The security field is rapidly evolving and this training allowed me to stay two steps ahead of these changes (and the adversaries). Thank you, SANS!

- John D., USG Corporation
SANS Instructors
Fewer than 100 individuals are currently qualified and designated to teach as SANS Instructors worldwide. This select group of professionals includes recognized industry experts and real-world practitioners, all of whom have proven to be engaging teachers in the classroom. Their up-to-date examples and deep knowledge ensure that what you learn in class will be relevant to your job.
For instructor bios, visit: www.sans.org/instructors
The line-up of SANS Instructors for SANS Northern VA Fall – Tysons 2018 includes:

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

General Session – Welcome to SANS – Keith Palmgren

KEYNOTE: Propelling Your InfoSec Career into the Next Decade – Joshua Wright

The New Internet (and it has nothing to do with IPv6 or PiedPiper) – Dr. Johannes Ullrich

Hunting Highs and Lows – David Mashburn

Courses at a Glance

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC301</td>
<td>Introduction to Cyber Security</td>
<td>SAT 10-13</td>
</tr>
<tr>
<td>SEC455</td>
<td>SIEM Design &amp; Implementation</td>
<td>SUN 10-14</td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td>MON 10-15</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>TUE 10-16</td>
</tr>
<tr>
<td>SEC575</td>
<td>Mobile Device Security and Ethical Hacking</td>
<td>WED 10-17</td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td>THU 10-18</td>
</tr>
<tr>
<td>FOR578</td>
<td>Cyber Threat Intelligence</td>
<td>FRI 10-19</td>
</tr>
<tr>
<td>MGT414</td>
<td>SANS Training Program for CISSP® Certification</td>
<td>SAT 10-20</td>
</tr>
<tr>
<td>MGT433</td>
<td>SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program</td>
<td></td>
</tr>
</tbody>
</table>

Save $400 when you register and pay by August 22nd using code EarlyBird18

Register today for SANS Northern VA Fall – Tysons 2018!
www.sans.org/fall-tysons

@SANSInstitute
Join the conversation: #SANSTysons
Securing Approval and Budget for Training

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.

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.

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.
Extend and Validate Your Training

Add an OnDemand Bundle OR GIAC Certification Attempt
to your course within seven days of this event to get bundle pricing.*

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 material

OnDemand Bundle price – $729

“**The course content and OnDemand delivery method have both exceeded my expectations.”**

- ROBERT JONES, TEAM JONES, INC.

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 bundle price – $729

“**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.
To determine if SANS SEC301: Introduction to Cyber Security is right for you, ask yourself five simple questions:

- Do you have basic computer knowledge, but are new to cybersecurity 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 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 cybersecurity and need formal training and certification?

If you answer yes to any of these questions, then the SEC301: Introduction to Cyber Security training course is for you. Students with a basic knowledge of computers and technology but no prior cybersecurity experience can jump-start their security education with insight and instruction from real-world security experts in SEC301. This completely revised and comprehensive five-day course covers a wide range of baseline topics, including terminology, the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles. The hands-on, step-by-step learning format will enable you to grasp all the information presented even if some of the topics are new to you. You’ll learn fundamentals of cybersecurity that will serve as the foundation of your security 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 SANS course in this progression, 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.

"The course provided me with a lot of great information from the low to the high levels in several areas. A lot of the concepts are something I will be able to use in my day-to-day job."

- Sandy Baguskas, John Hancock
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 and the ability to examine the alerts to give them meaning and context. You will learn to investigate and reconstruct activity to deem if it is noteworthy or a false indication.

This course 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.

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 working for 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.
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.

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 them.

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.

David Mashburn is currently the IT Security Manager for a global non-profit organization in the Washington, D.C. area. He also has experience working as an IT security professional for several civilian federal agencies, and over 15 years of experience in IT. He holds a masters 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.

“SEC504 is foundational and core strength-building in the most critical areas of incident handling. It reinforces and develops understanding around roles and TTPs of both the adversary and defender.”

-Araceli Ari Gomes, Dell Secureworks
Imagine an attack surface spread throughout your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports numerous different wireless technologies all ripe for attack. You don’t need to imagine any further because this already exists today: mobile devices. These devices are the biggest attack surface in most organizations, yet these same organizations often don’t have personnel with the skills needed to assess them.

Mobile devices are no longer a convenience technology; they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores throughout the world. Users rely on mobile devices more today than ever before – we know it, and the bad guys do too.

This course is designed to give you the skills you need to understand the security strengths and weaknesses in Apple iOS, Android, and wearable devices including Apple Watch and Android Wear. With these skills, you will evaluate the security weaknesses of built-in and third-party applications. You’ll learn how to bypass platform encryption, and how to manipulate Android apps to circumvent obfuscation techniques. You’ll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You’ll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS devices, and you’ll exploit lost or stolen devices to harvest sensitive mobile application data.

Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you’ll review ways to effectively communicate threats to key stakeholders. You’ll leverage tools including Mobile App Report Cards to characterize threats for management and decision-makers, while identifying sample code and libraries that developers can use to address risks for in-house applications.

You’ll then use your new skills to apply a mobile device deployment penetration test in a step-by-step fashion. Starting with gaining access to wireless networks to implement man-in-the-middle attacks and finishing with mobile device exploits and data harvesting, you’ll examine each step in conducting such a test with hands-on exercises, detailed instructions, and tips and tricks learned from hundreds of successful penetration tests. By building these skills, you’ll return to work prepared to conduct your own test, and you’ll be better informed about what to look for and how to review an outsourced penetration test.

Mobile device deployments introduce new threats to organizations, including advanced malware, data leakage, and the disclosure of enterprise secrets, intellectual property, and personally identifiable information assets to attackers. Further complicating matters, there simply are not enough people with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you’ll be able to differentiate yourself as being prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test – all critical skills to protect and defend mobile device deployments.
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!

Six-Day Program
Mon, Oct 15 - Sat, Oct 20
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Eric Zimmerman

Who Should Attend
- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Information security professionals
- Federal agents and law enforcement personnel
- Red team members, penetration testers, and exploit developers
- SANS FOR500 and SEC504 graduates

"FOR508 analyzes Advanced Persistent Threat samples that are affecting our industry today. This training can’t get any better!”
- Neel Mehta, Chevron

Eric Zimmerman
SANS Certified Instructor
@EricRZimmerman

As a Special Agent with the FBI, Eric Zimmerman had responsibilities that included managing on-scene triage. He identified several gaps in an existing process and started creating solutions to address them. What began as building and expanding a few live response tools took Eric down a path that eventually led to him writing more than 50 programs that are now used by nearly 8,800 law enforcement officers in over 80 countries. Much of Eric’s work involved designing and building software related to investigations of sexual abuse of children. In a single year, Eric’s programs led to the rescue of hundreds of these children. As a result, in May 2012, Eric was given a National Center for Missing and Exploited Children’s Award, which honors outstanding law enforcement professionals who have performed above and beyond the call of duty. Eric was also presented with the U.S. Attorney Award for Excellence in Law Enforcement in 2013. Today, Eric serves as a Senior Director at Kroll in the company’s cybersecurity and investigations practice. As an instructor, Eric’s focus on understanding the big picture of digital forensics prepares students to perform better analysis, do new research of their own, and identify the best tools or techniques to perform successful investigations – all skills that will have a lifelong impact.
THERE IS NO TEACHER BUT THE ENEMY

During a targeted attack, an organization needs a top-notch and cutting-edge threat hunting or incident response team to counter the threat. This course teaches the tactical, operational, and strategic level of cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, security operations more robust, and organizations more aware of the evolving threat landscape. Students taking the course will learn how to:

▐ Generate threat intelligence to detect, respond to, and defeat advanced persistent threats (APTs)
▐ Validate information received from other organizations to minimize resource expenditures on bad intelligence
▐ Develop and enhance analysis and critical thinking skills
▐ Leverage open-source intelligence to complement a security team of any size
▐ Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX

“This training very well summarizes CTI and connects all of the dots. We got clear answers to what CTI is, how important it is, what it is built upon, and how it can be applied in practice.”
- Nikita Martynov, NNIT A/S

“This course was invaluable in framing my role as a hunter in the intelligence consumption/generation process.”
- Christopher Vega, CitiGroup

In his past work with the military, Peter responded to network attacks and worked with both defensive and offensive red teams. Currently, Peter is a Senior Security Engineer with IBM. Peter believes that people lead technology, not the other way around. He works daily to bring actionable intelligence out of disparate security devices for customers, making systems interoperable. As Peter explains, “Putting together networks only to tear them apart is just plain fun, and allows students to take the information learned from books and this hands-on experience back to their particular work place.”
David R. Miller has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on information systems security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security programs. 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. Projects David has worked on include 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.

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.

After completing the course students will have:

- Detailed coverage of the eight domains of knowledge
- The analytical skills required to pass the CISSP® exam
- The technical skills required to understand each question
- The foundational information needed to become a Certified Information Systems Security Professional (CISSP®)

External Product Notice:

The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)².

“After completing the course students will have:

- Detailed coverage of the eight domains of knowledge
- The analytical skills required to pass the CISSP® exam
- The technical skills required to understand each question
- The foundational information needed to become a Certified Information Systems Security Professional (CISSP®)

External Product Notice:

The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)².

““This training was a comprehensive overview of all topics covered in the CISSP® exam. All in attendance were there for a common goal, including the instructor. It was easy to follow, and the real-world examples given were priceless.””
- Ron Pinnock, Navy Exchange Service Command

““I am new in the domain and this course was the perfect opening – clear explanations, covering all the areas, presenting real-life examples, and great material to support the learning.””
- Sorana Costache, Ubisoft

David R. Miller has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on information systems security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security programs. 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. Projects David has worked on include 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.
Security Information and Event Management (SIEM) can be an extraordinary benefit to an organization’s security posture, but understanding and maintaining it can be difficult. Many solutions require complex infrastructure and software that necessitate professional services for installation. The use of professional services can leave security teams feeling as if they do not truly own or understand how their SIEM operates. Combine this situation of complicated solutions with a shortage of available skills, a lack of simple documentation, and the high costs of software and labor, and it is not surprising that deployments often fail to meet expectations.

A SIEM can be the most powerful tool a cyber defense team can wield, but only when it is used to its fullest potential. This course is designed to address this problem by demystifying SIEM and simplifying the process of implementing a solution that is usable, scalable, and simple to maintain.

The goal of this course is to teach students how to build a SIEM from the ground up using the Elastic Stack. Throughout the course, students will learn about the required stages of log collection. We will cover endpoint agent selection, logging formats, parsing, enrichment, storage, and alerting, and we will combine these components to make a flexible, high-performance SIEM solution. Using this approach empowers SIEM engineers and analysts to understand the complete system, make the best use of technology purchases, and supplement current underperforming deployments. This process allows organizations to save money on professional services, increase the efficiency of internal labor, and develop a nimbler solution than many existing deployments. For example, many organizations pay thousands of dollars in consulting fees when a unique log source needs a custom parser. This course will train students how to easily parse any log source without requiring consulting services, saving their organizations both time and money, and facilitating faster collection and use of new log sources.

Find a full description of this course at www.sans.org/event/northern-va-fall-tysons-2018/courses

---

Organizations have invested a tremendous amount of money and resources into securing technology, but little if anything into securing their workforce. As a result, people, not technology, have become the most common target for cyber attackers. The most effective way to secure the human element is to establish a mature security awareness program that goes beyond just compliance, changes peoples’ behaviors and ultimately creates a secure culture. This intense two-day course will teach you the key concepts and skills needed to do just that, and is designed for those establishing a new program or wanting to improve an existing one. Course content is based on lessons learned from hundreds of security awareness programs from around the world. In addition, you will learn not only from your instructor, but from extensive interaction with your peers. Finally, through a series of labs and exercises, you will develop your own custom security awareness plan that you can implement as soon as you return to your organization.

Register at www.sans.org/fall-tysons | 301-654-SANS (7267)
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.

General Session – Welcome to SANS
Keith Palmgren
Join us for a 30-minute overview to help you get the most out of your SANS training experience. You will receive event information and learn about programs and resources offered by SANS. This brief session will answer many questions and get your training off to a great start. This session will be valuable to all attendees but is highly recommended for first-time attendees.

KEYNOTE:
Propelling Your InfoSec Career into the Next Decade
Joshua Wright
We live in the golden age of information security where mind-boggling breaches to pernicious malware regularly make their way to mainstream media. Never before has the role of the InfoSec pro been more important to top-level executives, creating tremendous opportunities for us to develop our careers for top compensation, exciting opportunities, and leadership promotions. Join SANS Senior Instructor and Counter Hack Director Joshua Wright as he examines some of the many opportunities to propel your InfoSec career into the next decade.

The New Internet (and it has nothing to do with IPv6 or PiedPiper)
Dr. Johannes Ullrich
We all know the Internet and the Web are synonyms, as the only protocol you will ever use is HTTP. Wrong! There is a second protocol that is simple and, unlike HTTP, it works: DNS. But as they say, quiet waters run deep. In this talk, you will learn what is changing about DNS, how DNSSEC, a very effective but much too complex (for the average sysadmin) protocol is being replaced by simpler “DNS Cookies.” And yes, you will learn how to finally run DNS over HTTP to finally render obsolete the last remaining reason for port-based firewalls. We’ll have some fun and excitement with one of the most boring protocols on the Internet. And you will never believe what happens on slide 23!

Hunting Highs and Lows
David Mashburn
Threat hunting has become an essential part of effective security operations. As attackers continue to develop and utilize new techniques, what adjustments must be made by hunt teams? How can defenders sort through the noise and find the indicators of attacker activity? This presentation will explore attacker use of native utilities and examine ways to get more value from your threat hunting activities.
Future Training Events

Boston Summer  Boston, MA  Aug 6-11
San Antonio  San Antonio, TX  Aug 6-11
New York City Summer  New York, NY  Aug 13-18
Northern VA – Alexandria  Alexandria, VA  Aug 13-18
Chicago  Chicago, IL  Aug 20-25
Virginia Beach  Virginia Beach, VA  Aug 20-31
San Francisco Summer  San Francisco, CA  Aug 26-31
Tampa-Clearwater  Tampa, FL  Sep 4-9
Baltimore Fall  Baltimore, MD  Sep 8-15

Future Summit Events

Security Awareness  Charleston, SC  Aug 6-15
Data Breach  New York City, NY  Aug 20-27
Threat Hunting & Incident Response  New Orleans, LA  Sep 6-13
Alaska  Anchorage, AK  Sep 10-15
Oil & Gas Cybersecurity  Houston, TX  Oct 1-6
Secure DevOps  Denver, CO  Oct 22-29
Pen Test HackFest  Bethesda, MD  Nov 12-19
Tactical Detection and Data Analytics  Scottsdale, AZ  Dec 4-11

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.

Network Security  Las Vegas, NV  Sep 23-30

Northern VA Fall – Tysons  McLean, VA  Oct 13-20
Denver  Denver, CO  Oct 15-20
Seattle Fall  Seattle, WA  Oct 15-20
Houston  Houston, TX  Oct 29 - Nov 3
Dallas Fall  Dallas, TX  Nov 5-10
DFIRCON Miami  Miami, FL  Nov 5-10
San Diego Fall  San Diego, CA  Nov 12-17
Austin  Austin, TX  Nov 26 - Dec 1
San Francisco Fall  San Francisco, CA  Nov 26 - Dec 1
Nashville  Nashville, TN  Dec 3-8
Santa Monica  Santa Monica, CA  Dec 3-8

Cyber Defense Initiative  Washington, DC  Dec 11-18
Register online at www.sans.org/fall-tysons

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.

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 26, 2018. 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.

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

Top 3 reasons to stay at the Hilton McLean Tysons Corner

1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Hilton McLean Tysons Corner, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
3. SANS schedules morning and evening events at the Hilton McLean Tysons Corner that you won’t want to miss!

Pay Early and Save*

Use code EarlyBird18 when registering early

<table>
<thead>
<tr>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-22-18</td>
<td>$400.00</td>
<td>9-12-18</td>
<td>$200.00</td>
</tr>
</tbody>
</table>

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

Hilton McLean Tysons Corner
7920 Jones Branch Drive
McLean, VA  22102
703-847-5000
www.sans.org/event/fall-tysons-2018/location

Experience impeccable service at the Hilton McLean Tysons Corner hotel near Washington, DC. This contemporary hotel is located in the center of Tysons Corner’s technology corridor, between Ronald Reagan National Airport and Washington Dulles International Airport. It is also just minutes from world-class shopping at Tysons Corner Center and the Galleria Mall. Take the Silver Line Metro from the McLean Station into downtown Washington, DC. A complimentary shuttle servicing a one-mile radius of the hotel is also provided.

Special Hotel Rates Available

A special discounted rate of $209.00 S/D will be honored based on space availability. Additional deluxe rooms and suites are available at discounted rates.

The group rate is lower than the current government per diem rate. Should the rate fall below the group rate, 20% of the guestroom block will be made available at the prevailing government per diem rate. These rates include high-speed Internet in your room and are only available through September 21, 2018.

Register online at www.sans.org/fall-tysons

Experience impeccable service at the Hilton McLean Tysons Corner hotel near Washington, DC. This contemporary hotel is located in the center of Tysons Corner’s technology corridor, between Ronald Reagan National Airport and Washington Dulles International Airport. It is also just minutes from world-class shopping at Tysons Corner Center and the Galleria Mall. Take the Silver Line Metro from the McLean Station into downtown Washington, DC. A complimentary shuttle servicing a one-mile radius of the hotel is also provided.

Special Hotel Rates Available

A special discounted rate of $209.00 S/D will be honored based on space availability. Additional deluxe rooms and suites are available at discounted rates.

The group rate is lower than the current government per diem rate. Should the rate fall below the group rate, 20% of the guestroom block will be made available at the prevailing government per diem rate. These rates include high-speed Internet in your room and are only available through September 21, 2018.

Register online at www.sans.org/fall-tysons

Experience impeccable service at the Hilton McLean Tysons Corner hotel near Washington, DC. This contemporary hotel is located in the center of Tysons Corner’s technology corridor, between Ronald Reagan National Airport and Washington Dulles International Airport. It is also just minutes from world-class shopping at Tysons Corner Center and the Galleria Mall. Take the Silver Line Metro from the McLean Station into downtown Washington, DC. A complimentary shuttle servicing a one-mile radius of the hotel is also provided.

Special Hotel Rates Available

A special discounted rate of $209.00 S/D will be honored based on space availability. Additional deluxe rooms and suites are available at discounted rates.

The group rate is lower than the current government per diem rate. Should the rate fall below the group rate, 20% of the guestroom block will be made available at the prevailing government per diem rate. These rates include high-speed Internet in your room and are only available through September 21, 2018.
Newsletters

**NewsBites**
Twice-weekly, high-level executive summaries 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.

Webcasts

**Ask the Experts 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 how a vendor’s commercial tool can be used to solve or mitigate that problem.

Other Free Resources (No SANS account is necessary)

- 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)

Save $400 when you pay for any 4-, 5-, or 6-day course and enter the code “EarlyBird18” by August 22nd. Register today at www.sans.org/fall-tysons