SANS

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

SEATTLE 2017

October 30 - November 4

Protect Your Business and Advance Your Career

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

CYBER DEFENSE
ETHICAL HACKING
DETECTION & MONITORING

DIGITAL FORENSICS
MANAGEMENT
SECURE DEVELOPMENT

GIAC CERTIFICATIONS

> "SANS provides very relevant training that addresses the challenges we face daily. I can take what I've learned back to the office and put it to use immediately!"
> -Utchay Okorie, Intercity Transit

SAVE $400

Register and pay by Sept 6th – Use code **EarlyBird17**

www.sans.org/seattle

SANS Seattle 2017

OCT 30 - NOV 4

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 Seattle 2017 lineup of instructors includes:

Chris Christianson
Certified Instructor
@cchristianson

Mick Douglas
Instructor
@BetterSafetyNet

David Hoelzer
Faculty Fellow
@it_audit

David R. Miller
Certified Instructor
@DRM_CyberDude

Hal Pomeranz
Faculty Fellow
@hal_pomeranz

Jason Lam
Certified Instructor
@jasonlam_sec

Jake Williams
Certified Instructor
@MalwareJake

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 9.

KEYNOTE: ***Exploitation 101: Stacks, NX/DEP, ASLR and ROP!***
– David Hoelzer

Infosec State of the Union
– Jake Williams

Using the Attack & Defense Matrix Scorecard
– Mick Douglas

Save $400 when you register and pay by September 6th using code EarlyBird17

Courses at a Glance

	MON 10-30	TUE 10-31	WED 11-1	THU 11-2	FRI 11-3	SAT 11-4
SEC401 **Security Essentials Bootcamp Style**	Page 2					
SEC503 **Intrusion Detection In-Depth**	Page 3 *NEW!*					
SEC504 **Hacker Tools, Techniques, Exploits, and Incident Handling**	Page 4					
FOR508 **Advanced Digital Forensics, Incident Response, and Threat Hunting**	Page 5					
FOR572 **Advanced Network Forensics and Analysis**	Page 6					
MGT414 **SANS Training Program for CISSP® Certification**	Page 7					
DEV522 **Defending Web Applications Security Essentials**	Page 8					

Register today for SANS Seattle 2017!
www.sans.org/seattle

@SANSInstitute
Join the conversation:
#SANSSeattle

Securing **Approval** and **Budget** for Training

Packaging matters

Write a formal request

- All organizations are different, but because training requires a significant investment of both time and money, most successful training requests are made via a written document (short memo and/or a few Powerpoint slides) that justifies the need and benefit. Most managers will respect and value the effort.
- Provide all the necessary information in one place. In addition to your request, provide all the right context by including the summary pages on Why SANS?, the Training Roadmap, the instructor bio, and additional benefits available at our live events or online.

Clearly state the benefits

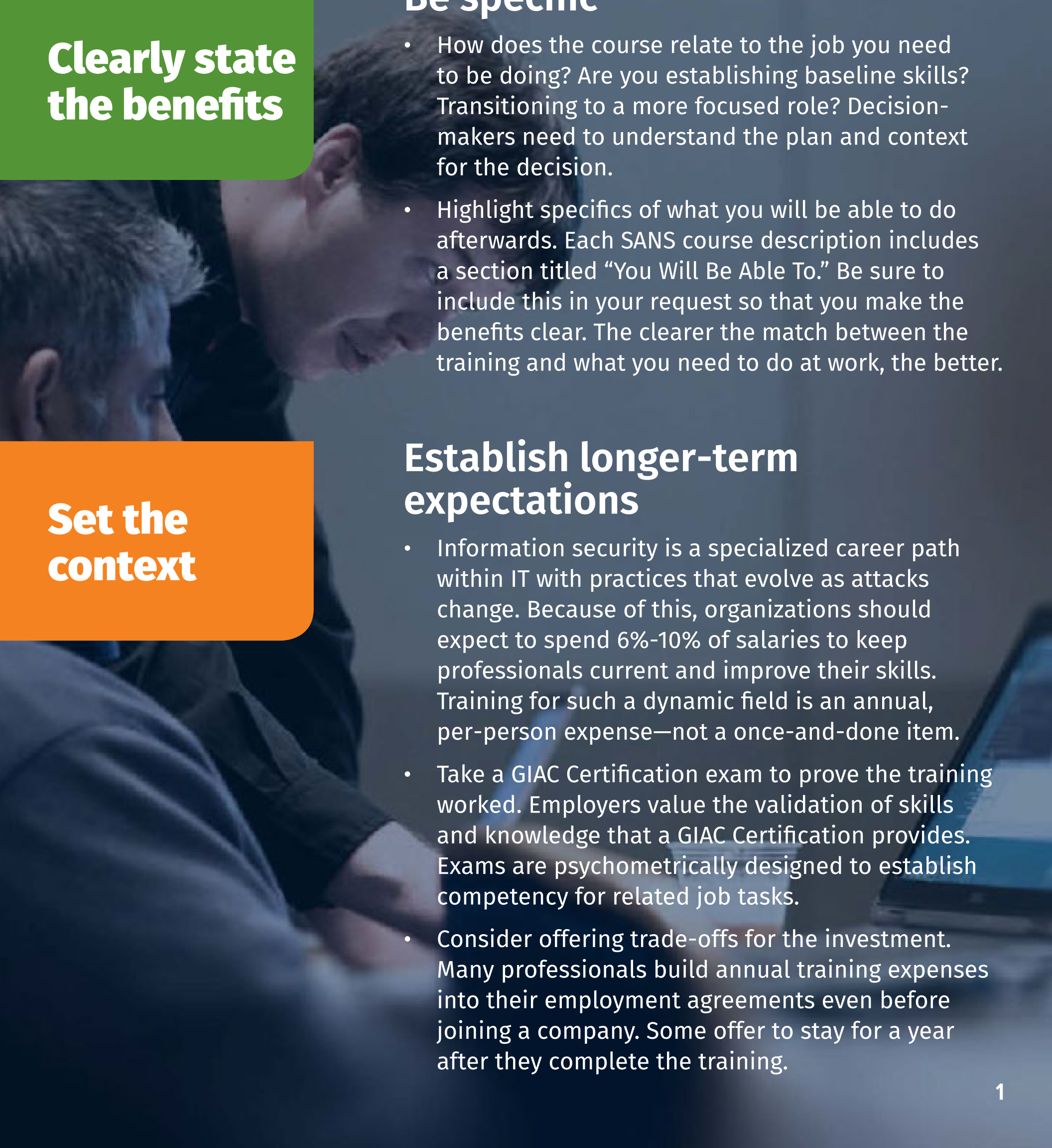
Be specific

- How does the course relate to the job you need to be doing? Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context for the decision.
- Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled "You Will Be Able To." Be sure to include this in your request so that you make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Set the context

Establish longer-term expectations

- Information security is a specialized career path within IT with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense—not a once-and-done item.
- Take a GIAC Certification exam to prove the training worked. Employers value the validation of skills and knowledge that a GIAC Certification provides. Exams are psychometrically designed to establish competency for related job tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expenses into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.



SEC401

GSEC Certification
Security Essentials

www.giac.org/gsec

Security Essentials Bootcamp Style

Six-Day Program
Mon, Oct 30 - Sat, Nov 4
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Chris Christianson

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 been invaluable in refreshing my networking, Windows, and security knowledge."
>
> -Ron Mason, SLT Expressway

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.

SANS Technology Institute
www.sans.edu

www.sans.org/8140

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

Chris Christianson *SANS Certified Instructor*

Chris Christianson is an information security consultant based in Northern California, with 20 years of experience and many technical certifications including the CCSE, CCDP, CCNP, GSEC, CISSP, IAM, GCIH, CEH, IEM, GCIA, GREM, GPEN, GWAPT, GISF, and GCED. He holds a bachelor of science degree in management information systems and was the assistant vice president in the information technology department at one of the nation's largest credit unions. Chris has also been an expert speaker at conferences and a contributor to numerous industry articles. **@cchristianson**

SEC503

Intrusion Detection In-Depth *NEW!*

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

Six-Day Program
Mon, Oct 30 - Sat, Nov 4
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: David Hoelzer

Who Should Attend

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

"SEC503 is helping me to understand better how to optimize my IOS to be more effective."

-Joey Barkley, Ingram Content Group

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

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.

David Hoelzer *SANS Faculty Fellow*

David Hoelzer is a high-scoring SANS instructor and author of more than 20 sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past 25 years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at the SANS Technology Institute, serving as a member of the Curriculum Committee, as well as audit curriculum lead. As a SANS instructor, David has trained security professionals from organizations including the NSA, DHHS, Fortune 500 companies, various Department of Defense sites, national laboratories, and many colleges and universities. David is a Research Fellow at the Center for Cybermedia Research as well as the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC). He also is an adjunct research associate for the UNLV Cybermedia Research Lab and a research fellow with the Internet Forensics Lab. David has written and contributed to more than 15 peer-reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open-source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a B.S. in IT, Summa Cum Laude, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University. @it_audit

SEC**504**

GCIH Certification

Incident Handler

GCIH

www.giac.org/gcih

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, Oct 30 - Sat, Nov 4
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: Mick Douglas

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

> "SEC504 not only teaches us how to perform incident response, but also why we do it, and, most importantly, what not to do."
>
> -Brad Milhorn, ll2P

> "Mick was fantastic. The stories from his vast, real-world experience really added value and drove the training home!"
>
> -Mick Leach, Nationwide

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

Mick Douglas *SANS Instructor*

Even when his job title has indicated otherwise, Mick Douglas has been doing information security work for over 10 years. He received a bachelor's degree in communications from 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! By studying with Mick, security professionals of all abilities will gain useful tools and skills that should make their jobs easier. When he's not "geeking out" you'll likely find Mick indulging in one of his numerous hobbies; photography, scuba diving, or hanging around in the great outdoors. **@BetterSafetyNet**

FOR508

Advanced Digital Forensics, Incident Response, and Threat Hunting

GCFA Certification
Forensic Analyst
www.giac.org/gcfa

Six-Day Program
Mon, Oct 30 - Sat, Nov 4
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jake Williams

Who Should Attend

- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Information security professionals
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR500 (formerly FOR408) and SEC504 graduates

> "Many people lack good forensics skills; being able to figure out what happened is sometimes more important than fixing it."
> -Justin, Davis, St. Jude Medical

> "Come prepared to learn a lot!"
> -Todd Black Lee, Golden 1 Credit Union

FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting will help you to:

- **Detect how and when a breach occurred**
- **Identify compromised and affected systems**
- **Determine what attackers took or changed**
- **Contain and remediate incidents**
- **Develop key sources of threat intelligence**
- **Hunt down additional breaches using knowledge of the adversary**

DAY 0: A 3-letter government agency contacts you to say an advanced threat group is targeting organizations like yours, and that your organization is likely a target. They won't tell how they know, but they suspect that there are already several breached systems within your enterprise. An advanced persistent threat, aka an APT, is likely involved. This is the most sophisticated threat that you are likely to face in your efforts to defend your systems and data, and these adversaries may have been actively rummaging through your network undetected for months or even years.

This is a hypothetical situation, but the chances are very high that hidden threats already exist inside your organization's networks. Organizations can't afford to believe that their security measures are perfect and impenetrable, no matter how thorough their security precautions might be. Prevention systems alone are insufficient to counter focused human adversaries who know how to get around most security and monitoring tools.

This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and hactivism. Constantly updated, FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting addresses today's incidents by providing hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to detect, counter, and respond to real-world breach cases.

GATHER YOUR INCIDENT RESPONSE TEAM – IT'S TIME TO GO HUNTING!

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

Jake Williams *SANS Certified Instructor*

Jake Williams is a principal consultant at Rendition Infosec. He has more than a decade of experience in secure network design, penetration testing, incident response, forensics, and malware reverse engineering. Before founding Rendition Infosec, Jake worked with various cleared government agencies in information security roles. He is well versed in cloud forensics and previously developed a cloud forensics course for a U.S. government client. Jake regularly responds to cyber intrusions by state-sponsored actors in the financial, defense, aerospace, and healthcare sectors using cutting-edge forensics and incident response techniques. He often develops custom tools to deal with specific incidents and malware-reversing challenges. Additionally, Jake performs exploit development and has privately disclosed a multitude of zero day exploits to vendors and clients. He found vulnerabilities in one of the state counterparts to healthcare.gov and recently exploited antivirus software to perform privilege escalation. Jake developed Dropsmack, a pentesting tool (okay, malware) that performs command and control and data exfiltration over cloud file sharing services. Jake also developed an anti-forensics tool for memory forensics, Attention Deficit Disorder (ADD). This tool demonstrated weaknesses in memory forensics techniques. @MalwareJake

FOR**572**

GNFA Certification
Network Forensic Analyst

www.giac.org/gnfa

Advanced Network Forensics and Analysis

Six-Day Program
Mon, Oct 30 - Sat, Nov 4
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Hal Pomeranz

Who Should Attend

- Incident response team members and forensicators
- Hunt team members
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- Anyone interested in computer network intrusions and investigations
- Security Operations Center personnel and information security practitioners

> "Stellar course! I highly recommend adding this course to the training plan of the new cyber protect teams."
> -Tom L., U.S. Air Force

SANS Technology Institute
www.sans.edu

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

Take your system-based forensic knowledge onto the wire. Incorporate network evidence into your investigations, provide better findings, and get the job done faster.

It is exceedingly rare to work any forensic investigation that doesn't have a network component. Endpoint forensics will always be a critical and foundational skill for this career, but overlooking network communications is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, uncover attackers that have been active for months or longer, or prove useful even in definitively proving a crime actually occurred.

FOR572: Advanced Network Forensics and Analysis was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking – we'll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence as well as how to place new collection platforms while an incident is already under way.

Whether you are a consultant responding to a client's site, a law enforcement professional assisting victims of cybercrime and seeking prosecution of those responsible, an on-staff forensic practitioner, or a member of the growing ranks of "threat hunters," this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS Security curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS Forensics alumni from FOR500 (formerly FOR408) and FOR508 can take their existing knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same caliber of real-world problems without the use of disk or memory images.

Hal Pomeranz *SANS Faculty Fellow*

Hal Pomeranz is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft to employee sabotage, organized cybercrime, and malicious software infrastructures. He has worked with law enforcement agencies in the United States and Europe and with global corporations. Equally at home in the Windows or Mac environment, Hal is recognized as an expert in the analysis of Linux and Unix systems. His research on EXT4 file system forensics provided a basis for the development of open-source forensic support for this file system. His EXT3 file recovery tools are used by investigators worldwide. Hal is a SANS Lethal Forensicator, and is the creator of the SANS Linux/Unix Security track (GCUX). He holds the GCFA and GREM certifications and teaches the related courses in the SANS Forensics curriculum. He is a respected author and speaker at industry gatherings worldwide. Hal is a regular contributor to the SANS Computer Forensics blog and co-author of the Command Line Kung Fu blog. **@hal_pomeranz**

MGT**414**

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

SANS Training Program for CISSP® Certification

Six-Day Program
Mon, Oct 30 - Sat, Nov 4
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

▶❚❚
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**

DEV522

Defending Web Applications Security Essentials

GWEB Certification
Web Application Defender
www.giac.org/gweb

Six-Day Program
Mon, Oct 30 - Sat, Nov 4
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Lam

Who Should Attend

- Application developers
- Application security analysts or managers
- Application architects
- Penetration testers who are interested in learning about defensive strategies
- Security professionals who are interested in learning about web application security
- Auditors who need to understand defensive mechanisms in web applications
- Employees of PCI-compliant organizations who need to be trained to comply with PCI requirements

> "DEV522 is absolutely necessary to all techies who work on web applications. I do not think developers understand the great necessity of web security and why it is so important."
>
> -Mahesh Kandru, Cabela's

This is the course to take if you have to defend web applications!

The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure those data. Traditional network defenses, such as firewalls, fail to secure web applications. DEV522 covers the OWASP Top 10 Risks and will help you better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world applications that have been proven to work. The testing aspect of vulnerabilities will also be covered so that you can ensure your application is tested for the vulnerabilities discussed in class.

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding-level implementation.

DEV522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting web applications. It is particularly well suited to application security analysts, developers, application architects, pen testers, auditors who are interested in recommending proper mitigations for web security issues, and infrastructure security professionals who have an interest in better defending their web applications.

The course will also cover additional issues the authors have found to be important in their day-to-day web application development practices. The topics that will be covered include:

- **Infrastructure security**
- **Server configuration**
- **Authentication mechanisms**
- **Application language configuration**
- **Application coding errors like SQL injection and cross-site scripting**
- **Cross-site request forging**
- **Authentication bypass**
- **Web services and related flaws**
- **Web 2.0 and its use of web services**
- **XPATH and XQUERY languages and injection**
- **Business logic flaws**
- **Protective HTTP headers**

The course will make heavy use of hands-on exercises and conclude with a large defensive exercise that reinforces the lessons learned throughout the week.

SANS Technology Institute
www.sans.edu

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

Jason Lam *SANS Certified Instructor*

Jason is accountable for cyber security at a large global financial company. He has over 15 years of experience in the information security industry progressing from hands-on research work to securing large-scale enterprise environments. His recent SANS Institute courseware development includes Defending Web Application Security Essentials and Web Application Pen Testing Hands-On Immersion. Jason started out as a programmer before moving on to an ISP as a network administrator. Handling security incidents for this ISP sparked his interest in information security. Over the years, Jason has performed and led intrusion detection, penetration testing, defense improvement programs and incident response in large enterprise environments. Recently, Jason specializes in building large-scale security operations teams to handle the full cycle of threat identification, response and remediation, in parallel with his passion for directing enterprise web application security programs. **@AuditClay**

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: Exploitation 101: Stacks, NX/DEP, ASLR and ROP!

David Hoelzer

In this two-hour talk, we will begin with basic stack overflows and then introduce the various protections one at a time...and demonstrate how they can be defeated! The talk will cover stack overflows, bypassing DEP/NX (non-executable stacks), defeating ASLR, and defeating code signing with ROP. While the talk covers technical topics, even those with less of a technical background will walk away with an appreciation of just how easy exploit development actually is!

Infosec State of the Union

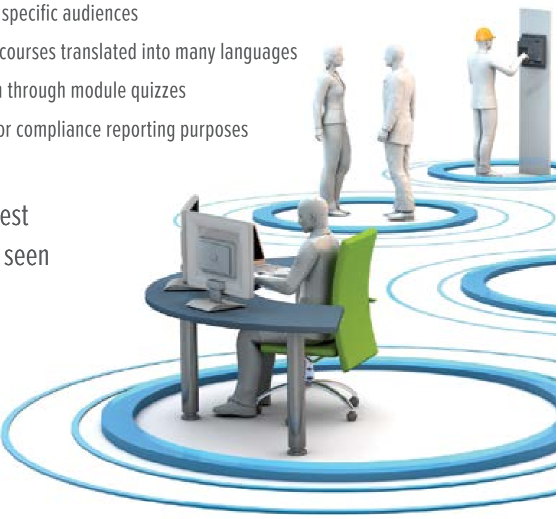
Jake Williams

Come attend this session and catch up with the latest InfoSec news and how it impacts your organization. In this session, we'll talk about Russian election hacking, FBI investigative techniques, implications of the latest Shadow Brokers dumps, software product liability, DoJ protecting government exploits and more. Come hang with us for this session, and you'll walk away bigger, badder, and smarter.

Using the Attack & Defense Matrix Scorecard

Mick Douglas

Have you ever wanted to know how an attack may impact your systems prior to running it? Have you ever wanted to know if your defenses are working as expected? Will the latest 0day go straight though your defense? Will the hot new exploit get you DA on your pen test? Come to this talk and find out! By leveraging the MITRE ATT&CK Framework, we've developed a holistic view of how the layers of your security controls work – or don't. Learn where you should be focusing your efforts. Find out what your biggest weaknesses are! Take your defensive or offensive game to the next level with this completely free and open tool.



SANS

Enhance Your **Training Experience**

Special Pricing

Add an **OnDemand Bundle** & **GIAC Certification Attempt***

to your course within seven days of this event for just **$689** each.

Price goes up to $729 Oct 1st

Extend Your Training Experience with an **OnDemand Bundle**

Four months of supplemental online review

24/7 online access to your course lectures, materials, quizzes, and labs

Subject-matter-expert support to help you increase your retention of course

> "The course content and OnDemand delivery method have both exceeded my expectations."
>
> -Robert Jones, Team Jones, Inc.

GIAC CERTIFICATIONS

Get Certified with **GIAC Certifications**

Distinguish yourself as an information security leader

30+ GIAC cybersecurity certifications available

Two practice exams included

Four months of access to complete the attempt

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

More Information

www.sans.org/ondemand/bundles | www.giac.org

*GIAC and OnDemand Bundles are only available for certain courses.

SANS Training Formats

Whether you choose to attend a training class live or online, the entire SANS team is dedicated to ensuring your training experience exceeds expectations.

Live Classroom Instruction

Premier Training Events

Our most recommended format, live SANS training events feature SANS's top instructors teaching multiple courses at a single time and location. This allows for:

- Focused, immersive learning without the distractions of your office environment
- Direct access to SANS Certified Instructors
- Interacting with and learning from other professionals
- Attending SANS@Night events, NetWars tournaments, vendor presentations, industry receptions, and many other activities

Our premier live training events in North America, serving thousands of students, are held in Orlando, Washington DC, Las Vegas, New Orleans, and San Diego. Regional events with hundreds of students are held in most major metropolitan areas during the year. See page 12 for upcoming training events in North America.

Summits

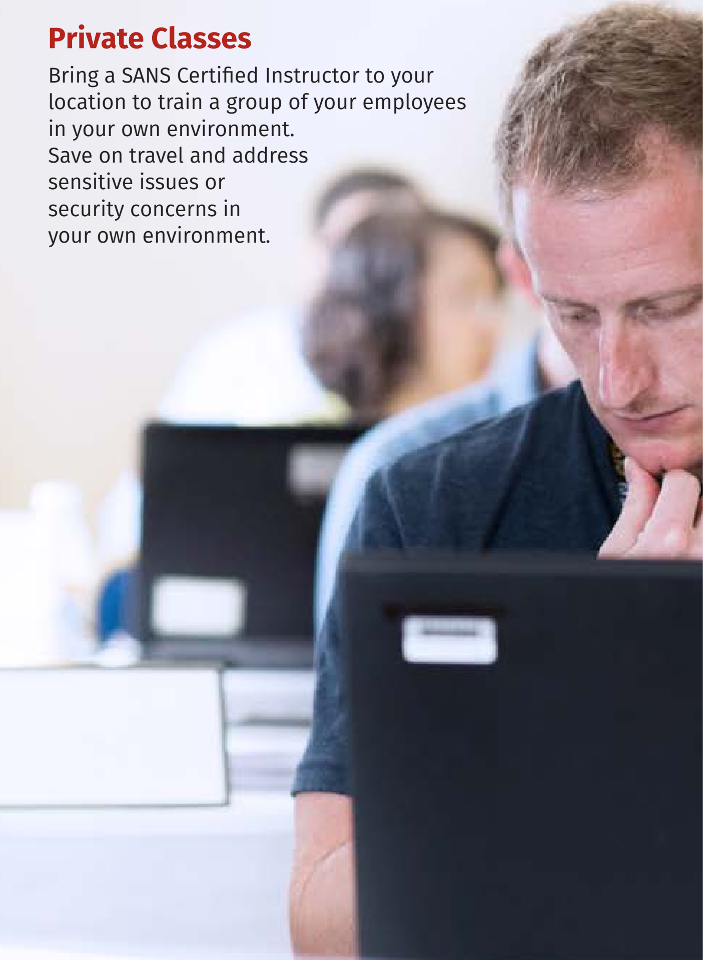
SANS Summits focus one or two days on a single topic of particular interest to the community. Speakers and talks are curated to ensure the greatest applicability to participants.

Community SANS Courses

Same SANS courses, courseware, and labs are taught by up-and-coming instructors in a regional area. Smaller classes allow for more extensive instructor interaction. No need to travel; commute each day to a nearby location.

Private Classes

Bring a SANS Certified Instructor to your location to train a group of your employees in your own environment. Save on travel and address sensitive issues or security concerns in your own environment.



Online Training

SANS Online successfully delivers the same measured learning outcomes to students at a distance that we deliver live in classrooms. More than 30 courses are available for you to take whenever or wherever you want. Thousands of students take our courses online and achieve certifications each year.

Top reasons to take SANS courses online:

- Learn at your own pace, over four months
- Spend extra time on complex topics
- Repeat labs to ensure proficiency with skills
- Save on travel costs
- Study at home or in your office

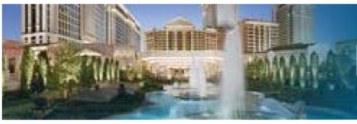
Our SANS OnDemand, vLive, Simulcast, and SelfStudy formats are backed by nearly 100 professionals who ensure we deliver the same quality instruction online (including support) as we do at live training events.

> **"I am thoroughly pleased with the OnDemand modality. From a learning standpoint, I lose nothing. In fact, the advantage of setting my own pace with respect to balancing work, family, and training is significant, not to mention the ability to review anything that I might have missed the first time."**
>
> -Kevin E., U.S. Army

> **"The decision to take five days away from the office is never easy, but so rarely have I come to the end of a course and had no regret whatsoever. This was one of the most useful weeks of my professional life."**
>
> -Dan Trueman, Novae PLC

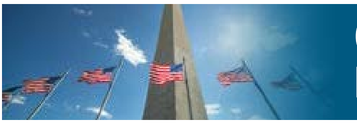
Future Training Events

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 14-21
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

Security East New Orleans, LA Jan 8-13, 2018

Northern Virginia Winter	Reston, VA	Jan 15-20
Las Vegas	Las Vegas, NV	Jan 28 - Feb 2
Miami	Miami, FL	Jan 29 - Feb 3
Scottsdale	Scottsdale, AZ	Feb 5-10
Anaheim	Anaheim, CA	Feb 12-17
Dallas	Dallas, TX	Feb 19-24

Future Summit Events

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
Cyber Threat Intelligence	Washington, DC	Jan 27 - Feb 6, 2018

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

Renaissance Seattle Hotel

515 Madison Street
Seattle, WA 98104
Phone: 206-583-0300
www.sans.org/event/seattle-2017/location

Experience the Renaissance Seattle Hotel, a stylish hotel in Seattle conveniently located just minutes from CenturyLink and Safeco Fields, Pike Place Market and upscale shopping. Staying at the Renaissance Seattle Hotel downtown allows you to eliminate travel stress thanks to easy access to major freeways and Sea-Tac International Airport. Unwind in spacious and newly renovated guest rooms. From colorful paintings by local artists displayed in the lobby to the fully-equipped fitness center and high-speed Internet, the Renaissance Seattle Hotel amenities outshine the rest.

Special Hotel Rates Available

A special discounted rate of $209.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; you will need to call reservations at **206-694-4944** and ask for the SANS government rate. These rates include high speed Internet in your room and are only available through **October 9, 2017**.

Top 5 reasons to stay at the Renaissance Seattle Hotel

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 Renaissance Seattle Hotel, 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 Renaissance Seattle Hotel that you won't want to miss!

5 Everything is in one convenient location!

Registration Information

Register online at **www.sans.org/seattle**

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.

Pay Early and Save*

Use code **EarlyBird17** when registering early

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code by	**9-6-17**	**$400.00**	**9-27-17**	**$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 **October 4, 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