# AppSec 2013

AUSTIN, TX

SANS

SECURING SANS 00100111 THE APP

## Program Guide

# Agenda

*All Summit evening sessions will be held in Lone Star on the 2nd floor (unless noted).*

*All approved presentations from the Summit evening sessions will be available online following the Summit at **https://files.sans.org/summits/appsec13**. An e-mail will be sent out within 5 business days once the presentations are posted.*

## Monday, April 22

8:00 am

**Class & Summit Registration**
Location: Lone Star Foyer

9:00 am – 5:00 pm all classes

**Training Courses** (location in parenthesis)

SEC542: Web App Penetration Testing and Ethical Hacking - (Austin North – 2nd Floor)

DEV522: Defending Web Applications Security Essentials - (Austin South – 2nd Floor)

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications - (Cellar – 1st Floor)

DEV544: Secure Coding in .NET: Developing Defensible Applications - (Bouquets – 1st Floor)

12:15 - 1:30 pm

**Lunch & Learn**
Location: Lone Star – 2nd Floor
*Sponsored by*

WhiteHat SECURITY

*Presented by Robert "RSnake" Hansen (CISSP)*

5:00 - 6:00 pm

**Summit Registration and Networking**
Location: Lone Star - 2nd Floor
Beverages and light snacks provided

6:00-6:30 pm

**Keynote: *Securing the App***

Critical software systems, designed to enable business, are at the root of many headlines about data breaches and corporate hacks. The most common attacks are often caused by simple mistakes that occur during development and deployment. This short talk identifies the top things you can do to arm your development team with the knowledge they need to develop secure applications.

*Speaker: Frank Kim, Certified Instructor, SANS Institute*

6:30 - 7:15 pm

### *Mobile App Security 2013: Phenomenal Cosmic Power, Itty Bitty Living Space*

Mobile is living up to the hype as the next great technology radiation, rivaling the Internet in its game-changing impact. Of course, with great change comes potential risk - is there a magic bullet to secure the inevitable adoption of mobile everywhere? Cigital presents the latest mobile app security trends and data from the field across our mobile app security consulting practice.

*Speaker: Joel Scambray, CISSP, Managing Principal, Cigital*

---

7:15 - 8:00 pm

### *AppSec 2.0: Strategies for Moving the Needle on Application Security*

Thousands of applications, millions of lines of code, numerous development teams spread across the planet. You thought your application security program had it bad! The participants in this panel discussion have been tackling the issue of software security in their large corporate environments for years, helping thousands of software developers improve how they build software and helping to identify software vulnerabilities before attackers do. They will discuss how they have built large-scale vulnerability scanning programs, how they interact with their respective business units, and how they get executive buy-in to further the case of application security. Come join this interactive session with application security industry leaders who will discuss practical approaches to securing software.

*Moderator: John Dickson, CISSP, Principal, Denim Group*

*Panelists: Jim Apple, Senior Manager, Applications, Bank of America*
*Chris Haggard, Manager of eCommerce/Application Security, FedEx*
*John Heimann, Senior Director-Security Programs, Oracle*

***Please remember to complete your speaker evaluation for today. You may leave completed surveys at your seat or turn them in to the SANS registration desk.***

## Tuesday, April 23

8:00 am

**Class & Summit Registration**
Location: Lone Star Foyer

---

9:00 am – 5:00 pm all classes

**Training Courses** (location in parenthesis)

SEC542: Web App Penetration Testing and Ethical Hacking - (Austin North – 2nd Floor)

DEV522: Defending Web Applications Security Essentials - (Austin South – 2nd Floor)

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications - (Cellar – 1st Floor)

DEV544: Secure Coding in .NET: Developing Defensible Applications - (Bouquets – 1st Floor)

---

12:15 - 1:30 p.m.

**Lunch & Learn**
Location: Lone Star – 2nd Floor
*Sponsored by*

DENIM GROUP

***Do You Have a Scanner or a Scanning Program?***

By this point, most organizations have purchased at least one code or application scanning technology to incorporate into their software security program. Unfortunately, for many organizations the scanner represents the entirety of that so-called “program” and often the scanners are not used correctly or on a consistent basis. This presentation looks at the components of a comprehensive software security program and the role that automation plays in these programs. It also looks at common pitfalls organizations encounter when trying to deploy scanning technologies as well as ways to address these issues. Finally it walks through metrics organizations can use to keep tabs on their scanning progress so they can identify and address issues such as portfolio and scanner coverage. Demonstrations using freely available tools are provided as well as discussion of how these approaches can be applied for both commercial and free static and dynamic scanning technologies.

*Speaker: Dan Cornell, Principal, Denim Group*

5:30 - 6:30 pm

**Networking Reception**

Location: Atrium

*Sponsored by*

Sonatype

Join your fellow AppSec attendees for refreshments, networking, and the exchange of ideas. Share best practices and network face-to-face with peers.

---

6:30 - 7:15 pm

***What's Hiding in Your Software Components?: Hidden Risks of Component-Based Software***

Software is no longer written, it's assembled. With 80% of a typical application now being assembled from components, it's time to take a hard look at the new risks posed by this type of development -- and the processes and tools that we'll need in order to keep them in check. Join Ryan Berg, Sonatype CSO, as he shares real-world data on component risks, outlines the scope of the problem, and proposes approaches for managing these risk. You'll learn how security professionals can work cooperatively with application developers to reduce risk AND boost developer efficiency.

*Speaker: Ryan Berg, Chief Security Officer, SonaType*

---

7:15 - 8:00 pm

***Compliance, Security & Innovation: Can They Co-Exist?***

ADP is near and dear to the hearts of many of us, at least twice a month. As one of the world's largest providers of business outsourcing services (including payroll processing), ADP does business in 104 countries worldwide; that's a lot of regulatory requirements to keep track of. Compliance means many things – not just government regulations, but also industry-imposed regulations like PCI and contractual requirements of clients – but it doesn't necessarily mean security. And compliance certainly doesn't mean innovation or customization to the needs and demands of users. How does an international leader like ADP balance cost-effective compliance, iron-clad security of PII and financial data, and the need to customize solutions for users of all types? Hear about their strategies and best practices, and what you can learn from their leadership.

*Speaker: Josh Brown-White, Application Security Architect, ADP*

***Please remember to complete your speaker evaluation for today. You may leave completed surveys at your seat or turn them in to the SANS registration desk.***

## Wednesday, April 24

8:00 am

**Class & Summit Registration**
Location: Lone Star Foyer

---

9:00 am – 5:00 pm all classes

**Training Courses** (location in parenthesis)

SEC542: Web App Penetration Testing and Ethical Hacking - (Austin North – 2nd Floor)

DEV522: Defending Web Applications Security Essentials - (Austin South – 2nd Floor)

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications - (Cellar – 1st Floor)

DEV544: Secure Coding in .NET: Developing Defensible Applications - (Bouquets – 1st Floor)

---

12:15 - 1:30 p.m.

**Lunch & Learn**
Location: Lone Star – 2nd Floor
*Sponsored by*

***Static Vulnerability Analysis in the Development Lifecycle***

Join us for a TexMex lunch buffet and open discussion on best practices and lessons learned on adding Static Vulnerability Analysis in the Development Lifecycle.

*Speaker: Andy Earle, Software Security Consultant, HP Enterprise Security*

---

5:00 - 6:00 pm

**Summit Registration and Networking**
Location: Lone Star
Beverages and light snacks provided

---

6:00 - 6:45 pm

***A Decade of Web Application Security : What Have We Learned?***

What has changed over the last 10 years in web application security? Gain insight into trends in web application vulnerabilities by reviewing data about attacks as well as changes to standards such as the OWASP Top 10 over the last decade. Has the increase in the number and types of tools helped? Has the focus on increasing developer awareness paid off? Find out what our future may hold by taking a look back at what has happened in web application security over the last decade.

*Speaker: Jason Kent, Director of Web Application Security, Qualys*

6:45 - 7:30 pm

***Testing at Cloud Speed***

As the world of system and application deployment continues to change, the sys admin and security community needs to change with it. With agile development and continuous deployment, the pace of change in IT has only increased. After adding in Dev/Ops and cloud, the traditional sys admin and security processes just don't work. How can you rapidly deliver servers and applications while making sure they are built reliably and securely? When you are deploying multiple times a day, when are you going to fit in your week-long security assessment?

A new concept of Test Driven Security, which is loosely based on the tenants of Test Driven Development, is beginning to emerge in the application security community. This talk will cover how Matt is putting the practices in place currently and how you can architect your next security work to be agile enough to keep up with the pace of change today. Even if you are not there today, you will be soon enough.

*Speaker: Matt Tesauro, WTE Project Lead, OWASP*

***Please remember to complete your speaker evaluation for today. You may leave completed surveys at your seat or turn them in to the SANS registration desk.***

## Thursday, April 25

9:00 am – 5:00 pm all classes

**Training Courses** (location in parenthesis)

SEC542: Web App Penetration Testing and Ethical Hacking - (Austin North – 2nd Floor)

DEV522: Defending Web Applications Security Essentials - (Austin South – 2nd Floor)

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications - (Cellar – 1st Floor)

DEV544: Secure Coding in .NET: Developing Defensible Applications - (Bouquets – 1st Floor)

## Friday, April 26 & Saturday, April 27

9:00 am – 5:00 pm all classes

**Training Courses** (location in parenthesis)

SEC542: Web App Penetration Testing and Ethical Hacking - (Austin North – 2nd Floor)

DEV522: Defending Web Applications Security Essentials - (Austin South – 2nd Floor)

# Exhibitors

### Denim Group

Denim Group, the leading secure software development firm, builds custom large-scale software for clients where privacy and security are key project drivers. Denim Group also helps clients secure the software they are building, through security training, SDLC consulting, and a variety of software security testing services.

### HP

HP Fortify, an HP Company, is the market leading solution for automating and managing a comprehensive software security program. With the most advanced technologies available on premise and on demand, HP Fortify empowers organizations to find, fix and fortify all their software applications – from legacy systems to today's mobile applications.

### Industrial Defender

Infogressive was founded upon a single focus: Information security. We reduce risk by creating defense-in-depth networks and we help implement best practices. We achieve this mission through three primary means:

- We acquire and continually train elite talent that prioritizes customer service and executing our standards of excellence.
- We identify market leading, effective technologies that reduce risk economically.
- We build and maintain a network of close, trusted relationships with people involved in the cyber security space all over the world. These relationships include: Information security experts, government, law enforcement, private industry, and academia. These relationships help us stay abreast of what is going on in our industry now and in the future.

### Qualys

Qualys is a pioneer and leading provider of cloud security and compliance solutions with over 6,000 customers in more than 100 countries. The QualysGuard Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance, delivering critical security intelligence on demand. **www.qualys.com**

### Sonatype

Sonatype is leading the component revolution. The company's innovative component lifecycle management products enable organizations to realize the promise of agile, component-based software development while avoiding security, quality and licensing risks.

### Veracode

Veracode is the only independent provider of cloud-based application intelligence andsecurity verification services. The Veracode platform provides the fastest, most comprehensive solution to improve the security of internally developed, purchased or outsourced software applications and third-party components. Visit **www.veracode.com**, follow on Twitter: @**Veracode** or read theVeracode Blog.

### WhiteHat Security

Headquartered in Santa Clara, California, WhiteHat Security delivers the most accurate, complete and cost-effective website security solutions available today. While most companies do a very good job of protecting their networks, websites have emerged as the number one target for attacks. And the ramifications can be sobering. Loss of data. Malware infection. Loss of consumer confidence. A failure to meet regulatory requirements. The truth is, no company can afford the black mark of a website attack. With thousands of websites already under our watchful eyes, WhiteHat Security has an unrivaled, real-world perspective on website risk management.

Infogressive Inc.

VERACODE
Securing the Software That Runs the World

Infogressive was founded upon a single focus: Information security. We reduce risk by creating defense-in-depth networks and we help implement best practices. We achieve this mission through three primary means:

- We acquire and continually train elite talent that prioritizes customer service and executing our standards of excellence.
- We identify market leading, effective technologies that reduce risk economically. We become experts on these technologies to help our clients learn and leverage them into their environments.
- We build and maintain a network of close, trusted relationships with people involved in the cyber security space all over the world. These relationships include: Information security experts, government, law enforcement, private industry, and academia. These relationships help us stay abreast of what is going on in our industry now and in the future. It also allows us to engage these relationships when needed, as we are the first to admit we can't know everything.

We live and breathe security. Some call us paranoid, some call us nerds; we call ourselves vigilant cyber security experts. While the world is being educated about what we do through daily headlines about breaches, we work tirelessly to make sure our clients aren't part of the media frenzy that is sure to continue for decades to come.

**John Reynolds**<br>
**Infogressive**<br>
JR@infogressive.com

**Dave Ferguson**<br>
**Veracode**<br>
DFerguson@veracode.com

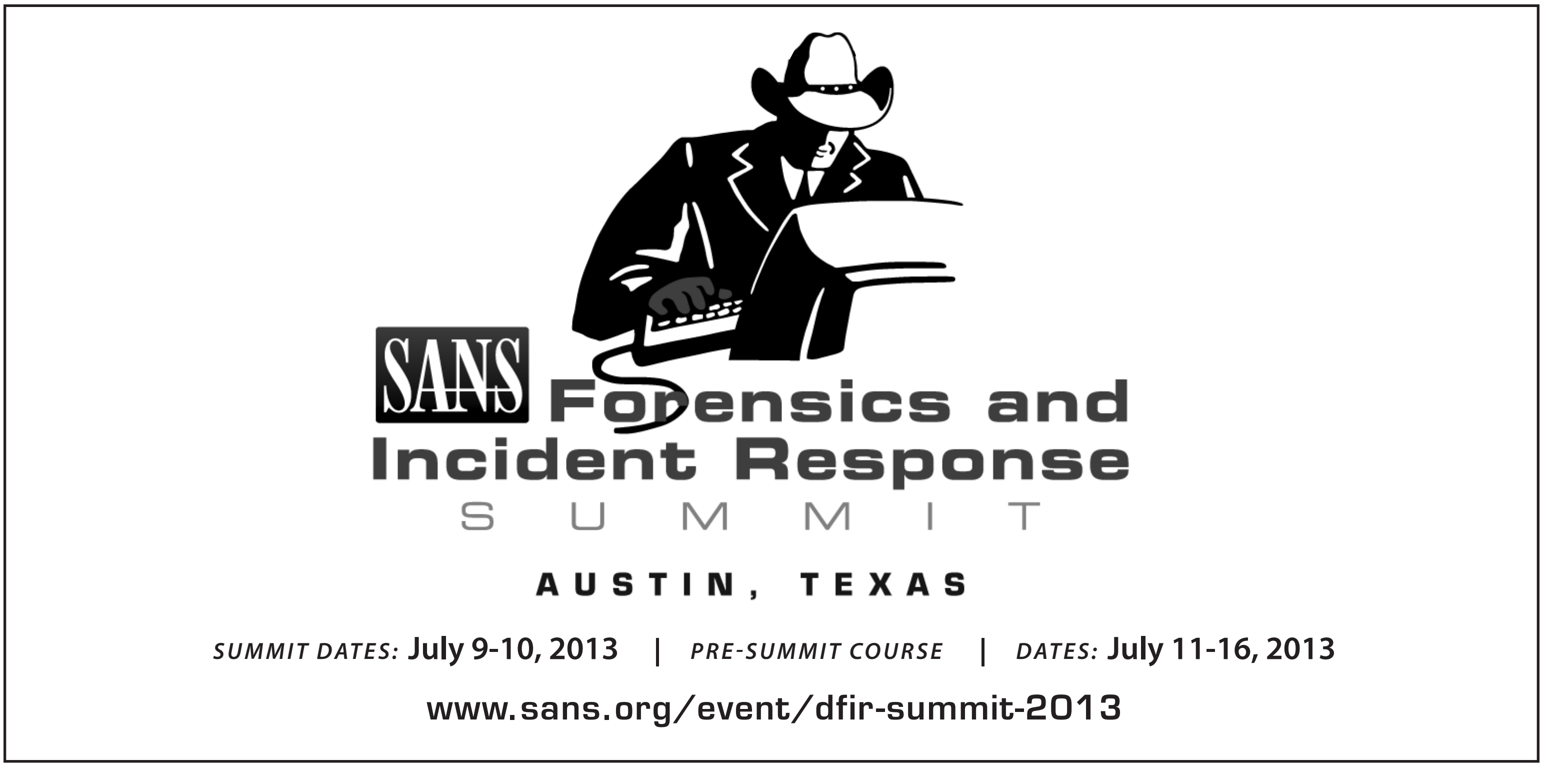
# 80%

**The percentage of your applications that are assembled from components that come from outside your organization**

*Do you know what's in your apps?*
*The Hidden Risks of Component-Based Software*

*See the talk:*
*Tuesday April 23, 2013 6:30pm-7:15pm*
*With Ryan Berg - CSO, Sonatype*

Sonatype



## 2013 UPCOMING SUMMITS & TRAINING COURSES

**Mobile Device Security Summit & Training**
Anaheim, CA | May 30 - June 6

**Security Analytics: Putting Big Data to Work Summit**
Anaheim, CA | May 30

**ICS Security Training Houston**
Houston, TX | June 10-15

**Security Impact of IPv6 Summit & Training**
Washington, DC | June 14-16

**Digital Forensics and Incident Response Summit & Training**
Austin, TX | July 9-16

**ICS Security Training DC**
Washington, DC | August 12-16

**Critical Security Controls Summit**
Washington, DC | August 12-18

**Digital Forensics and Incident Response Summit & Training**
Prague | October 6-12

**ICS Security Training Seattle**
Seattle, WA | October 2013

**Healthcare Summit**
San Francisco, CA | October 2013

**Securing the Internet of Things Summit**
San Francisco, CA | October 2013

**Pen Test Hackfest Training Event & Summit**
Washington, DC | November 7-14

**Asia Pacific ICS Security Summit**
Singapore | December 2-7

For more information on speaking at an upcoming summit or sponsorship opportunities, e-mail SANS at **summit@sans.org**

Visit **www.sans.org/summit** for detailed summit agendas as they become available.