The Vulnerability Management Summit agenda is dynamic and continues to evolve. In order to bring you the most up-to-date information and top rated speakers, the speakers and topics listed on this agenda may change.

Tuesday, August 14th

9:00-10:00 a.m.
Keynote Address
Unexpected Results: How I Learned to Love Complexity
To keep your critical infrastructure safe, you have to stay several steps ahead of numerous threats from multiple vectors, which attackers only need to be right one time to wreak havoc. In this talk, Tim Roxey will discuss the levels of complexity across just one critical infrastructure and will look at the four domains of complexity, with an eye towards applying kill chains and threats as a solution space.
Tim Roxey, Chief Cyber Security Officer, North American Electric Reliability Company (NERC)

10:00-11:00 a.m.
Expert Briefing
Vulnerability Management: What, Why & How
In the last several years, the field of vulnerability management has grown considerably, and the current scope of the domain now includes many traditionally disparate focus areas. Recent advancements in managed security services and new frameworks for the deployment of active countermeasures can make the task of building an effective vulnerability management strategy difficult. As cyber threats continue to increase in capability and quantity, asset owners are continuously challenged by trying to balance effective network operations and the increasing need to adjust their security countermeasures in real-time.
Mark Fabro, Summit Chair, President & Chief Security Scientist, Lofty Perch, Inc.

11:00-11:20 a.m.
Networking Break

11:20 a.m. -Noon
Case Study
Inside Job: Improving Security through In-House Innovation
In the absence of commercial products to address their requirements, USAA turned to in-house developers to create custom solutions. Facing challenges created by active vulnerability scanning, USAA Information Security, Change Management and System Availability teams worked together to create a self-service tool that shares scan schedules and improves communication between security and operations. But innovation didn't stop there; USAA also developed tools to combine Vulnerability Assessment and Security Event Monitoring (SEM) data to improve the Incident Response lifecycle. By combining event context with streamlined access to on demand scans and results, security analysts are better equipped to make informed decisions.
Josh Stevens, CISSP, CISA, Sr. Info Security Analyst, USAA

Noon-1:15 p.m.
Lunch & Learn Presented by Qualys & Denim Group
Web Application Scanning and Remediation in the SDLC
Qualys will review some of the reasons that web application security is so important - citing data from the Verizon Data Breach Investigations Report, which identified web applications as one of the primary attack and data loss vectors for the breaches investigated. Qualys will show how a cloud-based scanning service helps organizations find and fix web application vulnerabilities earlier in the software development lifecycle, which lowers both the risk as well as the cost associated with addressing the security issues. Denim Group will then show how the company's vulnerability management system, ThreadFix, helps customers use the data from Qualys scans to fix software vulnerabilities faster. ThreadFix gives a centralized view of software security defects across development teams and projects and simplifies feeds to software issue trackers. This presentation will show attendees how they can implement these tools to take a more proactive approach to application security.
Speakers: Will Bechtel, CISSP, CISA, PMP, Director of Product Management, Qualys
Dan Cornell, CTO, Denim Group

1:15-2:00 p.m.
User Panel
Are You In or Out? -- Outsourcing v. In-House
The economics associated with vulnerability management make outsourcing very attractive. But does letting an outside entity defend your critical information infrastructure really make sense? The complexity of cost versus ownership makes the decision difficult, and there are many aspects that need to be addressed when deciding. There is no substitution for experience and hindsight is always 20/20. The right option depends on the organization's preferences, goals, reasons for implementing vulnerability management, and capabilities of the IT team. Panelists share their decision making process and lessons learned.
Moderator: Mark Fabro, Summit Chair, President & Chief Security Scientist, Lofty Perch, Inc.
Panelists:
Charles W. Luginbill, CISSP, Assistant Treasurer/IT Director, Nebraska State Treasurer's Office
Nathan Sportsman, Founder & CEO, Praetorian
Greg Smith, Security Risk Analyst, Texas State Comptroller of Public Accounts

2:00-2:45 p.m.
User Panel
Ensuring Defense in Depth: Managing Vulnerabilities in Rapidly Changing Networks
Good networks are scalable and agile to grow and change with the organization's needs. But managing security in rapidly evolving networks is like trying to hit a moving target. Mobile devices and loosely-defined BYOD policies have also thrown many security pros into a tail spin. By the time one challenge is met, there are three new ones waiting. What are the best practices for managing vulnerabilities in a constantly shifting network environment?
Vern Williams, CISSP, ISSEP, CSSLP, CSO, The Patria Group
Kevin Lackey, Sr. Security Analyst, Electric Reliability Council of Texas (ERCOT)

2:45-3:00 p.m.
Networking Break

3:00-4:00 p.m.

Case Study

A Tale of Two Systems: When VM Programs Collide

In April of 2012, Medco Health Systems acquired and merged with Express Scripts, Inc. creating the country's leading healthcare services company. Great news for healthcare consumers who need affordable and convenient prescriptions; not such great news for IT staff who were met with the challenge of figuring out how to integrate two quite different vulnerability management programs. In this session, you'll learn how Express Scripts is meeting the challenge, including the assessment method used to determine the pros and cons of the two different models, the decision-making process around identifying third party beta integration tools, the successes to date, and a roadmap for completing the integration.

Speaker: Tim West, Information Risk Management, Express Scripts, Inc.

4:00:-5:00 p.m.

Case Study

Vulnerability Management from Scratch: Security and PCI Compliance

Love's owns and operates a chain of convenience stores and travel centers, with 292 locations in 38 states nationwide. With the growth of the company bringing them to a Level 1 merchant, and so many customers swiping their credit cards around the clock, Love's is keenly cognizant of compliance with the Payment Card Industry (PCI) Data Security Standard. But their vulnerability management strategy was running on empty, until Sherry and her team built one from scratch. Learn how they met this challenge.

Speaker: Sherry Zimmerman, CISSP, GSEC, Security Manager, Love's Travel Stops and Country Stores

Wednesday, August 15th

7:45-8:45 a.m.
Breakfast & Learn Presented by Rapid7
Rapid7 & Metasploit – Detecting Threats, Mitigating Risk and Meeting Compliance
Rapid7 offers the only integrated threat management solution that enables organizations to implement and maintain best practices and optimize their network security, Web application security and database security strategies. The Company's flagship product, NeXpose®, provides vulnerability management, policy compliance and remediation management and is designed for organizations with large networks, which require the highest levels of scalability, performance, customizability and deployment flexibility. Complementing its remediation-based reports, Rapid7 helps enterprises to further prioritize remediation with NeXpose's newest feature, Exploit Exposure, which identifies whether an exploit exists and combines exploit ranking with other factors to determine the probability of a successful attack. Attend this Breakfast & Learn to gain insight into Rapid7, NeXpose and Metasploit.
Trevor Richardson, Security Solutions Advisor, Rapid7

9:00-10:00 a.m.
Keynote Address
Mind the Gap: Hackable Holes You Don't Even Know You Have
The number of connected devices and machines grows exponentially by the week, and network operators are working hard to ensure impenetrable security …right? Speed and agility don't always make the best bedfellows for ironclad security; and skilled hackers can find even the tiniest gaps in security and use them to tear the network asunder. Learn what you don't know you don't know…if you dare.
Billy Rios, Security Researcher, Google, and Co-Author, *Hacking: The Next Generation*

10:00-11:00 a.m.
User Panel
Don't Forget the App: Taking Vulnerability Management to the Extreme
Asset owners work hard to identify vulnerabilities at the network and host levels, but it is the applications that are often the vector of choice for attackers. New strategies for addressing the vulnerabilities in applications are rapidly emerging – and you need to know the options to determine what's best for you. This session is dedicated to application security assessments, the methods of analysis, and how to incorporate results into your vulnerability management plan.
Moderator: John Dickson, CISSP, Principal, Denim Group
Speakers:
Chris Aidan, CISO, Freescale Semiconductor
Monica Bush, Security Analyst, University of Wisconsin at Madison
Alex Tosheff, CISO, x.commerce

11:00-11:15 a.m.
Networking Break

11:15-Noon
Expert Briefing
Threat Intelligence: Useful, but at What Price?

The rapid emergence of third-party threat intelligence services has created more options for the asset owner. However, how do you select the best provider based on your needs? Do you subscribe to all data of just the intelligence that is specific to your operations? This session will review the service options available and help make sure you get the right data - at the right time - and in the right format.
Kevin Lackey, Sr. Security Analyst, Electric Reliability Council of Texas (ERCOT)

Noon-1:15 p.m.
Lunch & Learn, Presented by Fortinet & Infogressive
Justin Kallhoff, CEO, Inforgressive
Robert Ayoub, Fortinet

1:15-2:15 p.m.
User Panel
Applied Data: Using Assessment and Audit Results to Refine Your Vulnerability Management Strategy
It's a valid and worthwhile approach to vulnerability management: scan, analyze results, and fine-tune based on the findings. But is it the best approach? Is there a danger in letting audits or auditors help define a VM strategy?
Panelists:
Matthew Reed GCFE, GCIH, GCIA. GPEN, Director – Information Security Compliance and Awareness, Consolidated Graphics
Sherry Zimmerman, CISSP, GSEC, Security Manager, Love's Travel Stops and Country Stores

2:15-2:35 p.m.
Networking Break

2:35-3:30 p.m.
User Briefing
Combating Spear-phishing: Convergence of Intel, Operations, and Forensics
The Air Force Network or "AFNET" is vigilantly being defended 24/7 against attacks by APT, cyber-criminals, and cyber-hacktivists. This briefing will give the attendee insight to Air Force Computer Network Defense Operations (AF-CND) and provide a case study from an intelligence tip to execution of vulnerability management (prevention), detection, response, and sharing with the community.
Speakers:
Billy Rodriguez, Chief, Intrusion Prevention Section, 33NWS (AFCERT)
Jacob Stauffer, GCFA, GREM, CISSP, Chief, Intrusion Forensics Section, 33NWS (AFCERT)

3:30-4:30 p.m.
Closing Keynote
Empirical Exploitation
Learn best practices and strategies for identifying soft spots in security through global network analysis.
HD Moore, CSO, Rapid7 & Chief Architect, Metasploit