SANS San Francisco 2016

November 27 - December 2

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

PROTECT YOUR COMPANY AND ADVANCE YOUR CAREER
WITH HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Nine courses on

CYBER DEFENSE

ETHICAL HACKING

DIGITAL FORENSICS

SECURITY MANAGEMENT

"SANS courses are real-world practical info – not just textbook!"

-Reza Salari,
DRS Technologies

SAVE $400

when you register and pay by Oct 5th using code **EarlyBird2016**

GIAC

GIAC-Approved Training

www.sans.org/san-francisco

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 San Francisco 2016 lineup of instructors includes:

Chris Christianson
SANS Instructor
@cchristianson

Sarah Edwards
Certified Instructor
@iamevltwin

G. Mark Hardy
Certified Instructor
@g_mark

Micah Hoffman
Certified Instructor
@WebBreacher

Ryan Johnson
SANS Instructor
@ForensicRJ

Michael Murr
Principal Instructor
@mikemurr

Stephen Sims
Senior Instructor
@Steph3nSims

James Tarala
Senior Instructor
@isaudit

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 10.

KEYNOTE: ***Simplifying Risk Management: A Practical Approach to Security Intelligence*** James Tarala

iOS Location Forensics – Sarah Edwards

How to Commit Card Fraud – G. Mark Hardy

Running Away from Security: Web App Vulnerabilities and OSINT Collide – Micah Hoffman

Save $400 when you register and pay by Oct 5th using code EarlyBird2016

Courses-at-a-Glance

		SUN 11-27	MON 11-28	TUE 11-29	WED 11-30	THU 12-1	FRI 12-2
SEC401	Security Essentials Bootcamp Style	Page 1					
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	Page 2					
SEC542	Web App Penetration Testing and Ethical Hacking	Page 3					
SEC566	Implementing and Auditing the Critical Security Controls – In-Depth		Page 4				
SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	Page 5					
FOR518	Mac Forensic Analysis	Page 6					
FOR572	Advanced Network Forensics and Analysis	Page 7					
FOR578	Cyber Threat Intelligence		Page 8 NEW!				
MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™		Page 9				

SEC401:

Security Essentials Bootcamp Style

SANS

Six-Day Program
Sun, Nov 27 - Fri, Dec 2
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Chris Christianson

www.giac.org/gsec

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"This course establishes an excellent foundation on the first day, and builds very well over the next few days."
-Chris Crudele, BDP International

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

Learn to build a security roadmap that can scale today and into the future.

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. This course will show you how to prevent your organization's security problems from being headline news in the *Wall Street Journal*!

"SEC401 training is foundational to information security." -Mark Francis, BB&T

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 analysts, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

With the rise of 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'll 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.

PREVENTION IS IDEAL BUT DETECTION IS A MUST.

Chris Christianson *SANS Instructor*

Chris Christianson is an information security consultant based in Northern California, who has twenty years of experience and many technical certifications including the CCSE, CCDP, CCNP, GSEC, CISSP, IAM, GCIH, CEH, IEM, GCIA, GREM, GPEN, GWAPT, and GISF. He holds a bachelor of science degree in management information systems and he has served as 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 industry articles. @cchristianson

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Sun, Nov 27 - Fri, Dec 2
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Michael Murr

www.giac.org/gcih

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"This was a really good course, of which I learned a lot that will be totally useful on my job."
-Edgar Jimenez, Palo Alto Networks

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or 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.***

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

"I love Mike Murr's analogies they are spot on and help break down complex information. The intensity of the course is matched by the knowledge and enthusiasm of the instructor." -Elizabeth Murrell, Boston Medical Center

This course enables you to turn the tables on computer attackers by helping you to 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 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 for, exploiting, and defending systems. This 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.***

"Learning about what is valuable, what to focus on, and how I can improve in my work place was awesome!"
-Mike Waxman, Mosaic451

Michael Murr *SANS Principal Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years. He has conducted numerous investigations and computer forensic examinations, and performed specialized research and development. Michael has taught SANS SEC504 (Hacker Techniques, Exploits, and Incident Handling), SANS FOR508 (Computer Forensics, Investigation, and Response), and SANS FOR610 (Reverse-Engineering Malware). He has also led SANS Online Training courses, and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. He holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about digital forensics on his forensic computing blog (www.forensicblog.org). @mikemurr

SEC542:
Web App Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Sun, Nov 27 - Fri, Dec 2
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Micah Hoffman

www.giac.org/gwapt

www.sans.edu

www.sans.org/cyber-guardian

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"(Day 6) Capture the Flag was an amazing eye opener to the real world of web pen testing."
-Derick Ansignia, Scarfold Consult

Web applications play a vital role in every modern organization. But if your organization does not properly **test** and **secure** its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

Who Should Attend

- General security practitioners
- Penetration testers
- Ethical hackers
- Web application developers
- Website designers and architects

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. **Unfortunately, there is no "patch Tuesday" for custom web applications, so major industry studies find that web application flaws play a major role in significant breaches and intrusions.** Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

"This course has been well worth it!
I can't wait to take the advanced pen testing course." -Ben Johnson, Time Inc.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

Students will come to understand major web application flaws and their exploitation and, most importantly, learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations. Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. The course will help you demonstrate the true impact of web application flaws through exploitation.

In addition to more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. **This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way to hammer home lessons learned.**

Micah Hoffman *SANS Certified Instructor*

Micah Hoffman has been working in the information technology field since 1998 supporting federal government and commercial customers in their efforts to discover and quantify information security weaknesses within their organizations. He leverages years of hands-on, real-world penetration testing and incident response experience to provide excellent solutions to his customers. Micah holds the GMON, GAWN, GWAPT, and GPEN certifications as well as the CISSP. Micah is an active member in the NoVAHackers community, writes Recon-ng modules and enjoys tackling issues with the Python scripting language. When not working, teaching, or learning, Micah can be found hiking or backpacking on the Appalachian Trail or the many park trails in Maryland. @WebBreacher

SEC566:

Implementing and Auditing the Critical Security Controls – In-Depth

SANS

Five-Day Program
Mon, Nov 28 - Fri, Dec 2
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: James Tarala

www.giac.org/gccc

SANS Technology Institute
www.sans.edu

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Staff and clients of federal agencies
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks, (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle. The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

"This is a must-do course if you are looking to steer your company through some hefty controls to security."-Jeff Evenson, AgStar Financial Services

SANS' in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

The course shows security professionals how to implement the Controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

James Tarala *SANS Senior Instructor*

James Tarala is a principal consultant with Enclave Security and is based in Venice, Florida. He is a regular speaker with the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years developing large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them in their security management, operational practices, and regulatory compliance issues, and he often performs independent security audits and assists internal audit groups in developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications. @isaudit

SEC660:

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SANS

Six-Day Program
Sun, Nov 27 - Fri, Dec 2
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Stephen Sims

www.giac.org/gxpn

www.sans.edu

www.sans.org/cyber-guardian

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

"SEC660 is a great course, although very challenging and I feel completely out of my depth, and I loved it."
-Daniel Stewart, Dell SecureWorks

This course is designed as a logical progression point for those who have completed **SEC560: Network Penetration Testing and Ethical Hacking**, or for those with existing penetration testing experience.

Who Should Attend

- Network and systems penetration testers
- Incident handlers
- Application developers
- IDS engineers

Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. **Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises.** A sample of topics covered includes weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, return-oriented programming (ROP), Windows exploit-writing, and much more!

"I learned a lot from taking this course, and it has motivated me to learn more about exploit writing." -Daniel Alvarez, UBS AG

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, you need a strong desire to learn, the support of others, and the opportunity to practice and build experience. **SEC660 provides attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios.** This course goes far beyond simple scanning for low-hanging fruit, and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

"This course, while tough, I enjoyed and I would recommend it."
-Pietro Stroia, Accenture

Stephen Sims *SANS Senior Instructor*

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant performing reverse engineering, exploit development, threat modeling, and penetration testing. Stephen has an master's of science degree in information assurance from Norwich University. He is the author of SANS' only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author of SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP, CISA, Immunity NOP, and many other certifications. In his spare time, Stephen enjoys snowboarding and writing music. @Steph3nSims

FOR518:
Mac Forensic Analysis

SANS

Six-Day Program
Sun, Nov 27 - Fri, Dec 2
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Sarah Edwards

BUNDLE ONDEMAND
WITH THIS COURSE
sans.org/ondemand

"The information in this course is very helpful, and it has some great resources and reference material."
-Jheran Denis, Verizon Wireless

"Very comprehensive in-depth coverage of the course topic. Excellent reference materials as a take-away."
-Jennifer B., Indiana State Police

Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are familiar with Windows-only machines.

Times and trends change and forensic investigators and analysts need to change with them. The new **FOR518: Mac Forensic Analysis** course provides the tools and techniques necessary to take on any Mac case without hesitation. The intense hands-on forensic analysis skills taught in the course will enable Windows-based investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyze any Mac or iOS system.

FORENSICATE DIFFERENTLY!

Who Should Attend

- Experienced digital forensic analysts who want to solidify and expand their understanding of file system forensics and advanced Mac analysis
- Law enforcement officers, federal agents, or detectives who want to master advanced computer forensics and expand their investigative skill set
- Media exploitation analysts who need to know where to find the critical data they need from a Mac system
- Incident response team members who are responding to complex security incidents/intrusions from sophisticated adversaries and need to know what to do when examining a compromised system
- Information security professionals who want to become knowledgeable with Mac OS X and iOS system internals
- SANS FOR408, FOR508, FOR526, FOR610, FOR585 alumni looking to round out their forensic skills

FOR518 will teach you:

- **Mac Fundamentals:** How to analyze and parse the Hierarchical File System (HFS+) by hand and recognize the specific domains of the logical file system and Mac-specific file types.
- **User Activity:** How to understand and profile users through their data files and preference configurations.
- **Advanced Analysis and Correlation:** How to determine how a system has been used or compromised by using the system and user data files in correlation with system log files.
- **Mac Technologies:** How to understand and analyze many Mac-specific technologies, including Time Machine, Spotlight, iCloud, Versions, FileVault, AirDrop, and FaceTime.

FOR518: Mac Forensic Analysis aims to form a well-rounded investigator by introducing Mac forensics into a Windows-based forensics world. This course focuses on topics such as the HFS+ file system, Mac-specific data files, tracking user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac exclusive technologies. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac forensics case.

Sarah Edwards *SANS Certified Instructor*
A self-described Mac nerd, Sarah Edwards is a forensic analyst, author, speaker, and both author and instructor of SANS FOR518: Mac Forensic Analysis. She has worked specifically in Mac forensics since 2004, carving out a niche for herself when this area of forensics was still new. Sarah has worked with federal law enforcement agencies on a variety of high-profile investigations in such areas as computer intrusions, criminal cases, counter-intelligence, counter-narcotics, and counter-terrorism. She has a bachelor's degree in information technology from the Rochester Institute of Technology and a master's in information assurance from Capitol College. @iamevltwin

FOR572:
Advanced Network Forensics and Analysis

SANS

Six-Day Program
Sun, Nov 27 - Fri, Dec 2
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Ryan Johnson

www.giac.org/gnfa

www.sans.edu

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

digital-forensics.sans.org

"This course is very realistic in comparison to what I see in my normal day. Having to slice and aggregate log flows and pcap alone lends to the realism."
-Everett Sherlock, Kapstone Paper and Packaging

The network IS the new investigative baseline.

There is simply no incident response action that doesn't include a communications component any more – whether you conduct threat hunting operations, traditional casework, or post-mortem incident response, understanding the nature of how systems have communicated is critical to success. Even in disk- and memory-based incident response work, artifacts that clarify a subject's network actions can be keystone findings you can't afford to miss. Whether you are handling a data breaches, intrusion scenario, employee misuse, or threat hunting (proactively trawling your organization's data stores for evidence of an undiscovered compromise), the need to effectively examine and interpret network artifacts is here to stay.

Who Should Attend

- Incident response team members and forensicators
- 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

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 and analytic approach needed to incorporate a network perspective into proactive hunting or traditional casework. Even the most skilled attacker can't fully escape leaving some evidence of communications on the network - so you'll learn the skills to identify reconnaissance, exploitation, operational, command-and-control, and data exfiltration phases of an incident. If you're chasing leads on an existing case or seeking evidence of a compromise you haven't yet discovered, the network is the key to success. 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 needs, a law enforcement professional assisting victims of cyber crime and seeking prosecution of those responsible, or an on-staff forensic practitioner, 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 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 any convenient hard drive or memory images.

Ryan Johnson *SANS Instructor*

Ryan Johnson is the head of CSIRT Readiness and Investigations at PricewaterhouseCoopers. In this role, Ryan is responsible for global CSIRT readiness, insider threat, and strategic threat intelligence. Previously, Ryan was a senior director and lead incident responder in the Cyber Division of consulting firm Alvarez & Marsal. Ryan has been investigating crimes in the digital realm for more than 12 years including performing media exploitation for the U.S. Army in Iraq. Ryan has run multiple large-scale breach investigations and has also provided clients with proactive assessments that assisted them in identifying both security gaps, and identifying systems which are already compromised. Ryan taught digital forensics for the US State Department's Anti-Terrorism Assistance program and was a co-author of several of their digital forensics courses. Ryan also co-authored *Mastering Windows Network Forensics and Investigations*, Second Edition. Ryan's industry credentials include: GNFA, GMON, GCIH), CISSP, CFCE, DFCP, EnCE, and PCIP. He has earned an M.S. from Dalhousie University and two bachelor's degrees from Queen's University. @ForensicRJ

FOR578:
Cyber Threat Intelligence

NEW

SANS

Five-Day Program
Mon, Nov 28 - Fri, Dec 2
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Jake Williams

Make no mistake: current network defense, threat hunting, and incident response practices contain a strong element of intelligence and counterintelligence that cyber analysts must understand and leverage in order to defend their networks, proprietary data, and organizations.

FOR578: Cyber Threat Intelligence will help network defenders, threat hunting teams, and incident responders to:

- Understand and develop skills in tactical, operational, and strategic level threat intelligence
- 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
- 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.

Who Should Attend

- Incident response team members
- Threat hunters
- Security Operations Center personnel and information security practitioners
- Experienced digital forensic analysts
- Federal agents and law enforcement officials
- SANS FOR408, FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

"Jake's use of real-life scenarios is very useful, it keeps everything relevant and interesting."
-Hayley Roberts, MOD

The collection, classification, and exploitation of knowledge about adversaries - collectively known as cyber threat intelligence - gives network defenders information superiority that is used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture.

Cyber threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats. Malware is an adversary's tool but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders.

During a targeted attack, an organization needs a top-notch and cutting-edge threat hunting or incident response team armed with the threat intelligence necessary to understand how adversaries operate and to counter the threat. FOR578: Cyber Threat Intelligence will train you and your team in the tactical, operational, and strategic level cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, and organizations more aware of the evolving threat landscape.

THERE IS NO TEACHER BUT THE ENEMY!

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 performed by state-sponsored actors in 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, that demonstrated weaknesses in memory forensics techniques. @MalwareJake

MGT512:

SANS Security Leadership Essentials for Managers with Knowledge Compression™

SANS

Five-Day Program
Mon, Nov 28 - Fri, Dec 2
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop NOT Needed
Instructor: G. Mark Hardy

www.giac.org/gslc

www.sans.edu

www.sans.org/8140

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

"Mark is a wealth of knowledge and experience which adds value to the class. His injection of real-world scenarios as he is teaching is very helpful."
-Pam L., National Nuclear Security Administration

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. In addition, the course has been engineered to incorporate the NIST Special Publication 800 series guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

Who Should Attend

- All newly appointed information security officers
- Technically-skilled administrators who have recently been given leadership responsibilities
- Seasoned managers who want to understand what their technical people are telling them

Essential security topics covered in this management track include network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, web application security, and offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression™, special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA's CAQC Program for Security+ 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

Knowledge Compression™

Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class that aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. He serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 sailors. He also served as wartime Director, Joint Operations Center for U.S. Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for InfoSec, public key infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he has bachelor's degrees in computer science and mathematics, and master's degrees in business administration and strategic studies, along with the GSLC, CISSP, CISM, and CISA certifications. @g_mark

SANS@NIGHT EVENING TALKS

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: Simplifying Risk Management: A Practical Approach to Security Intelligence

James Tarala

Simply put, people make risk management too difficult. Yes, there are competing security control frameworks and more threats discovered every day, but that does not mean that it must be difficult to defend an enterprise. Blueprints are freely available to organizations that want to catalog threats, define security controls, and then present security capabilities to executive leadership. In this presentation, James Tarala will demonstrate the risk management models that are freely available to organizations and explain practical tips for implementing a thorough security architecture. He will also show how these models can be used to automate security intelligence to show executive leadership precisely what risk their organization is accepting. No matter what phase of maturity an organization is at in their efforts, they will leave this presentation with a specific framework and action items to put security intelligence in the hands of business leaders who can act on the threat.

iOS Location Forensics

Sarah Edwards

It is no secret iOS devices can track users every move providing location data that can be a major factor in many types of investigations. This valuable information can be found in a variety of areas on the iOS device. In this presentation, we will walk you through native iOS databases, plist files, and 3rd-party applications where this information is kept and tracked. We will also introduce you to scripts created to make data analysis easier by allowing you to do fast data correlation and build historical map of locations.

How to Commit Card Fraud

G. Mark Hardy

Well, we're not going to show you how to commit fraud, but will show you how the bad guys do it and how you can protect yourself and your business. We'll take a look into the "dark web" and see how these big card heists are pulled off, why chip-and-pin won't solve the fraud problem, and why payment technologies like Apple Pay pose new risks. You'll learn the ecosystem of fraud, and how it's become a big business that costs banks and merchants over $16 billion annually. See if your bank even bothers to use the security protections it could – we'll have a mag stripe card reader so you can really see what's in your wallet.

Running Away from Security: Web App Vulnerabilities and OSINT Collide

Micah Hoffman

Lately it seems like more and more of our lives are being sucked into the computer world. There are wrist-sensors for tracking our steps, phone apps that plot our workouts on maps, and sites to share our healthy-eating and weight loss progress. When people sign up for these sites, they usually use pseudonyms or the sites give them a unique numbered ID to keep their information "private." How hard would it be to connect a person's step-counting, diet history, and other info on these health sites to their real lives? Are businesses using these sites for non-fitness purposes? This talk will show weaknesses in several web applications used for health and exercise tracking and reveal [spoiler alert] how trivial it is to find the real people behind the "private" accounts.

Enhance Your Training Experience

Add an

OnDemand Bundle & GIAC Certification Attempt*

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

SPECIAL 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

"The course content and OnDemand delivery method have both exceeded my expectations."

-Robert Jones, Team Jones, Inc.

Get Certified with GIAC Certification

- Distinguish yourself as an information security leader
- 30+ GIAC certifications to choose from
- 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

LIVE CLASSROOM TRAINING

Multi-Course Training Events www.sans.org/security-training/by-location/all
Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers

Community SANS www.sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

Private Training www.sans.org/private-training
Live Onsite Training at Your Office Location. Both In-person and Online Options Available

Mentor www.sans.org/mentor
Live Multi-Week Training with a Mentor

Summit www.sans.org/summit
Live IT Security Summits and Training

ONLINE TRAINING

OnDemand www.sans.org/ondemand
E-learning Available Anytime, Anywhere, at Your Own Pace

vLive www.sans.org/vlive
Online Evening Courses with SANS' Top Instructors

Simulcast www.sans.org/simulcast
Attend a SANS Training Event without Leaving Home

OnDemand Bundles www.sans.org/ondemand/bundles
Extend Your Training with an OnDemand Bundle Including Four Months of E-learning

FUTURE SANS TRAINING EVENTS

Network Security 2016
Las Vegas, NV | Sep 10-19

Security Leadership SUMMIT & TRAINING 2016
Dallas, TX | Sep 27 - Oct 4

Seattle 2016
Seattle, WA | Oct 3-8

Baltimore 2016
Baltimore, MD | Oct 10-15

Tysons Corner 2016
Tysons Corner, VA | Oct 22-29

San Diego 2016
San Diego, CA | Oct 23-28

Pen Test HackFest SUMMIT & TRAINING 2016
Crystal City, VA | Nov 2-9

Miami 2016
Miami, FL | Nov 7-12

Health Care Cybersecurity SUMMIT & TRAINING 2016
Houston, TX | Nov 14-21

Cyber Defense Initiative 2016
Washington, DC | Dec 10-17

Security East 2017
New Orleans, LA | Jan 9-14

Las Vegas 2017
Las Vegas, NV | Jan 23-28

Cyber Threat Intelligence SUMMIT & TRAINING 2017
Arlington, VA | Jan 25 - Feb 1

SOUTHERN CALIFORNIA **Anaheim** 2017
Anaheim, CA | Feb 6-11

Information on all events can be found at
www.sans.org/security-training/by-location/all

SANS SAN FRANCISCO 2016

Hotel Information

Training Campus

Hilton San Francisco Union Square

333 O'Farrell Street
San Francisco, CA 94102
www.sans.org/event/san-francisco-2016/location

Hilton San Francisco Union Square boasts an ideal location in the heart of downtown San Francisco, with easy access to Nob Hill, Chinatown and fantastic shopping, dining and entertainment in and around Union Square. Enjoy proximity to attractions such as the Golden Gate Bridge, Fisherman's Wharf and the Marina, and easy access to public transportation such as MUNI, BART and the famous cable cars at this central San Francisco hotel.

Special Hotel Rates Available

A special discounted rate of $229.00 S/D will be honored based on space availability.
Should the prevailing Government per diem rate fall below the SANS group rate, Government per diem rooms will be made available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high speed Internet in your room and are only available through November 4, 2016.

Top 5 reasons to stay at the Hilton San Francisco Union Square

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 Hilton San Francisco Union Square 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 Hilton San Francisco Union Square that you won't want to miss!
5. Everything is in one convenient location!

SANS SAN FRANCISCO 2016

Registration Information

We recommend you register early to ensure you get your first choice of courses.

Register online at www.sans.org/san-francisco

Select your course or courses and indicate whether you plan to test for GIAC certification.

If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Use code **EarlyBird16** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**10-5-16**	**$400.00**	**11-2-16**	**$200.00**

Some restrictions 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

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by November 9, 2016 – processing fees may apply.