SANS

The Most Trusted Source for Information Security Training,
Certification, and Research

BALTIMORE FALL 2017

September 25-30

Protect Your Business and Advance Your Career

10 hands-on, immersion-style information security courses taught by real-world practitioners

CYBER DEFENSE

ETHICAL HACKING

PENETRATION TESTING

DIGITAL FORENSICS

MANAGEMENT

GIAC CERTIFICATIONS

> "SANS has some of the best security-related classes I have ever been to. The instructors are excellent and the material is always current."
>
> -Daniel Touchette, Enterprise Holdings, Inc.

SAVE $400

Register and pay by Aug 2nd –
Use code **EarlyBird17**

www.sans.org/baltimore-fall

SANS Baltimore Fall 2017 SEPTEMBER 25-30

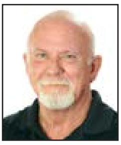
SANS Instructors

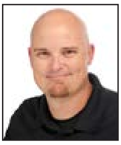
SANS instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses. This guarantees that what you learn in class will be up to date and relevant to your job. The SANS Baltimore Fall 2017 lineup of instructors includes:

David Cowen
Certified Instructor
@hecfblog

Bryce Galbraith
Principal Instructor
@brycegalbraith

G. Mark Hardy
Principal Instructor
@g_mark


Paul A. Henry
Senior Instructor
@phenrycissp


David Mashburn
Instructor
@d_mashburn

Jeff McJunkin
Instructor
@jeffmcjunkin

David R. Miller
Certified Instructor
@DRM_CyberDude

My-Ngoc Nguyen
Certified Instructor
@MenopN

Anuj Soni
Certified Instructor
@asoni

Dr. Johannes Ullrich
Senior Instructor
@johullrich

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 11.

KEYNOTE: ***The Internet of Evil Things*** – Dr. Johannes Ullrich

The Red Pill. Become Aware: Squashing Security Misconceptions and More – My-Ngoc Nguyen

Anti-Ransomware: How to Turn the Tables – G. Mark Hardy

Malware Analysis: House Rules – Anuj Soni

Save $400 when you register and pay by August 2nd using code EarlyBird17

Courses at a Glance

<table>
<tr><th></th><th></th><th>MON 9-25</th><th>TUE 9-26</th><th>WED 9-27</th><th>THU 9-28</th><th>FRI 9-29</th><th>SAT 9-30</th></tr>
<tr><td>SEC301</td><td>Intro to Information Security</td><td colspan="5">Page 1</td><td></td></tr>
<tr><td>SEC401</td><td>Security Essentials Bootcamp Style</td><td colspan="6">Page 2 SIMULCAST</td></tr>
<tr><td>SEC501</td><td>Advanced Security Essentials – Enterprise Defender</td><td colspan="6">Page 3 SIMULCAST</td></tr>
<tr><td>SEC503</td><td>Intrusion Detection In-Depth</td><td colspan="6">Page 4 SIMULCAST</td></tr>
<tr><td>SEC504</td><td>Hacker Tools, Techniques, Exploits, and Incident Handling</td><td colspan="6">Page 5</td></tr>
<tr><td>SEC560</td><td>Network Penetration Testing and Ethical Hacking</td><td colspan="6">Page 6</td></tr>
<tr><td>FOR500</td><td>Windows Forensic Analysis (FORMERLY FOR408)</td><td colspan="6">Page 7</td></tr>
<tr><td>FOR610</td><td>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td><td colspan="6">Page 8 NEW! SIMULCAST</td></tr>
<tr><td>MGT414</td><td>SANS Training Program for CISSP® Certification</td><td colspan="6">Page 9</td></tr>
<tr><td>MGT514</td><td>IT Security Strategic Planning, Policy, and Leadership</td><td colspan="5">Page 10</td><td></td></tr>
</table>

Register today for SANS Baltimore Fall 2017!
www.sans.org/baltimore-fall

@SANSInstitute
Join the conversation:
#SANSBaltimore

SEC301

Intro to Information Security

GISF Certification
Information Security Fundamentals
www.giac.org/gisf

Five-Day Program
Mon, Sep 25 - Fri, Sep 29
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: My-Ngoc Nguyen

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

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

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

This course is designed for students who have a basic knowledge of computers and technology but no prior knowledge of cybersecurity. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

Written by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next course up the line, **SEC401: Security Essentials Bootcamp Style**. It also delivers on the ***SANS promise: You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.***

> "Labs reinforced the security principles in a real-world scenario."
> -Tyler Moore, Rockwell

> "This is the perfect course for establishing a foundation of information security, and the instructor is very knowledgeable and well-versed in the topics."
> -Stephen Pridmore, Protective Life

▶II
Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

My-Ngoc Nguyen *SANS Certified Instructor*

My-Ngoc Nguyen (pronounced Mee-Nop Wynn) is the CEO/Principal Consultant for Secured IT Solutions. She has 15 years of experience in information systems and technology, with the past 12 years focused on cybersecurity and information assurance for both the government and commercial sectors. My-Ngoc is highly experienced in IT security and risk methodologies, and in legal and compliance programs. She led a cybersecurity program under a federal agency for a highly-regulated, first-of-a-kind project of national importance. With that experience, she has been helping client organizations in both the public and private sectors implement secure and compliant business processes and IT solutions using defense-in-depth and risk-based approaches. Along with a master's degree in management information systems, she has top security certifications that include GPEN, GCIH, GSEC, and CISSP, and is a former QSA. She is a member of the FBI's InfraGard, the Information Systems Security Association (ISSA), the Information Systems Audit and Control Association (ISACA), and the International Information Systems Security Certification Consortium (ISC). My-Ngoc founded the non-profit organization CyberSafeNV to raise security awareness among Nevada residents and is currently the organization's chairperson. @MenopN

SEC401

GSEC Certification
Security Essentials
www.giac.org/gsec

Security Essentials Bootcamp Style

Six-Day Program
Mon, Sep 25 - Sat, Sep 30
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Bryce Galbraith

Who Should Attend

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

> "This course has opened my eyes to just how important security is, and has given me a deeper understanding of how to protect our systems."
> -Travis Sorensen, Xpress Solutions

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

STOP and ask yourself the following questions:

- **Do you fully understand why some organizations get compromised and others do not?**
- **If there were compromised systems on your network, are you confident you would be able to find them?**
- **Do you know the effectiveness of each security device and are you certain they are all configured correctly?**
- **Are proper security metrics set up and communicated to your executives to drive security decisions?**

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

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

Prevention Is Ideal but Detection Is a Must

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

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

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

Bryce Galbraith *SANS Principal Instructor*

As a contributing author of the internationally bestselling book *Hacking Exposed: Network Security Secrets & Solutions*, Bryce 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. He was a member of Foundstone's renowned penetration testing team, and he served as a senior instructor and co-author of Foundstone's 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**

SEC501

GCED Certification
Certified Enterprise Defender
www.giac.org/gced

Advanced Security Essentials – Enterprise Defender

Six-Day Program
Mon, Sep 25 - Sat, Sep 30
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Paul A. Henry

Who Should Attend

- Incident response and penetration testers
- Security Operations Center engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

> "SEC501 is the best SANS course I've taken. The content is relevant, the labs were interactive. I strongly recommend it for SOC analysts and IR professionals."
> -Brett Smetanka, KeyBank

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. **SEC501: Advanced Security Essentials – Enterprise Defender** builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

It has been said of security that "prevention is ideal, but detection is a must." However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured, regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

> "The hands-on lab approach is a great way to make sense of what is being taught, and working with other classmates helped expand our knowledge and brought cohesion." -Rachel Weiss, UPS Inc.

Despite an organization's best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organizations need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, looking for indications of an attack, and performing penetration testing and vulnerability analysis against your organization to identify problems and issues before a compromise occurs.

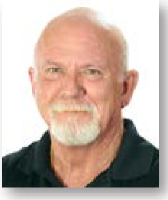
Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

SANS Technology Institute
www.sans.edu

www.sans.org/8140

▶❚❚ Bundle OnDemand
with this course
www.sans.org/ondemand

Also available via Simulcast
See page 13 for details.



Paul A. Henry *SANS Senior Instructor*

Paul is one of the world's foremost global information security and computer forensic experts, with more than 20 years' 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 key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. He 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 and telecommunications projects throughout Southeast Asia. Paul is frequently cited by major publications as an expert on perimeter security, incident response, computer forensics, 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 is a featured speaker at seminars and conferences worldwide, delivering presentations on diverse topics such as anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, perimeter security, and incident response. **@phenrycissp**

SEC503

Intrusion Detection In-Depth

GCIA Certification
Certified Intrusion Analyst
www.giac.org/gcia

Six-Day Program
Mon, Sep 25 - Sat, Sep 30
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Dr. Johannes Ullrich

Who Should Attend

- Intrusion detection (all levels), system, and security analysts
- Network engineers/ administrators
- Hands-on security managers

> "Having taken several SANS courses, this one provided clear and concise information from an instructor who did an excellent job keeping the material interesting – well done."
> -David Holland, Stroz Friedberg Special Investigations

Also available via Simulcast
See page 13 for details.

Reports of prominent organizations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?

Preserving the security of your site in today's threat environment is more challenging than ever before. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and sometimes vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in **SEC503: Intrusion Detection In-Depth** is to acquaint you with the core knowledge, tools, and techniques to defend your networks with insight and awareness. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

Mark Twain said, "It is easier to fool people than to convince them that they've been fooled." Too many IDS/IPS solutions provide a simplistic red/green, good/bad assessment of traffic and too many untrained analysts accept that feedback as the absolute truth. This course emphasizes the theory that a properly trained analyst uses an IDS alert as a starting point for examination of traffic, not as a final assessment. SEC503 imparts the philosophy that the analyst must have access to alerts and the ability to examine them in order to give them meaning and context. You will learn to investigate and reconstruct activity to determine if it is noteworthy or a false indication.

SEC503: Intrusion Detection In-Depth delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to master different open-source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material.

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

Bundle OnDemand
WITH THIS COURSE
www.sans.org/ondemand

Dr. Johannes Ullrich *SANS Senior Instructor*

As Dean of Research for the SANS Technology Institute, Johannes is currently responsible for the SANS Internet Storm Center (ISC) and the GIAC Gold program. In 2000, he founded DShield.org, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. Prior to joining SANS, Johannes worked as a lead support engineer for a web development company and as a research physicist. Johannes holds a PhD in physics from SUNY Albany and is based in Jacksonville, Florida. His daily podcast summarizes current security news in a concise format. **@johullrich** **@sans_isc**

SEC504

Hacker Tools, Techniques, Exploits, and Incident Handling

GCIH Certification
Incident Handler
www.giac.org/gcih

Six-Day Program
Mon, Sep 25 - Sat, Sep 30
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
(If your laptop supports only wireless, please bring a USB Ethernet adapter.)
Instructor: David Mashburn

Who Should Attend

- Incident handlers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

"This is an amazing opportunity to understand how the people we are battling with think!"
-Dan McKibben, Nationwide Insurance

"SEC504 showed me the how and why for the things I've been monitoring."
-Michael Shaver, Sony Network Entertainment International

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection and one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. **As defenders, it is essential we understand these hacking tools and techniques.**

"Fills the gap of 'here's what adversaries do and the evidence it leaves.'"
-Kevin Heithaus, JPMorgan Chase

This course enables you to turn the tables on computer attackers by helping you understand their tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan. It addresses the latest cutting-edge, insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents and a detailed description of how attackers undermine systems so you can prepare for, detect, and respond to those attacks. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning, exploiting, and defending systems. **This course will enable you to discover the holes in your system before the bad guys do!**

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. General security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

www.sans.org/8140

▶❚❚ **Bundle OnDemand**
WITH THIS COURSE
www.sans.org/ondemand

David Mashburn *SANS Instructor*

David Mashburn is currently the IT security manager for a global non-profit organization in the Washington, D.C. area. He also has worked as an IT security professional for several civilian federal agencies, and has over 15 years of experience in IT. He holds a master's degree in computer science from John Hopkins University, and a B.S. from the University of Maryland at College Park. David holds multiple security-related certifications, including the CISSP, GPEN, GCIH, GCIA, and CEH. He is also a member of the SANS/GIAC Advisory Board, and has previously taught courses in the cybersecurity curriculum at the University of Maryland – University College. @d_mashburn

SEC560

Network Penetration Testing and Ethical Hacking

GPEN Certification
Penetration Tester
www.giac.org/gpen

Six-Day Program
Mon, Sep 25 - Sat, Sep 30
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Jeff McJunkin

Who Should Attend

- Security personnel whose jobs involve assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red and blue team members
- Forensics specialists who want to better understand offensive tactics

> "As a career 'network defender' this course makes me feel I will be more well-rounded."
> -Chris Frighelis, Fibernet

> "I like that the labs provided clear step-by-step guidance. The instructor's level of knowledge and ability to relay information was fantastic."
> - Bryan Barnhart, Infiltration Labs

As a cybersecurity professional, you have a unique responsibility to find and understand your organization's vulnerabilities, and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this task head-on.

SEC560 is the must-have course for every well-rounded security professional.

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step-by-step and end-to-end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. **The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with more than 30 detailed hands-on labs throughout.** The course is chock-full of practical, real-world tips from some of the world's best penetration testers to help you do your job safely, efficiently...and masterfully.

Learn the best ways to test your own systems before the bad guys attack.

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test – and on the last day of the course you'll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the knowledge you've mastered in this course.

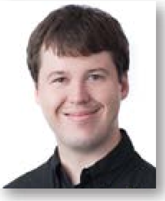
You will bring comprehensive penetration testing and ethical hacking know-how back to your organization.

You will learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover run-of-the-mill options and configurations, we'll also go over the lesser-known but super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

Bundle OnDemand
with this course
www.sans.org/ondemand



Jeff McJunkin *SANS Instructor*

Jeff McJunkin is a senior staff member at Counter Hack Challenges with more than nine years of experience in systems and network administration and network security. His greatest strength is his breadth of experience – from network and web application penetration testing to digital/mobile forensics, and from technical training to systems architecture. Jeff is a computer security/information assurance graduate of Southern Oregon University and holds many professional certifications. He has also competed in many security competitions, including taking first place at a regional NetWars competition and a U.S. Cyber Challenge capture-the-flag competition. He also joined the Red Team for the Pacific Rim Collegiate Cyber Defense Competition. His personal blog can be found at http://jeffmcjunkin.com/. @jeffmcjunkin

FOR500 (Formerly FOR408)

Windows Forensic Analysis

GCFE Certification
Forensic Examiner
www.giac.org/gcfe

Six-Day Program
Mon, Sep 25 - Sat, Sep 30
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: David Cowen

Who Should Attend

- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

> "The course content was excellent and well presented. From start to finish, there were many different pieces of information that went into solving the main time-line of events."
>
> -Chris Then, Morris County, NJ Prosecutor's Office

MASTER WINDOWS FORENSICS – YOU CAN'T PROTECT WHAT YOU DON'T KNOW ABOUT

All organizations must prepare for cyber-crime occurring on their computer systems and within their networks. Demand has never been greater for analysts who can investigate crimes such as fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover vital intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation experts capable of piecing together what happened on computer systems second by second.

FOR500: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and artifacts is a core component of information security. You'll learn how to recover, analyze, and authenticate forensic data on Windows systems, track particular user activity on your network, and organize findings for use in incident response, internal investigations, and civil/criminal litigation. You'll be able to use your new skills to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unbelievable amount of data about you and your users. FOR500 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7, Windows 8/8.1, Windows 10, Office and Office365, cloud storage, SharePoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques, prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows 7 systems to just-discovered Windows 10 artifacts.

FOR500: Windows Forensic Analysis will teach you to:

- **Conduct in-depth forensic analysis of Windows operating systems and media exploitation focusing on Windows 7, Windows 8/8.1, Windows 10, and Windows Server 2008/2012/2016**
- **Identify artifact and evidence locations to answer critical questions, including application execution, file access, data theft, external device usage, cloud services, geolocation, file download, anti-forensics, and detailed system usage**
- **Focus your capabilities on analysis instead of on how to use a particular tool**
- **Extract critical answers and build an in-house forensic capability via a variety of free, open-source, and commercial tools provided within the SANS Windows SIFT Workstation**

David Cowen *SANS Certified Instructor*

David Cowen is a Partner at G-C Partners, LLC, where his team of expert digital forensics investigators pushes the boundaries of what is possible on a daily basis. He has been working in digital forensics and incident response since 1999 and has performed investigations covering thousands of systems in the public and private sector. Those investigations have involved everything from revealing insider threats to serving as an expert witness in civil litigation and providing the evidence to put cyber criminals behind bars. David has authored three series of books on digital forensics: *Hacking Exposed Computer Forensics* (1st-3rd editions); *Infosec Pro Guide to Computer Forensics*; and the *Anti Hacker Toolkit* (3rd Edition). His research into file system journaling forensics has created a new area of analysis that is changing the industry. Combined with Triforce products, David's research enables examiners to go back in time to find previously unknown artifacts and system interactions. David is a Certified Information Systems Security Professional (CISSP) and a GIAC Certified Forensic Examiner. He is the winner of the first SANS DFIR NetWars and a SANS Lethal Forensicator whose passion for digital forensics can be seen in everything he does. He started in 1996 as a penetration tester and has kept up his information security knowledge by acting as the Red Team captain for the National Collegiate Cyber Defense Competition for the last nine years. **@hecfblog**

FOR610

GREM Certification
Reverse Engineering Malware
www.giac.org/grem

Reverse-Engineering Malware: Malware Analysis Tools and Techniques *NEW!*

Six-Day Program
Mon, Sep 25 - Sat, Sep 30
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Anuj Soni

Who Should Attend

- Individuals who have dealt with incidents involving malware and want to learn how to understand key aspects of malicious programs
- Technologists who have informally experimented with aspects of malware analysis prior to the course and are looking to formalize and expand their expertise in this area
- Forensic investigators and IT practitioners looking to expand their skillsets and learn how to play a pivotal role in the incident response process

Learn to turn malware inside out! This popular course explores malware analysis tools and techniques in depth. FOR610 training helps forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems.

Understanding the capabilities of malware is critical to an organization's ability to derive threat intelligence, respond to information security incidents, and fortify defenses. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and many other freely available tools.

The course begins by establishing the foundation for analyzing malware in a way that dramatically expands upon the findings of automated analysis tools. You will learn how to set up a flexible laboratory to examine the inner workings of malicious software, and how to use the lab to uncover characteristics of real-world malware samples. You will also learn how to redirect and intercept network traffic in the lab to explore the specimen's capabilities by interacting with the malicious program.

Malware is often obfuscated to hinder analysis efforts, so the course will equip you with the skills to unpack executable files. You will learn how to dump such programs from memory with the help of a debugger and additional specialized tools, and how to rebuild the files' structures to bypass the packer's protection. You will also learn how to examine malware that exhibits rootkit functionality to conceal its presence on the system, employing code analysis and memory forensics approaches to examining these characteristics.

FOR610 malware analysis training also teaches how to handle malicious software that attempts to safeguard itself from analysis. You will learn how to recognize and bypass common self-defensive measures, including code injection, sandbox evasion, flow misdirection, and other measures.

Hands-on workshop exercises are a critical aspect of this course. They enable you to apply malware analysis techniques by examining malicious software in a controlled and systematic manner. When performing the exercises, you will study the supplied specimens' behavioral patterns and examine key portions of their code. To support these activities, you will receive pre-built Windows and Linux virtual machines that include tools for examining and interacting with malware.

Anuj Soni *SANS Certified Instructor*

Anuj Soni initially pursued a career fighting cybercrime for the thrill of the hunt. These days, Anuj feeds his passion for technical analysis through his role as a Senior Threat Researcher at Cylance, where he performs malware research and reverse engineering. Anuj also brings his problem-solving abilities to his position as a SANS Certified Instructor, which gives him the opportunity to impart his deep technical knowledge and practical skills to students. When teaching Reverse-Engineering Malware (FOR610) and Advanced Digital Forensics and Incident Response (FOR508), Anuj emphasizes establishing goals for analysis, creating and following a process, and prioritizing tasks. Since entering the information security field in 2005, Anuj has performed numerous intrusion investigations to help government and commercial clients mitigate attacks against the enterprise. His malware hunting and technical analysis skills have resulted in the successful identification, containment, and remediation of multiple threat actor groups. @asoni

MGT414

GISP Certification
Information Security Professional
www.giac.org/gisp

SANS Training Program for CISSP® Certification

Six-Day Program
Mon, Sep 25 - Sat, Sep 30
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: David R. Miller

Who Should Attend

- Security professionals who are interested in understanding the concepts covered on the CISSP® exam as determined by (ISC)^2
- Managers who want to understand the critical areas of information security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® eight domains
- Security professionals and managers looking for practical ways the eight domains of knowledge can be applied to their current job

www.sans.org/8140

▶II **BUNDLE ONDEMAND**
WITH THIS COURSE
www.sans.org/ondemand

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam.

MGT414 focuses solely on the eight domains of knowledge as determined by (ISC)^2 that form a critical part of the CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

Obtaining Your CISSP® Certification Consists of:

- **Fulfilling minimum requirements for professional work experience**
- **Completing the Candidate Agreement**
- **Review of your résumé**
- **Passing the CISSP® 250 multiple-choice question exam with a scaled score of 700 points or greater**
- **Submitting a properly completed and executed Endorsement Form**
- **Periodic audit of CPEs to maintain the credential**

"Best security training I have ever received and just the right amount of detail for each domain."
-Tony Barnes, United States Sugar Corporation

"It was extremely valuable to have an experienced information security professional teaching the course as he was able to use experiential knowledge in examples and explanations."
-Sean Hoar, Davis Wright Tremaine

"I think the course material and the instructor are very relevant for the task of getting a CISSP®. The overall academic exercise is solid."
-Aaron Lewter, Availity

David R. Miller *SANS Certified Instructor*

David has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on information system security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security program, including through policy writing, network architecture design (including security zones), development of incident response teams and programs, design and implementation of public key infrastructures, security awareness training programs, specific security solution designs such as secure remote access and strong authentication architectures, disaster recovery planning and business continuity planning, and pre-audit compliance gap analysis and remediation. He serves as a security lead and forensic investigator on numerous enterprise-wide IT design and implementation projects for Fortune 500 companies, providing compliance, security, technology, and architectural recommendations and guidance. His current projects include work on Microsoft Windows Active Directory enterprise designs, security information and event management systems, intrusion detection and protection systems, endpoint protection systems, patch management systems, configuration monitoring systems, and enterprise data encryption for data at rest, in transit, in use, and within email systems. David is an author, lecturer and technical editor of books, curriculum, certification exams, and computer-based training videos. **@DRM_CyberDude**

MGT514

GIAC CERTIFICATION COMING SOON! GSTRT

IT Security Strategic Planning, Policy, and Leadership

Five-Day Program
Mon, Sep 25 - Fri, Sep 29
9:00am - 5:00pm
30 CPEs
Laptop NOT Needed
Instructor: G. Mark Hardy

Who Should Attend

- CISOs
- Information security officers
- Security directors
- Security managers
- Aspiring security leaders
- Other security personnel who have team lead or management responsibilities

> "I moved into management a few years ago and am currently working on a new security strategy/roadmap and this class just condensed the past two months of my life into a one-week course and I still learned a lot!"
>
> -Travis Evans, SiriusXM

As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to do three things:

• Develop Strategic Plans
Strategic planning is hard for people in IT and IT security, because we spend so much time responding and reacting. We almost never get to practice until we get promoted to a senior position, and then we are not equipped with the skills we need to run with the pack. Learn how to develop strategic plans that resonate with other IT and business leaders.

• Create Effective Information Security Policy
Policy is a manager's opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and your response was, "No way, I am not going to do that!"? Policy must be aligned with an organization's culture. We will break down the steps to policy development so that you have the ability to develop and assess policy to successfully guide your organization.

• Develop Management and Leadership Skills
Leadership is a capability that must be learned, exercised, and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organization's mission. Learn to utilize management tools and frameworks to better lead, inspire, and motivate your teams.

How the Course Works

Using case studies from Harvard Business School, team-based exercises, and discussions that put students in real-world scenarios, students will participate in activities they can carry out with their own team members when they return to work.

The next generation of security leadership must bridge the gap between security staff and senior leadership by strategically planning how to build and run effective security programs. After taking this course, you will have the fundamental skills to create strategic plans to protect your company, enable key innovations, and work effectively with your business partners.

G. Mark Hardy *SANS Principal Instructor*

G. Mark Hardy is the founder and president of the National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 35 years, and is an internationally recognized expert and keynote speaker who has made presentations at over 250 events world-wide. He provides consulting services as a virtual CISO, expert witness testimony, and domain expertise in blockchain and cryptocurrency. He serves on the Advisory Board of CyberWATCH, an Information Assurance/ Information Security Advanced Technology Education Center of the National Science Foundation. Mark is a retired U.S. Navy captain who was entrusted with nine command assignments, including responsibility for leadership training for 70,000 sailors. A graduate of Northwestern University, he holds a BS in computer science, a BA in mathematics, a masters in business administration, and a masters in strategic studies. He also holds the GSLC, CISSP, CISM and CISA certifications. @g_mark

Bonus Sessions

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

KEYNOTE: The Internet of Evil Things

Dr. Johannes Ullrich

Embedded systems are the new target. As our networks grow uncontrolled and unsupervised, forgotten machines will take over and soon rule us all. Analyzing the embedded malware that comes with this presents a number of challenges. Current debuggers and virtualization techniques that mimic these systems are incomplete and will not allow us to completely analyze malware the way we are used to in good old desktop malware environments. These malware blackboxes need different instrumentations and techniques. We will present some ideas on how to analyze these malware samples, and introduce you to embedded system analysis (unless your bot is removing this event from your smart watch's reminder list).

The Red Pill. Become Aware: Squashing Security Misconceptions and More

My-Ngoc Nguyen

Take the red pill, come join us down this rabbit hole, and get your head out of the sand to better protect yourself, your company/organization, and the things that matter to you (e.g., your loved ones, your finances, your identity). In this presentation, you will get insights on common misconceptions and trends that led to many breaches, especially those that were headlined. We'll touch on some details from those headlined breaches to show commonalities, address the main misconceptions, describe attackers' approaches, provide some statistics, and most importantly, provide helpful tips applicable to all those who attend.

Anti-Ransomware: How to Turn the Tables

G. Mark Hardy

"OMG! We just got hit with ransomware!" What you don't usually hear next is "LOL!" You can build defenses that prevent ransomware from paralyzing your organization – we'll show you how. Ransomware is a billion dollar industry, and it's growing tremendously. Lost productivity costs far more than the average ransom, so executives just say, "Pay the darn thing." But what if you could stop ransomware in its tracks? We'll demonstrate tools and methodologies that are battle-proven and ACTUALLY WORK as evidenced by fully contained ransomware "explosions" that went nowhere. We'll offer insights into the future of this attack vector and venture predictions on how this industry will evolve and what to expect next.

Malware Analysis: House Rules

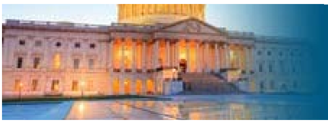
Anuj Soni

Welcome to malware analysis. You're invited to explore, examine, and enjoy. However, we strongly encourage you to review and respect the house rules to make the most of your experience. Whether this is your first time or you're a frequent visitor, we hope this discussion of process and technical suggestions will be a helpful guide to the adventures ahead.

Future Training Events

SANSFIRE	Washington, DC	July 22-29
San Antonio	San Antonio, TX	Aug 6-11
Boston	Boston, MA	Aug 7-12
New York City	New York, NY	Aug 14-19
Salt Lake City	Salt Lake City, UT	Aug 14-19
Chicago	Chicago, IL	Aug 21-26
Virginia Beach	Virginia Beach, VA	Aug 21 - Sep 1
Tampa – Clearwater	Clearwater, FL	Sep 5-10
San Francisco Fall	San Francisco, CA	Sep 5-10

Network Security	Las Vegas, NV	Sep 10-17
Baltimore Fall	Baltimore, MD	Sep 25-30
Rocky Mountain Fall	Denver, CO	Sep 25-30
Phoenix-Mesa	Mesa, AZ	Oct 9-14
Tysons Corner Fall	McLean, VA	Oct 16-21
San Diego	San Diego, CA	Oct 30 - Nov 4
Seattle	Seattle, WA	Oct 30 - Nov 4
Miami	Miami, FL	Nov 6-11
San Francisco Winter	San Francisco, CA	Nov 27 - Dec 2
Austin Winter	Austin, TX	Dec 4-9



Cyber Defense Initiative	Washington, DC	Dec 12-19

Future Summit Events

ICS & Energy	Houston, TX	July 10-15
Security Awareness	Nashville, TN	July 31 - Aug 9
Data Breach	Chicago, IL	Sep 25 - Oct 2
Secure DevOps	Denver, CO	Oct 10-17
SIEM & Tactical Analytics	Scottsdale, AZ	Nov 28 - Dec 5

Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit **www.sans.org/community** for up-to-date Community course information.

Hotel Information

Sheraton Inner Harbor

300 South Charles Street
Baltimore, MD 21201
Phone: 410-962-8300
www.sans.org/event/baltimore-fall-2017/location

The Sheraton Inner Harbor Hotel surrounds you with the best of Baltimore. It is steps from the magnificent Inner Harbor and Oriole Park at Camden Yards. The hotel has everything you need for a comfortable and relaxing stay.

Special Hotel Rates Available

A special discounted rate of $205.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID. If you are a government attendee, you must call the hotel directly at **410-962-8300** to book your room and mention you are a SANS government attendee. These rates include high-speed Internet in your room and are only available through **August 24, 2017**.

Top 5 reasons to stay at the Sheraton Inner Harbor

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 Sheraton Inner Harbor, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.

4 SANS schedules morning and evening events at the Sheraton Inner Harbor that you won't want to miss!

5 Everything is in one convenient location!

Registration Information

REGISTER ONLINE AT
www.sans.org/baltimore-fall

WE RECOMMEND YOU REGISTER EARLY TO ENSURE YOU GET YOUR FIRST CHOICE OF COURSES.

Select your course and indicate whether you plan to test for GIAC certification. If the course is still open, the secure, online 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.

SANS Simulcast

To register for a SANS Baltimore Fall 2017 Simulcast course, please visit **www.sans.org/event/baltimore-fall-2017/attend-remotely**

Pay Early and Save*

Use code **EarlyBird17** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code by	**8-2-17**	**$400.00**	**8-23-17**	**$200.00**

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

SANS Voucher Program

Expand your training budget!

Extend your fiscal year. The SANS Voucher Program provides flexibility and may earn you bonus funds for training.

www.sans.org/vouchers

Cancellation & Access Policy

If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply. All substitution requests must be submitted by email to **registration@sans.org**. If an attendee must cancel and no substitute is available, a refund can be issued for any received payments by **September 6, 2017**. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.

Open a SANS Account today to enjoy these FREE resources:

WEBCASTS

Ask The Expert Webcasts – SANS experts bring current and timely information on relevant topics in IT Security.

Analyst Webcasts – A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

WhatWorks Webcasts – The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.

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

NEWSLETTERS

NewsBites – Twice-weekly high-level executive summary of the most important news relevant to cybersecurity professionals

OUCH! – The world's leading monthly free security-awareness newsletter designed for the common computer user

@RISK: The Consensus Security Alert – A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data

OTHER FREE RESOURCES

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

www.sans.org/account