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?

2. **Align the Defense with the Offense**
   - **1** Reconnaissance
   - **2** Scanning
   - **3** Exploitation
   - **4** Creating backdoors
   - **5** Covering tracks

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

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

5. **Common Metrics**
   - Utilize the Critical Controls:
     - 1 Offense informing the defense
     - 2 Automation and continuous monitoring of security
     - 3 Metrics to drive measurement and compliance
How Are You Protecting Your

Data?

Network?

Systems?

Critical Infrastructure?

Get GIAC certified!

GIAC offers over 30 specialized certifications in security, digital forensics, penetration testing, web application security, IT audit, management, and IT security law, including:

- SEC301: GIAC Information Security Fundamentals (GISF)
- SEC401: GIAC Security Essentials (GSEC)
- SEC501: GIAC Certified Enterprise Defender (GCED)
- SEC502: GIAC Certified Perimeter Protection Analyst (GPPA)
- SEC503: GIAC Certified Intrusion Analyst (GCIA)
- SEC505: GIAC Certified Windows Security Administrator (GCWN)
- SEC506: GIAC Certified UNIX Security Administrator (GCUX)
- SEC511: GIAC Continuous Monitoring Certification (GMON)
- SEC566: GIAC Critical Controls Certification (GCCC)
- MGT414: GIAC Information Security Professional (GISP)

SANS Technology Institute transforms the world’s best cybersecurity training and certifications into a comprehensive and rigorous graduate education experience.

Master’s Degree Programs:

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

Specialized Graduate Certificates:

- Cybersecurity Engineering (Core)
- Cyber Defense Operations
- Penetration Testing and Ethical Hacking
- Incident Response

Eligible for Veterans Education benefits!

Earn industry-recognized GIAC certifications throughout the program.

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

GI Bill® is a registered trademark of the U.S. Department of Veterans Affairs (VA).

More information about education benefits offered by VA is available at the official U.S. government website at www.benefits.va.gov/gibill.
<table>
<thead>
<tr>
<th><strong>SANS TRAINING FORMATS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LIVE CLASSROOM TRAINING</strong></td>
</tr>
<tr>
<td><strong>Multi-Course Training Events</strong></td>
</tr>
<tr>
<td>Live Instruction From SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking With Your Peers</td>
</tr>
<tr>
<td>sans.org/security-training/by-location/all</td>
</tr>
<tr>
<td><strong>Community SANS</strong></td>
</tr>
<tr>
<td>Live Training in Your Local Region with Smaller Class Sizes</td>
</tr>
<tr>
<td>sans.org/community</td>
</tr>
<tr>
<td><strong>Private Training</strong></td>
</tr>
<tr>
<td>Your Location! Your Schedule!</td>
</tr>
<tr>
<td>sans.org/private-training</td>
</tr>
<tr>
<td><strong>Mentor</strong></td>
</tr>
<tr>
<td>Live Multi-Week Training with a Mentor</td>
</tr>
<tr>
<td>sans.org/mentor</td>
</tr>
<tr>
<td><strong>Summit</strong></td>
</tr>
<tr>
<td>Live IT Security Summits and Training</td>
</tr>
<tr>
<td>sans.org/summit</td>
</tr>
<tr>
<td><strong>ONLINE TRAINING</strong></td>
</tr>
<tr>
<td><strong>OnDemand</strong></td>
</tr>
<tr>
<td>E-learning Available Anytime, Anywhere, At Your Own Pace</td>
</tr>
<tr>
<td>sans.org/ondemand</td>
</tr>
<tr>
<td><strong>vLive</strong></td>
</tr>
<tr>
<td>Convenient Online Instruction From SANS' Top Instructors</td>
</tr>
<tr>
<td>sans.org/vlive</td>
</tr>
<tr>
<td><strong>Simulcast</strong></td>
</tr>
<tr>
<td>Attend a SANS Training Event Without Leaving Home</td>
</tr>
<tr>
<td>sans.org/simulcast</td>
</tr>
<tr>
<td><strong>OnDemand Bundles</strong></td>
</tr>
<tr>
<td>Extend Your Training with an OnDemand Bundle Including Four Months of E-learning</td>
</tr>
<tr>
<td>sans.org/ondemand/bundles</td>
</tr>
<tr>
<td><strong>SelfStudy</strong></td>
</tr>
<tr>
<td>Self-Paced Online Training for the Motivated and Disciplined Infosec Student</td>
</tr>
<tr>
<td>sans.org/selfstudy</td>
</tr>
</tbody>
</table>