SANS

Critical Security Controls

SUMMIT 2013

Washington, DC

Program Guide

UPCOMING SUMMITS & TRAINING COURSES

2013

Digital Forensics and Incident Response Summit & Training
Prague, Czech Republic | October 6-12

Securing the Internet of Things Summit & Training
San Francisco, CA | October 17-22

Healthcare Cybersecurity Summit
San Francisco, CA | October 23-24

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

Asia Pacific ICS Security Summit & Training
Singapore | December 2-7

2014

AppSec Summit & Training
Austin, TX | February 3-8

Industrial Control Systems Security Summit & Training
Orlando, FL | March 12-18

Digital Forensics & Incident Response Summit & Training
Austin, TX | June 3-10

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.

Agenda

All Summit Sessions will be held in Washington Ballroom (unless noted).

All approved presentations will be available online following the Summit at ***https://files.sans.org/summits/critcontrols13***

An e-mail will be sent out within 5 business days once the presentations are posted.

Monday, August 12

8:00-9:00 am

Registration

9:00-9:45 am

The Critical Security Controls: From Best Practice To Common Practice

Despite great efforts among technologists, policymakers, educators and end users, we have all collectively struggled to establish what we need to do to provide an open and secure internet. But the community around the Critical Security Controls has done a remarkable job of creating a framework for widely applicable, vendor-supported, intuitively-understandable action which can immediately improve the cybersecurity of any organization. So what do we do to scale and support this idea across enterprises, sectors, and nations? Hear why and how the Controls are an essential element of an integrated approach to cybersecurity, one which also encompasses best practices by people and in policy.

***Jane Lute**, Former Deputy Secretary, US Dept. of Homeland Security*

9:45-10:00 am

Networking Break

10:00-10:45 am

The Threat Environment: Using Offense to Inform the Defense

In this session, technical experts will share their insight on current and emerging threats, and their role in the Critical Security Controls. You'll learn how their knowledge is captured in the Controls, giving you a way to identify and prioritize the most effective, highest-leverage defensive steps you should take to stop attacks. The panel of experts will also discuss how the Controls focus on automation of information flow and action is essential to the sharing and use of threat intelligence.

The panel will be moderated by Tony Sager, who served as the chief of every major element of the cyber defense mission at the National Security Agency (NSA), finishing his 34-year career there as Chief of the Vulnerability Analysis and Operations Group and Chief Operating Officer of the IAD (Information Assurance Directorate).

Moderator: ***Tony Sager**, Director, SANS Institute*

Panelists: ***Stephen Brannon**, Senior Researcher, Verizon*
***Marshall Heilman**, Director, Mandiant*
***Adam Meyers**, Director of Intelligence, CrowdStrike*

10:45-11:30 am

Decision Framework for Choosing Solutions

How do organizations effectively select solutions within the context of their business environment and strategy? Learn suggested criteria for choosing solutions that align with the organization's overall strategy and objectives.

***John Pescatore**, Director of Emerging Security Trends, SANS Institute*

11:30 am-12:30 pm

Initial Assessment: Getting Started with the Controls

This session brings together experienced practitioners who have helped many enterprises start down the road to implementation of the Critical Controls. The panel will discuss performing gap analyses (comparing their current security programs with the Critical Controls, identifying gaps, and planning a program to close the gaps). In the process, they will share fascinating data about extra benefits that accrue when those plans have been rolled out.

Moderator: ***Tony Sager**, Director, SANS Institute*

Panelists: ***Addai Borden**, VP-IT Security, Neuberger Berman*
***John Pescatore**, Director of Emerging Security Trends, SANS Institute*
***James Tarala**, Principal Consultant, Enclave Security*

12:30-1:45 pm

Lunch & Learn

Presented by

FORTINET™

&

Infogressive, Inc.

***Aggressive** Information Security*

An Overview of Fortinet's Next Generation Firewalls.

***Justin Kallhoff**, CEO, Infogressive, Inc.*

1:45-2:45 pm

Measuring Up: Assessing Progress in an Enterprise

This talk will examine two key aspects of tracking and measuring Critical Controls efforts:

- the measurement of the progress of implementation
- the achievement of the business case/drivers.

***James Tarala**, Principal Consultant, Enclave Security*

2:45-3:45 pm

Putting the Critical Controls into Action: Real World Use Cases

Organizations have come to accept that there is no single product that can guarantee complete security. But there are alternatives: by implementing the CSC through the application of prioritized system administration techniques, IT can harden their computer infrastructure. With a combination of accurate inventory of systems and applications, secure base configurations, diligent patching and segmented network, organizations become immune to opportunistic attacks and raises the bar for targeted attacks. Larry and Wolfgang will go over the implementation challenges in the

20 Critical Security Controls and provide introduce a set of intuitive use cases and procedures that can serve as guidelines for the IT department and ease them through an implementation.

***Wolfgang Kandek**, Chief Technical Officer, Qualys*
***Larry Wilson**, Information Security Officer, UMASS President's Office*

3:45-4:00 pm

Networking Break

4:00-5:00 pm

What Works: The Controls in Action

In this session, Tony Sager will guide a discussion on how the controls were adopted in organizations in a way that immediately and radically reduced vulnerabilities and risks. He will also share evidence that just four of the Critical Controls are surprisingly effective in stopping what is commonly known as the "advanced persistent threat."

*Moderator: **Tony Sager**, Director, SANS Institute*

*Panelists: **Jim Beechey**, Cyber Security Manager, Consumer Energy*
***Jonathan C. Trull**, Chief Information Security Officer, State of Colorado Governor's Office of Information Technology*
***Larry Wilson**, Information Security Officer, UMASS President's Office*

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.

5:00-7:00 pm

Networking Reception & Summit Suite

Hosted by

FireEye™

Join your fellow SANS attendees for a chance to network over refreshments and light hors d'oeuvres.

Tuesday, August 13

8:00 am-9:00 am

Registration

9:00-10:00 am

Common Framework: Working With National & Industry Standards

In an earlier session, we explored how the Critical Controls integrate into an existing security program and fit into a comprehensive risk management program. This session pulls in a panel of leading experts to discuss the details behind the relationship of the Critical Controls to various key, national and industry standards.

Moderator: ***Tony Sager****, Director, SANS Institute*

Panelists: ***Adam Montville****, Technical Product Manager, Center for Internet Security (CIS)*
John Streufert*, Director, Federal Network Resilience, U.S. Department of Homeland Security*
Speaker from CPNI

10:00-10:15 am

Networking Break and Vendor Expo

10:15-11:15 am

How to "Connect Security to the Business" (CSTB)

When CISOs are briefing their executive teams or boards on the organization's security (usually only when there's a security incident), this is usually the challenge. Distill the volumes of data, assets, silos, operations, threats, and remediations down to a couple of key points. And this is to an audience who typically get their security information from their mobile newsfeed or WSJ. No wonder the average tenure is about 18 months for most CISOs.

How to "Connect Security to the Business" (CSTB), describes the issues and suggests some meaningful ways CISOs, CIOs, and their IT Security teams can effectively communicate security metrics to the business or mission leadership.

Katherine A. Brocklehurst*, Senior Product Marketing Manager, Tripwire*

11:15 am - 12:15 pm

The Integrator Perspective: Continuing the Implementation of the Controls

In an earlier session, we brought together experienced practitioners who discussed helping enterprises get started down the road to implementation of the Critical Controls. In this session, moderated by Dr. Eric Cole, participants discuss continued adoption.

Dr. Eric Cole*, Fellow, SANS Institute*

12:15 - 1:30 pm

Lunch & Learn

Presented by

Delivering Situational Awareness - Putting the Critical Security Controls to Work

Organizations of all sizes, and across almost every industry, face significant challenges protecting critical IT assets from an exponentially increasing threat landscape. And, of course, serious vulnerabilities continue to be discovered in both legacy and emerging IT systems. Many security programs have focused too much on compliance reporting and not enough on implementing effective security controls that have been shown to significantly reduce the risk of information breach.

In this session, Brian Mehlman, Senior Director of Product Management, at EiQ Networks, will discuss an approach for delivering simplified security intelligence through security control automation. He will also provide a case study on how EiQ's flagship solution, SecureVue®, can increase information security, improve operational efficiency, and lower cost for an organization through automation of many of the top Critical Security Controls recommended by SANS.

Brian Mehlman*, Senior Director, Product Management at EiQ Networks*

1:30-2:30 pm

Increase Security Effectiveness with the Critical Controls

The Critical Security Controls (CSCs) have been shown to increase the effectiveness of security programs and lower the cost of maintaining security across government and commercial organizations. These controls focus on real-world security issues and not just a checkbox compliance exercise by evaluating products, processes, architectures, and services to address constantly evolving attacks. Organizations can achieve immediate results by implementing and automating the controls in a prioritized manner.

Tenable solutions allow organizations to implement and automate the CSCs in a unique way by combining active, passive, and log correlation. This combination provides broad coverage of the critical security controls and offers capabilities that others cannot deliver such as identification of 100% of assets, continuous real-time vulnerability assessment, and integrated log correlation combined with the most popular scanner on the market, Nessus. Learn more and get your questions answered in this interactive discussion.

***Ron Gula**, CEO, Tenable Network Security*

2:30-2:45 pm

Networking Break and Vendor Expo

2:45-3:30 pm

The Future of The Controls

In this final session, we'll look at the future of the Controls, including the development of a global career development and pathways program. This program aims to map and enhance career growth opportunities for cybersecurity professionals , critical for companies trying to ensure they have the talent they need.

***Tony Sager**, Director, SANS Institute*

Thank you for attending the SANS Critical Security Controls Summit.

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

Exhibitors

EiQ Networks
EiQ Networks, a pioneer in simplified security, risk and compliance solutions, transforms how organizations identify threats, mitigate risks and enable compliance. SecureVue®, a unified situational awareness™ platform, proactively detects threats, minimizes "false positives" and delivers timely and actionable intelligence by simplifying often complex interactions and relationships between security, risk and compliance.

FireEye
FireEye is the leader in stopping next generation threats such as zero-day and next-generation attacks that bypass traditional defenses and compromise over 95% of networks. The FireEye solution is the world's only signature-less protection against multiple threat vectors. FireEye solutions are deployed by more than 25% of the Fortune 100.

Fortinet
Fortinet, a global provider of IT security, delivers customer-proven solutions that provideorganizations with the power to protect and control their IT infrastructure. Our customers rely onour purpose-built technologies, integrated solution architecture, and global security intelligence toblock external threats and gain precise control of their network, data, and users.

Infogressive
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 (www.qualys.com) 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.

Tenable Network Security
Tenable Network Security is relied upon by more than 17,000 organizations, including the entire U.S. Department of Defense and many of the world's largest companies and governments, to stay ahead of emerging vulnerabilities, threats and compliance-related risks. Its Nessus and SecurityCenter solutions continue to set the standard for identifying vulnerabilities, preventing attacks and complying with a multitude of regulatory requirements. For more information, please visit **www.tenable.com**.

Tripwire
Tripwire's IT security software reduces risk, ensures systems and data security, and automates regulatory compliance. Tripwire offerings solve the security configuration management, continuous monitoring, and incident detection problems facing organizations of all sizes, as stand-alone solutions or in concert with other IT security controls.

Simplified Security Intelligence

Has Your Information Security Program Reached Critical Mass?

85% of breaches go undetected because you don't have the right information. With most security products, you're stuck with mountains of data—without the intelligence you need to interpret it. Until now.

The SANS Top 20 Critical Security Controls provide the framework for effective cyber defense. SecureVue® from EiQ Networks simplifies and automates monitoring of many of the controls and provides assessment and guidance to keep your environment secure. Try it for yourself.

For a limited time, get a free 5-node license at:
offers.eiqnetworks.com/SANS

EiQ Networks.
Get the Whole Picture.

ADVANCED CYBER ATTACKS

HAVE PENETRATED **95%** OF ALL NETWORKS.

THINK YOU'RE IN THE 5%?

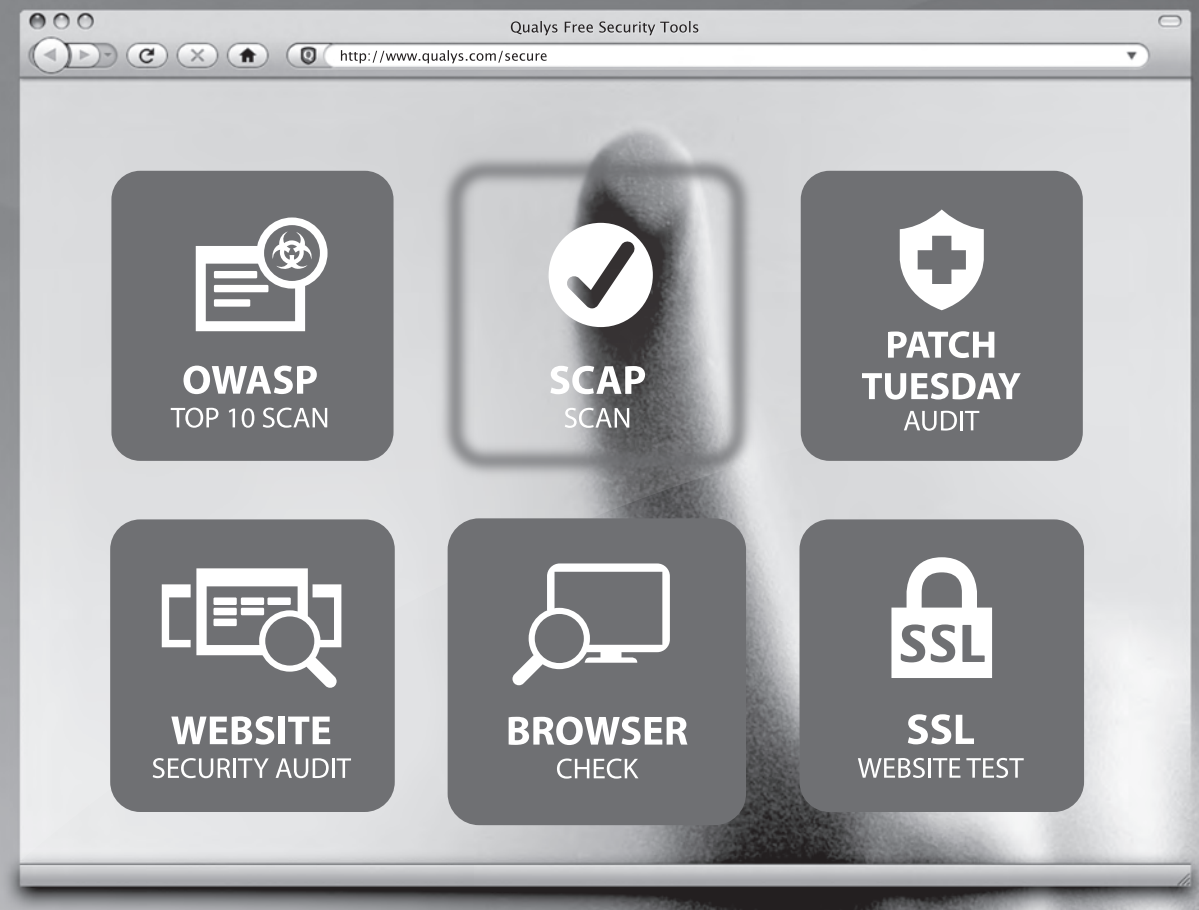
You may think your existing security defenses prevent advanced cyber attacks from entering your network and stealing your data. They don't. Advanced attacks easily evade traditional and next-generation firewalls, IPS, AV, and gateways.

FireEye is your best defense. Put a stop to advanced attacks with next-generation threat protection. Visit us today at **www.FireEye.com** and let us help you close the hole in your network.

FireEye™

Free Security at Your Fingertips

Visit **qualys.com/secure** today!



QUALYS®
NASDAQ: QLYS

Find out if you are secure from hackers and compliant with regulations. Audit the security of browsers, systems and web applications in your organization. Qualys makes these free security tools available at your fingertips at **www.qualys.com/secure.**

tenable
network security

Attend a technical session by

Ron Gula

Tenable CEO and Co-founder

ON HOW TO

Increase Security Effectiveness

WITH THE

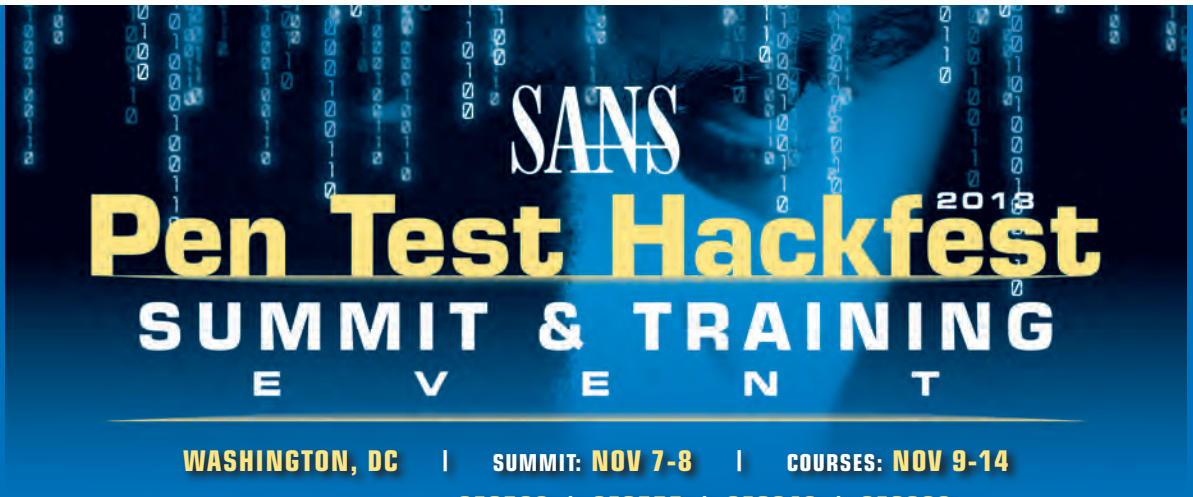
SANS 20 Critical Controls

Find out how Tenable solutions are enabling organizations to automate the 20 CSCs by uniquely combining active scanning, passive monitoring, and log analysis.

Tuesday, August 13th

1:30 p.m. – 2:30 p.m.

www.tenable.com



WASHINGTON, DC | SUMMIT: NOV 7-8 | COURSES: NOV 9-14

COURSES AVAILABLE: SEC560 | SEC575 | SEC642 | SEC660

SANS is hosting our ultimate annual penetration testing training event in November. Featuring top-notch talks, in-depth training, and evening activities to help participants build awesome skills, the SANS Pen Test Hackfest Summit and Training Event is specially designed for penetration testers across a broad range of skills and disciplines. Here are the top 5 reasons to attend this event:

NetWars, NetWars, NetWars! This event will include FOUR full evenings of NetWars challenges, doubling the amount of NetWars time over a traditional SANS conference. NetWars is an action-packed challenge environment where people can build their skills while having fun.

Coin-a-palooza For participants who have taken a given SANS course, but have not won the capture-the-flag challenge coin, this event will offer the ability to catch up on the coins by participating in the four nights of NetWars challenges. If you've taken SEC504 in the past (but didn't win the coin), and make it from NetWars Level 1 into 2, you'll earn the 504 coin! If you make it into Level 3, you'll get your choice of a 542, 560, or 575 coin, provided you've taken the associated course sometime in the past. Make it into Level 4, and you'll get your choice of a 617, 642, or 660 coin if you've had those classes! And, if you win NetWars, you'll get the NetWars coin. With Coin-a-palooza, you'll have an opportunity to win up to 4 challenge coins for your collection.

CyberCity The SANS CyberCity project helps train cyber warriors that computer and network activities can have major kinetic impact on the real-world. With its power grid, traffic lights, and water reservoir included in a physical model city, participants access and gain control over these assets, preventing attackers from wreaking havoc. This event will include a full evening session of CyberCity missions, the first time SANS has offered access to CyberCity at a training event!

Summit Two full-days of in-depth presentations chock full of cutting-edge penetration testing topics focused on helping you provide technical excellence and real business value in your vulnerability assessment and penetration testing work.

Training Six days of deep SANS training in real-world penetration techniques you can use immediately when you return to your job.

Learn more at **www.sans.org/event/pen-test-hack-fest-2013**

Penetration Testing Resources

Penetration Testing Blog Posts
http://pen-testing.sans.org/blog

Penetration Testing Links
http://pen-testing.sans.org/resources/links

Twitter
https://twitter.com/#!/pentesttips

Webcasts
http://pen-testing.sans.org/resources/webcasts

SANS Penetration Testing Whitepapers
http://pen-testing.sans.org/resources/whitepapers