ISSA International Conference
Detailed Agenda

Monday, October 9, 2017

ISSA Chapter Leaders Summit
10/9/2017, 10:00 am – 5:00 pm, Grande C
Join ISSA leaders from around the world in San Diego, California for an event focused on growing and supporting your chapters. Whether you are a new or long-time chapter board member, this one-day summit is a must. How can you make it easy for members to get the most out of their membership? Learn how to increase the number of volunteers and build an effective board to help you. The Chapter Leaders Summit is open to all ISSA Chapter Board Members, Chapter Officers & Chapter Management Team Members.

International Conference Registration Open
10/9/2017, 4:45 pm – 7:00 pm, Bayview Foyer

Opening Reception and Capture the Flag in the Exhibit Hall
10/9/2017, 5:00 pm – 7:00 pm, Pavilion

Tuesday, October 10, 2017

International Conference Registration Open
10/10/2017, 7:45 am – 4:00 pm, Bayview Foyer

Breakfast, Welcome Remarks, and Keynote Address
10/10/2017, 8:30 am – 10:15 am, Grande B/C

Exhibit Hall Open
10/10/2017, 10:15 am – 4:15 pm, Pavilion

Break in the Exhibit Hall
10/10/2017, 10:15 am – 11:00 am, Pavilion

Cyber Solutions Live Session
10/10/2017, 10:30 am – 10:50 am, Pavilion

Breakout Sessions: 11:00 am – 11:45 am

Featured Session: Career Advice Panel: Ask the Experts
10/10/2017, 11:00 am - 11:45 am, Grande B/C
Track: Career Development for the Information Security Professional
Are you looking to take your cybersecurity career to the next level? Join our panel of experts for a Career Advice Panel. From education and certifications, to interview and communication skills, we will cover everything you need to know to make a lasting impression. Get perspectives on career growth from recruiters, practitioners, and seasoned industry leaders.
Speaker information coming soon!

GDPR is Effective May 2018: If you operate in Europe and don't know that acronym, you probably should attend this session.
10/10/2017, 11:00 am - 11:45 am, Spinnaker
Track: Laws and Regulations
The General Data Protection Regulation becomes effective May 25, 2018. Every company that processes personal data from the EU will need to comply with this new regulation. Fines may be assessed against non-compliant companies at a rate of 4% of global revenue (not profit, not limited to EU). This presentation will focus on practical implementation advice for compliance with this new regime. Learn from both outside counsel and in-house attorneys on how they are working with information security, information technology, and privacy departments to prepare.
Nick Merker: Partner, Ice Miller LLP, @nmerker
Stephen Reynolds: Partner, Ice Miller LLP, @steyren
Kevin Nassery: Managing Principal, Synopsys, Inc., @knassery

Lessons Learned Securely Embracing DevOps/Agile
10/10/2017, 11:00 am - 11:45 am, Nautilus 1
Track: Application Security
The standard approach for web application security over the last decade and beyond has focused heavily on slow gatekeeping controls like static analysis and dynamic scanning. However, these controls was originally designed in a world of Waterfall development and their heavy weight nature often cause more problems than they solve in today's world of agile, DevOps, and CI/CD. This talk will share practical lessons learned at Etsy on the most effective application security techniques in todays increasingly rapid world of application creation and delivery. Specifically, it will cover how to: 1) Adapt traditionally heavyweight controls like static analysis and dynamic scanning to lightweight efforts that work in modern development and deployment practices 2) Obtain visibility to enable, rather than hinder, development and DevOps teams ability to iterate quickly 3) Measure maturity of your

organizations security efforts in a non-theoretical way
Zane Lackey: Chief Security Officer, Signal Sciences, @zanelackey

EAS-SEC - framework to align ERP Security with global Cybersecurity initiatives
10/10/2017, 11:00 am - 11:45 am, Nautilus 2
Track: Application Security
EAS-SEC SAP Cybersecurity Framework is designed to systemize all the necessary activities to secure business applications, e.g. ERP System, against cyberattacks and espionage, sabotage, and fraud. The growing number of incidents against ERP systems and the looming majority of new vulnerabilities appearing almost daily require systemizing approaches to secure ERP systems. Security managers have not only to identify, analyze vulnerabilities, and control access, e.g. introducing Segregation of Duties, but also in global terms regard every aspect of security management ranging from executive support and creation of effective processes to incident management. All the above has now been implemented in our framework. It accumulated 10 years of my research in this field from the first identified vulnerability in 2007 to my experience working with the heads of security departments at the world's largest companies in different industries. The aim of this framework is to provide all critical orientations toward ensuring security of ERP systems and underscore the most important steps for each of the aforementioned areas. This document, as well as all EAS-SEC guidelines, is based on the approach that integrates the comprehensive coverage, on the one hand, and the priority of implementation on the other. This methodology allows you to focus the efforts applying the Pareto principle. The framework is divided into 4 key areas, i.e. Predict, Prevent, Detect, and Respond according to Gartner's PPDR Model. There is a number of required initiatives in each direction. These initiatives were selected to assemble best practices from the current frameworks and standards such as NIST, SANS, CSC, ISO with regard to the specific nature of ERP systems. This presentation will reveal the details and elaborate on the significant fields such as Vulnerability Management, SDLC, Secure Architecture, and Threat Detection.
Alexande Polyakovr: CTO, EASSEC, ERPScan, @sh2kerr

Let's Hack a Thing!
10/10/2017, 11:00 am - 11:45 am, Nautilus 3
Track: Infrastructure
Let's take IoT security from conference buzzword to a hands-on reality; no engineering experience required. This workshop will take an adversary's perspective of the IoT with live demonstrations, hands-on activities, and real-world case studies. Attendees will gain an understanding of how attackers target and exploit IoT devices, and what can be done to present a harder attack surface. The planned agenda is: First Half: Attacking the Device = Introduction and Goals (5 minutes) = Embedded Linux: A Crash Course (10 minutes) = OSINT Research: Forums, the FCC and more (10 minutes) = Cracking the Case: Hardware Teardown of an IoT Device (10 minutes) = Hardware Hacking: Finding Points of Interaction (10 minutes) = Slack time (5 minutes) Second Half: Establishing a Presence and Expanding = Review of First Half and the Path Forward (5 minutes) = Fun with Firmware: Extracting and Exploring (15 minutes) = Implantation and Exploitation (15 minutes) = What We Didn't Cover and Where to Learn

More (5 minutes) = Questions and Answers (10 minutes) Additional Information: -\tThe workshop will use a combination of â€œfreshâ€ and pre-prepared devices to keep things running on time. -\tFor hands-on exercises, attendees will be divided into 3 groups. -\tAttack activity will be limited to local devices- no upstream (read: unlawful) activities will be performed or possible. -\tTo enable self-study after the workshop, attendees will receive a BOM and methodology. The targeted device will be low-cost and commonly available. -\tTo reiterate: No previous experience is required.
Tony Gambacorta: Vice President, Security Operations, Synack, @tgambacorta

...AGAIN?!?! What I learned from our Ransomware events
10/10/2017, 11:00 am - 11:45 am, Nautilus 4
Track: Incident Response
Two Ransomware events in 11 days will teach an information security professional a lot about their organization. In this talk I will discuss the "real world practical experience" responding to over four million files being encrypted (twice) gave me and what could have been done differently to limit the impact. You will hear about the attack vectors, controls that broke down, and the mistakes that were made that lead to incident. Finally, I will cover the changes we made to mitigate the risk of future incidents in impact of a potential incident.
Justin Bumpus: Director of Information Security, GEODIS Logistics US, @chmpagnprotect

Break and Book Signing in the Exhibit Hall
10/10/2017, 11:45 am – 12:15 pm, Pavilion

Breakout Sessions: 12:15 pm – 1:00 pm

Sherman, Set the Wayback Machine to Risk!
10/10/2017, 12:15 pm - 1:00 pm, Nautilus 1
Track: Business Skills for the Information Security Professional
Let's take a trip in the wayback machine and find out what gambling and diseases and stock market performance have to do with risk management. Join a lighthearted but deep talk that looks at the discoveries that created our modern concept of risk and eliminated fate as a legitimate business excuse. Then learn how those theories can be leveraged with current risk management practices to improve how your organization effectively manages risks.
James K. Adamson: Principle Consultant, Urbane Security, @jameskdamson

The Power of Trust: How Application Control Stops Ransomware and other Malware
10/10/2017, 12:15 pm - 1:00 pm, Nautilus 2
Track: Application Security
Homeland Security's US-CERT recommends "App Control" as the #1 Malware Mitigation Strategy. What is this

technology, and how does it block what Antivirus can't? Hackers are winning the cyberwar and the global impact of malware has exceeded $3 Trillion and is now more profitable than the global drug trade in marijuana, cocaine and heroin combined. The cost of Ransomware in Q1 2016 was $209 Million. Almost a 3,500% increase from 2015. Application Control is the number one type of breach prevention solution recommended by Dept. of Homeland Security's US-CERT, Australia's ASD, Canada, AIG, SANS, ISA, and NACD. It's the only effective solution to the rapidly expanding array of today's ransomware and malware threats.
Steven "Ziggy" Shanklin: Founder & CEO, White Cloud Security, Inc.

Weaponizing Threat Intelligence - A Practical and Actionable Approach
10/10/2017, 12:15 pm - 1:00 pm, Nautilus 3
Track: Infrastructure
As more attacks occur, defenders are depending on threat intelligence to get early notification of attacks. By analyzing the latest indicators of compromise (IoCs), organizations can react quickly on attacks targeting their peers before they become a victim. However, the challenge for organizations is how to operationalize and weaponize this threat intelligence data. Using the payment industry as a case study, we present ways to weaponize threat intelligence-- from publicly-available tools to more sophisticated approaches that transform IoCs into breach simulations.
Itzik Kotler: CTO and Co-Founder, SafeBreach, SafeBreach, @itzikkotler
Glenn Jones: Head of Payment System Cyber Intelligence, Visa

Lunch in the Exhibit Hall
10/10/2017: 1:00 pm – 2:00 pm, Pavilion

Breakout Sessions: 2:00 pm – 2:45 pm

Featured Session: The Analogue Prism of Network Security
10/10/2017, 2:00 pm - 2:45 pm, Grande B/C
Track: Infrastructure
Imagine if network security had no '0's and no '1's. That Digital was not Binary. Imagine, instead, that network security has no absolutes but applies 'Continua'. Imagine if we added dynamic analogue functionality to security processes. Imagine if we used OODA and feedback and feedforward loops as core security concepts. Imagine if we added the word 'Time' to every question and every answer when discussing security. Imagine we can actually employ Negative Time. Imagine if we added new OOB functionality to TCP/IP rather than redesign fundamental communications protocols. Imagine. Just imagine how our views of security would suddenly change, and new answers, approaches and models appeared… just because we looked at security through an analogue prism. Winn Schwartau will walk us through a new conceptual model of security (Not a Product or Vendor anything! Just some ideas…) that applies to everything from coding to networking to inter-networking… and maybe, just maybe, in its

abstraction, solves DDoS, Spam and Phishing? Bring it on and tell Winn what is wrong with his ideas. THIS CAN BE MADE (Preferably) into a Workshop for more technical approach... it is Geeky!!!
Winn Schwartau: Founder, SAC

Global Shortage on Cyber Security Workforce: An Analysis of a Complex Issue
10/10/2017, 2:00 pm - 2:45 pm, Spinnaker
Track: Career Development for the Information Security Professional
Everywhere we turn, we hear that there is a shortage of cyber security professionals with highly sought after skill sets and experienced tradecraft to fill widening cyber security program requirements. I have sat on workforce development panels with federal, state and city government leaders, education professionals and industry partners looking for ways to address the problem. I have seen many startup companies claiming they have the key to filling the needs of various industries. I have also seen well-established organizations realigning current training & certification programs in an effort to keep up with the startups. While very few are embedded into true workforce development initiatives, most companies are jumping on the bandwagon and trying to capitalize on a new revenue stream called “Cyber” or “Cyber Security”. My take away is that the issue is more complex than just finding the right person with the right skills to fill a need. There are several factors that need to be considered when analyzing the problem, which do not revolve around training and certification.
Moderator: Dr. Shawn Murray: Principal Scientist, United States Missile Defense Agency.

Growth & Opportunities for Women in Cybersecurity
10/10/2017, 2:00 pm - 2:45 pm, Nautilus 1
Track: Career Development for the Information Security Professional
This session will highlight the growth of women in cybersecuity as they expand their technical expertise and defy stigmas of what is the norm in technology. This session will also highlight paths that some successful women in cybersecurity have taken and share advice for those who are desirous to do so.
Asia A Lewis: Manager of Security and Privacy, Protiviti

Saving the Perimeter
10/10/2017, 2:00 pm - 2:45 pm, Nautilus 3
Track: Infrastructure
The talk will be divided into two distinct parts. The first part will discuss what it means to have a perimeter in a world full of clouds, outsourcing, BYOD, and SAAS vendors. These trends break down traditional network perimeters, but they don't foretell the death of the perimeter altogether. The perimeter is simply evolving to be less network focused and more data focused. We will talk about the theory and goals of replacing a network perimeter with a data perimeter and what that means for SAAS, cloud, and BYOD implementations. The second half will discuss our companies efforts to create a perimeter, what worked and what didn't. It will highlight techniques that can help create a perimeter with current technology, and areas where we are dependent on

vendors to step up their game and catch-up to the new requirements.
Steve Horstman: Director of Cybersecurity, TPG Capital, @STHorstman

Breakout Sessions: 3:00 pm – 3:45 pm

Securing the 'Weakest Link' - Helping Users Become Part of the Security Team
10/10/2017, 3:00 pm - 3:45 pm, Nautilus 1
Track: Securing the End Users
Abstract: It's well known that humans are the 'weakest link' in the chain, when it comes to security. No matter how strong your security program is, your entire efforts and investment can easily be neutralized by one simple click or a clever social engineer. Building user awareness is a critical component of any complete security program. Recruiting users into an active role in protecting assets - essentially bringing them onto the security team - can magnify your security program beyond what you would otherwise be able to achieve. In this session, we will explore real world cases and examples of security education and awareness programs, along with tips and ideas to help you help your users from becoming... 'The Weakest Link'!
Roy Wilkinson, PhD, CISSP, CPCS, CHS-V, HISP: Principal, CIO/CISO Services, Rausch Advisory Services

Are Zero-Days the Biggest Threat to ERP Systems?
10/10/2017, 3:00 pm - 3:45 pm, Nautilus 2
Track: Application Security
Zero-day vulnerabilities are one every CISO's worst nightmares. Nothing can be more frightening than the lurking threat of an undisclosed vulnerability in your ERP system without a preventative patch available. But, is there a greater threat other than 0-day vulnerabilities facing ERP systems? Based on a real attack that access several SAP Servers around the globe in 2016, we will analyze how this attack was leveraged and how the exploited vulnerability works. It was a zero-day attack? Finally, we will discuss how threats facing business-critical applications such as SAP are rapidly evolving and how malicious outsiders are exploiting vulnerabilities to access these critical systems. During this discussion, we will cover best strategic practices to employ in order to keep up with the latest vulnerabilities impacting your SAP system and applications. It's critical to continually secure business information and processes stored in ERP systems.
Sebastian Bortnik: Head Of Research, Onapsis

Critical Security Issues in SSH & Automated Access
10/10/2017, 3:00 pm - 3:45 pm, Nautilus 3
Track: Infrastructure
SSH is used in every data center for network management, system administration, file transfers, and configuration automation. Many enterprises have accumulated SSH credentials for 20 years, and they have been ignored in most IAM projects. Today, it is common to see tens to hundreds of SSH keys per server - adding up to millions of

keys in the largest enterprises. Often 90% of the keys are unused and 10% grant root access. The unused keys are access that was provisioned but never terminated. SSH keys can be used for stealthy lateral spread from server to server and data center to data center - including backups and disaster recovery. Think APT, think malware, think ransomware, think cyberwarfare - enterprise-wide, with the most critical servers and data. The talk helps understand the problem, how it can be exploited, and gives a roadmap to addressing it. It also looks at compliance requirements related to SSH keys. NIST has published guidelines around the topic (NIST IR 7966) and IDC called it the Gaping Hole in Your IAM Strategy. This year I'm going full disclosure on how to exploit it. It is not a vulnerability or protocol flaw; it is a configuration management, IAM, and process issue. Just like you manage user accounts and passwords, you must manage other access credentials, including SSH keys.

Tatu Ylonen: Founder & SSH Fellow, SSH Communications Security, @tjssh

Introduction to Malware Analysis

10/10/2017, 3:00 pm - 3:45 pm, Nautilus 4

Track: Incident Response

Knowing how to analyze malware has become a critical skill for infosec professionals, especially incident responders. A good way to get started with such efforts involves examining how malicious software behaves in a controlled laboratory environment. In this session, Lenny Zeltser, who's been teaching malware analysis for over a decade, will demonstrate key aspects of this process. He'll walking you through behavioral analysis of a real-world Windows malware specimen by using several free tools. You will see practical techniques in action and understand how malware analysis will help you to triage the incident to assess key capabilities of the malicious software. You will also learn how to determine ways of identifying this malware on systems in your environment by establishing indicators of compromise.

Lenny Zeltser: Senior Instructor / Director of Product Management, SANS Institute / Minerva Labs, @lennyzeltser

ISSA Women in Security SIG Session: Breaking into Cyber Security

10/10/2017, 3:00 pm - 3:45 pm, Spinnaker

Track: Career Development for the Information Security Professional

The WIS SIG panel discussion called Breaking into Cyber Security will include various panel member experiences, challenges, and successes as they entered the cyber security area. The panel will offer insight into how to break into Cyber Security as a Woman and how to provide an impactful presence in cyber security forums. There will be a discussion surrounding the different paths in cybersecurity (business vs. technical) and how to determine which is right for you. This panel will also explore the entrepreneur side of the cyber security industry as women owned businesses and how to navigate that space as well.

Moderator: Jeff Combs: Cyber Security Recruitment Leader, J. Combs Search Advisors, LLC

Panelists: Antonella Commiato: Partner and CISO, DeNovo Perspective

Robin Dudash: President & Owner, Innovative Quality Products & Systems, Inc.

Betty Lambuth: President and Chief Information Officer, Information Technology Solutions & Security, Inc.

Paige Needling: President and CEO, Needling Worldwide, LLC, @needling_world

Break in the Exhibit Hall
10/10/2017, 3:45 pm – 4:15 pm, Pavilion

Cyber Solutions Live Session
10/10/2017, 3:55 pm – 4:15 pm, Pavilion

Breakout Sessions: 4:15 pm – 5:00 pm

Contracts for the Security Professional
10/10/2017, 4:15 pm - 5:00 pm, Spinnaker
Track: Laws and Regulations
Security practitioners are increasingly interacting with legal counsel to assist in the review of contracts, such as master service and data use agreements, as well as provide consultation on security and privacy regulation control requirements, to ensure the organization reduces its risk and liability. The problem? While you know information security governance, you may not be familiar with basic contract concepts that could result in a lack of understanding during negotiations or inadequately identifying risk. This session will provide the information security and privacy practitioner a crash course on basic concepts and wording that you should be aware of, and be able to direct your counsel to review, before executing any contract. This session is geared toward the security practitioner and will focus on good third party hygiene based upon the speaker's experience as part of the contract team.
Tim McCain, CISM, CIPM: Information Security Officer, City of Aurora

Red Teaming: Bring your security testing program to the next level
10/10/2017, 4:15 pm - 5:00 pm, Nautilus 1
Track: Career Development for the Information Security Professional
The term Red Team or Red Teaming has become more prevalent in the security industry. Both commercial and government organizations conduct "Red Team Exercises". What does this mean? What is a Red Team engagement? How is it different that other security tests? Isn't current penetration and vulnerability security testing enough? Red Teaming shares many of the fundamentals of other security testing types, yet focuses on specific scenarios and goals that are used to evaluate and measure an organization's overall security defense posture. Organizations spend a great deal of time and money on the security of their systems. Red Teams have a unique goal of testing an organization's ability to detect, respond to, and recover from an attack. When properly conducted, Red Team activities significantly improve an organization's security controls, help hone defensive capabilities, and measure the effectiveness of security operations. This presentation examines the role of a Red Teaming; the differences between other security testing types, and how scenario based engagements can provide

a view of not only technical defenses, but the entire defensive posture of an organization.
Joe Vest: Director, MINIS, @joevest

Shields Up For WordPress Websites and Blogs
10/10/2017, 4:15 pm - 5:00 pm, Nautilus 2
Track: Application Security
In this presentation you will learn why WordPress sites are an attractive target for cyber-criminals and attackers, why they want to hijack your site, and how to harden your WordPress site to keep your site safe. We will discuss the merits of different security plugins, as well as cover WordPress best practices for security. Technologies included are WordPress plugins WordFence, Bulletproof Security, and Sucuri, as well as two-factor plugin Mini-Orange. We will be examining the value of a Web Application Firewall. There will also be some advance techniques that involve making changes to the WordPress installation code itself.
Bob Weiss, CISSP, CEH: Senior Cybersecurity Engineer, Computer Integration Technologies, Inc., @wyzguys

Make Access Control Great Again! (and what it means anyway)
10/10/2017, 4:15 pm - 5:00 pm, Nautilus 3
Track: Infrastructure
Access control means many things to many people. The least common denominator is user logins and roles. However, there is a lot (!) more to access control than that. Unfortunately access control is among the most ill-understood, least developed (source: NIST) aspects of cybersecurity. At the same time controlling access to IT resources it is the core underpinning of cybersecurity. Over the years both scientists and marketeers came up with a myriad of concepts, acronyms and terms to describe different kinds of aspects of access control. Acronyms incl. MAC vs DAC, IBAC/AuthNBAC, RBAC, ABAC, PBAC, ZBAC/AuthZBAC, NAC/AppAC/OSAC/VMAC, HistBAC, NGAC, RAdAC, HBAC, CBAC, GraphBAC, BPMBAC, and many more. In addition, terms such as entitlement management, authorization management, micro segmentation, nano segmentation, VLANs, isolation, separation, adaptive/dynamic authorization etc. are used by vendors to describe their products. On top of that, vendors talk about security automation/orchestration, security policy automation. Because this terminology soup keeps changing, it leaves security professionals mostly confused. This presentation will cut through the fog and provide clarity about the reasons/benefits/challenges of the various access control concepts. It will peel off the â€œmarketing layerâ€ and categorize concepts according to pertinent characteristics such as granularity, assurance/verifiability, adoption, enforceability, manageability etc. The audience will learn that once the acronyms and terms are peeled off, there are numerous underlying concepts that are critically important for security professionals to protect their organizations (incl. IIoT/IoE). Dr. Lang has been working on access control for 20 years and is excited to share his experiences.
Ulrich Lang: CEO, CEO, ObjectSecurity, @objectsecurity

An Evolving Adversary: Building a Threat-Based Cyber Team
10/10/2017, 4:15 pm - 5:00 pm, Nautilus 4
Track: Incident Response
In the last few years we have noticed an evolution of adversary's tactics, techniques and procedures that have become increasingly more challenging to detect, given current culture and defensive methodologies. We have had to take a close and critical look at our Defensive Cyber Operations and determine whether we had adequate defenses to detect these adversaries. What we found was not only technical deficiencies, but philosophical misalignments that were embedded in our cyber culture. I will start by outlining a case study we did on a specific actor sets malware and how the malware capabilities evolved over a short period of time. By coincidence, we were asked by a peer organization to assist in an incident response involving this same adversary. We will highlight how the adversary leveraged Windows WMI for persistence and lateral movement. This was a change from using the registry for persistence and RDP for lateral movement and is much more difficult to detect. To understand our defensive posture I will also highlight the current state of Defensive Cyber Operations at the time of the incident, which was more of a ground up approach. We had the usual suspects in Security Operations: IPS, Sandbox, Forensics, Anti-Virus, Blackhole, Application Whitelisting, but was this sufficient for the aforementioned adversary? Simply, no! Our Cyber Threat Team construct and Defensive Cyber Operations Conops was developed and implemented at JHUAPL. The Cyber Threat Team was broken into 4 major areas: Research, Adaptive Red Team, DevOps, and Analytics. The Threat Team targeted more advanced adversaries and had a different philosophical approach than what we traditionally had in Information Security. We weren't trying to detect malicious hashes or nefarious IP addresses, we were looking at the activities a more advanced adversary would be doing in our environment. Ultimately, a lot of this came down to increased visibility and maturation of advanced use cases. The change in philosophy wasn't easy and not everyone accepted it or could excel in it. I needed to identify existing talent in Security Operations, but what was I looking for agility, innovation, and out-of-the-box thinkers!
Anthony Talamantes: Manager, Defensive Cyber Operations, JHUAPL
Todd Kight: Lead Analyst, Defensive Cyber Operations, JHUAPL

Party on the Flight Deck
10/10/2017, 6:30 pm – 8:30 pm, USS Midway
Join us for a reception aboard the USSA Midway! Bus transportation will pick up in the front of the Sheraton Hotel and Marina beginning at 6:00 pm and return transportation to the hotel will be available from the reception.

Sponsored by:

Wednesday, October 11, 2017

International Conference Registration Open
10/11/2017, 8:30 am – 2:00 pm, Bayview Foyer

Exhibitor Networking Breakfast and Keynote Address
10/11/2017, 8:30 am – 10:00 am, Grande B/C

Exhibit Hall Open
10/11/2017, 10:00 am – 2:00 pm, Pavilion

Break in the Exhibit Hall
10/11/2017, 10:00 am – 10:30 am, Pavilion

Cyber Solutions Live Session
10/11/2017, 10:10 am – 10:30 am, Pavilion

Breakout Sessions: 10:30 am – 11:15 am

Smart City: The Value, Security Risks, and Challenges in Transportation
10/11/2017, 10:30 am - 11:15 am, Spinnaker
Track: Infrastructure
A Smart City environment offers metropolitan areas an essential way to grow and move its people, both logically and physically. The advancement of technology offers urban areas many opportunities to leverage its infrastructure, including communications networks, and other means of transportation for its communities. However, to establish an effective means of supporting and expanding its urban transportation needs, security risk management has to be a focal point when addressing the physical and logical landscape upon which smart city exists.
Angela Jackson-Summers: Director of Information Technology Audit, Metropolitan Atlanta Rapid Transit Authority,
Ndidi Osemene, CISA: Metropolitan Atlanta Rapid Transit Authority
Donald McCall, CPA, CISA: Metropolitan Atlanta Rapid Transit Authority

262 Days Later: A Review of President Trump's Cybersecurity Policies
10/11/2017, 10:30 am - 11:15 am, Nautilus 1
Track: Laws and Regulations
Come join us for an in depth discussion about cybersecurity policy under the Trump Administration. We will review the policies in the U.S. for both the private and public sectors, international policy, Department of Defense policy and changes with the NSA, information sharing, and major changes from the prior administration and the present one relating to cybersecurity. Specifically, attendees will hear about the impact of the President's Executive Order on Cybersecurity, changes in lead agencies in the U.S. that differ from the prior PPD-41/National Cyber Incident Response Policy of DHS, expanded roles for the DOJ, DOD, and DHS, and potential impacts to our foreign partners. Who is in charge when a large breach hits the public or private sectors? What role will this White House play in these incidents? We will examine data breaches on the national stage and how the administration covered and responded to those breaches. In addition, we will review the public sector changes in the White House (with or without the CISO at OMB) and how this has shaped the U.S. policy on a national and global stage. This will be a non-partisan factual look at those policies that are in place, being put in place, or coming soon to provide attendees with a full picture of cybersecurity policy at the top of the house in the U.S.
Dr. Christopher Pierson: Chief Security Officer & General Counsel, Viewpost, @DrChrisPierson
James T. Shreve: Attorney, BuckleySandler, LLP

Web Application Testing - approach and cheating to win
10/11/2017, 10:30 am - 11:15 am, Nautilus 2
Track: Application Security
As security professionals, we are often called upon to assess the security of web delivered applications and/or services. Not all of us have either experience or a methodology for responding to this type of assessment request. Web based applications and services are the key technologies behind modern service delivery. And their security, or lack thereof, can make or break a company. We will lay out an approach to follow including tools to help with the assessment throughout each step of the process. We will discuss free and commercial products that can assist the assessment process. The user will leave with information they can take back to their home organization to serve as a foundation for either an ad-hoc or ongoing capability. Prepared by LLNL under Contract DE-AC52-07NA27344. LLNL-ABS-720000
Lee Neely: Senior Cyber Analyst, Lawrence Livermore National Laboratory, @lelandneely
Chelle Clemenets: Web Mistress
Jim Mc Murry: CEO and Founder, Milton Security Group

ISSA Security Education and Awareness SIG Session: Grave Danger! Is there any other type of Danger?
10/11/2017, 10:30 am - 11:15 am, Nautilus 3
Track: Career Development for the Information Security Professional
As flying in the Danger Zone, using proper skills to protect others, sound ethical behavior and judgment when developing training materials will provide better material for Security Awareness and Training, including for you and your company. By following these guidelines your Security Awareness Program will assist in reducing the risk

of cyber attacks, e.g. Phishing, Ransomware, etc.
Kelley Archer: Distinguished Fellow, CISSR, Cantel Medical

"Watson, come here! I need you."- Artificial Intelligence in Cyberscecurity
10/11/2017, 10:30 am - 11:15 am, Nautilus 4
Track: Incident Response
Limited Artificial Intelligence is permeating many aspects of our lives - from financial advice to medical research - even physics and mathematics. Cyber attacks can occur at wire speed, and even the best humans with the best tools may not be able to respond quickly enough. Deep machine learning, neural networks, and other capabilities are coming out of research laboratories and entering commerce (think of IBM's Watson being used and advertised by H&R Block to help the average person complete their tax returns). Although machine systems find it difficult to function effectively in the physical world, the digital world is their native ecology, where humans are slow, clumsy, and at a disadvantage. This strategic-level session will look at the current state of AI, how near-future AI may be integrated into cybersecurity, and some of the issues involved. These issues include: possible impacts to human cybersecurity practitioners, the risks and benefits of autonomous responses to cyber attacks, and machine ethical concerns. In some ways, these reflect the issues we are looking at with respect to fully autonomous vehicles and weapons systems, but with different risks, dangers, and potential benefits.
Frank Gearhart: System Analyst, COLSA Corp., @fgearhart

Break and Book Signing in the Exhibit Hall
10/11/2017, 11:15 am – 11:45 am, Pavilion

Awards Luncheon
10/11/2017, 11:45 am – 1:15 pm, Grande B/C

Breakout Sessions: 1:15 pm – 2:00 pm

The Approaching Age of Autonomous Computing
10/11/2017, 1:15 pm - 2:00 pm, Nautilus 1
Track: Career Development for the Information Security Professional
Are you sick of hearing about AI, ML, robots, big data, and automation? Too bad! Not only are they here to stay - they're going to continue growing, maturing, and spreading. The future is autonomous computing where data centers operate themselves, computers write their own code, and humans merely oversee and benefit from these advancements. If you thought the world has changed a lot in the past 15-20 years, just wait until you hear what's

next (and how we can secure it)!
Ben Tomhave: @falconsview

Federation: More than Just Security; Challenges with Disparate Policy Integration
10/11/2017, 1:15 pm - 2:00 pm, Nautilus 2
Track: Application Security
The lures of the potentials of cloud computing are growing as more cloud providers offer secured cloud solutions. As companies continue to create and advertise more PaaS and IaaS offerings, the need for integrated authorization and authentication systems will also grow. This is not just a cloud issue. More companies are integrating business solutions with partner organizations. Do we require users to have dual logon IDs or is there another solution. Federation promises to be the solution to integrate identity needs between disparate systems and user groups. But does federation really address to needs of the partner organizations? Is it just an identity management tool or can it deliver more? What happens when contractual provisions of the federated services are in conflict with existing organizational constraints and policies? What are some of the challenges that currently exist with federation as relates not only to technical implementation but also relates to business concerns? In this breakout session we will explore issues surrounding federation implementation and identities -- both organizational and technical. We will also discuss the policy issues that any organization should be aware of as relates to cloud services or shared identity services between organizations.
Jill Feagans: Privacy and Security Manager, Optum

Information Security and eDiscovery: It's not just Forensics.
10/11/2017, 1:15 pm - 2:00 pm, Nautilus 3
Track: Infrastructure
Law firms and in-house corporate legal departments, with their respective systems and data, are rapidly becoming prime targets of costly security breaches by cyber criminals (hacks and/or leaks). So how do we protect ourselves? As the corporate Electronic Discovery (eDiscovery) process evolves and matures so must the integration of information security controls. eDiscovery, historically interpreted by some to only involve the information security discipline of forensically collecting data, involves numerous other security disciplines and functions. The development, deployment, and operations of an eDiscovery platform must be deployed to not only achieve compliance, but also risk reduction. This presentation will provide a brief introduction of eDiscovery, Information Security, and the relationship between these two critical functions. The presentation will also show risks and controls that apply to each of segment of the eDiscovery Reference Model (EDRM) or workflow. Specifically, 1.\tWhat to protect 2.\tWhere to protect. 3.\tHow to protect. 4.\tWhen to protect. The presentation will also provide risk reduction recommendations for organizations that outsource their requirements to Third Party providers. Case study examples will also be provided.
Henry Moreno: Principal - Information Security, Global M Group

Cyber Resilience: the what & why
10/11/2017, 1:15 pm - 2:00 pm, Nautilus 4
Track: Incident Response
With the increase in breaches and other security incidents, a new concept is come to the fore: â€œcyber resilienceâ€. Some tout is as the next step in cyber security. What is it, and why should the information security professional care? Cyber resilience goes beyond just focusing on preventing and then responding to incidents, but looks at how organizations can recovery from the impact of incidents by working to make systems more resilient to those impacts. We will look at several models for cyber resilience: CERT-RMM, CERT's CRR, McKinsey's Cyber Resilience Levels, AIG's Cyber Resilience Steps, and Axelos Resilia. We will also look at some of the organizations working on cyber resilience such as Global Forum to Advance Cyber Resilience., GICSR- Global Institute for Cybersecurity + Research, Cyber resilience Institute (CRI), and the Forum on Cyber Resilience (National Academies of Sci, Eng, Med), CERT (thru their Cyber Risk and Resilience management area) and the World Economics Forum.
Michael Brown: Manager, 24by7Security, Inc, @emb021

Break in the Exhibit Hall
10/11/2017, 2:00 pm – 2:30 pm, Pavilion

Cyber Solutions Live Session
10/11/2017, 2:10 pm – 2:30 pm, Pavilion

Breakout Sessions: 2:30 pm – 3:15 pm

Applying Common Business Metrics to Information Risk Reporting
10/11/2017, 2:30 pm - 3:15 pm, Nautilus 1
Track: Business Skills for the Information Security Professional
There's an old axiom: "What gets measured gets done." So how have you been demonstrating to management and governance that your cybersecurity program is performing? In this presentation, we "re-center" risk management and cybersecurity around the business of doing business, setting aside technology for just a moment. Learn how your organization's existing business tools and methodologies - the ones that other business functions are probably already using for their own processes can help you to start demonstrating productivity, responsiveness, and return on investment. Real-world examples and samples of tools and metrics you can apply immediately will be provided.
Daniel Ziesmer: President and CRO, Centripetum, LLC

Cybersecurity of Interbank Messaging and Wholesale Payment Networks
10/11/2017, 2:30 pm - 3:15 pm, Nautilus 2
Track: Application Security
This session will focus on measures that financial institutions and financial market infrastructures (FMIs) can take

to protect against cybersecurity threats to the payments ecosystem. The FFIEC warns and recent attacks on SWIFT messaging systems (Bangladesh central bank, commercial bank in Vietnam, and over a dozen more) illustrate that sophisticated hackers are successfully initiating and completing unauthorized transactions using interbank networks and wholesale payment systems.

Joseph Salazar: Technical Marketing Professional, Attivo Networks

Ins and Outs of Blockchain for Security

10/11/2017, 2:30 pm - 3:15 pm, Nautilus 3

Track: Infrastructure

Blockchain technology is being touted as the Next BigThing, seemingly capable of great feats of strength and perhaps even curing the common cold. But what exactly is it and how could it contribute to a security program? This session will describe how blockchain works, define its value proposition, and identify specific use cases where blockchain makes sense and some where it doesn't. Along the way, we will discuss similar capabilities and technologies that accomplish the objectives.

Pete Lindstrom: VP, Security Strategies, IDC

Threat Injection: Leveraging the MITRE ATT&CK Framework to Improve Detection

10/11/2017, 2:30 pm - 3:15 pm, Nautilus 4

Track: Incident Response

The asymmetric nature of the current threat landscape presents significant challenges for defenders and the organizations they work diligently to protect. Attackers have a seemingly endless arsenal of tools and techniques at their disposal, while defenders commonly find themselves buried under waves of alerts from a multitude of platforms that may or may not detect the adversary. To protect and enable the business, leadership must have an accurate picture of risk so they can deploy resources in a manner that fits the organization's threat model. As information security professionals, we need to improve our ability to detect threats in our environment. One proven approach to increasing the detection capabilities involves executing "Threat Injections." We'll define Threat Injections as specific attacks performed by internal or external red teams, in this case based on the MITRE ATT&CK Framework's technique matrix. Techniques focus on later-stage attack activities such as Lateral Movement, Execution, Exfiltration, and Command & Control. Rather than a "red team vs. blue team" mentality, this approach involves a structured, planned collaboration designed to validate current threat detection capabilities and identify visibility gaps. This presentation will include a demonstration of how to plan and execute a threat injection in a simulated victim network. The audience will observe the simulated attack, the defensive detection and response (or lack of response), analysis of the results, remediation and tuning actions, and finally the metrics and reporting view that is provided to leadership.

Brian Genz: Threat Hunting Analyst, Fortune 500 Financial / Insurance Company, @briangenz

ISSA Financial SIG Session: Governing without Clear Standards: Lessons Learned from the Trenches
10/11/2017, 2:30 pm - 3:15 pm, Spinnaker
Track: Career Development for the Information Security Professional
Learn from practical experience how to develop a defensible program where new and existing regularities schemes provide little guidance. The main premise is that true "standards" are not being provided. Instead, these sources provide some guidance, but primarily demonstrate the importance of having a sound process for continually monitoring and improving information security. The presentation will then turn to how regulators and tribunals have been relying on these "standards" if at all. The presentation will focus on sound governance principles and discuss what is required to build a defensible program. How to successfully collaborate among business, technologists, CISOs, CPOs, and attorneys will be discussed as well as developing and maintaining a defensible program. From real world examples, we will discuss how to develop a program which will stand up under scrutiny and what common pitfalls to avoid.
Ronald Raether: Partner, Troutman Sanders LLP

Breakout Sessions: 3:30 pm – 4:15 pm

Be My Wingman Any Day- Why Legal and the ISO need to fly together!
10/11/2017, 3:30 pm - 4:15 pm, Spinnaker
Track: Laws and Regulations
Increasingly, data security and privacy are falling under the purview of laws and regulations. Whether it is a state's department of financial services promulgating new cyber-security regulations, federal laws aimed at protecting health information, or a contract for an engagement with a SaaS vendor, news laws and regulations are now also driving information security and privacy practices. Just as information security has never been just an IT concern; laws and regulations are not just a legal concern. It is becoming necessary for information security professionals to be familiar with the legal implication of their work. Information security professionals have to work with their legal counterparts to navigate these new challenges presented by laws and regulations.
Sid Bose: Attorney, Ice Miller LLP
Nick Merker: Attorney, Ice Miller LLP

Closing the Gap: Forging Pathways to a Cybersecurity Career
10/11/2017, 3:30 pm - 4:15 pm, Nautilus 1
Track: Career Development for the Information Security Professional
Building a skilled and agile cyber workforce can be a daunting challenge. The DHS NCTEP program offers several cyber education and training resources to help address the exponentially growing need for a knowledgeable and skilled cybersecurity workforce. They are foundationally rooted to the DHS co-developed, National Cybersecurity Workforce Framework - a blueprint to describe, categorize and organize cybersecurity work into Specialty Areas, tasks, knowledge, skills, and abilities. It provides a common language to describe cybersecurity across the public

and private sectors, and academia. With this serving as the backbone to all DHS resources, all stakeholders can have a consistent nationwide understanding of cybersecurity work. In support of cybersecurity professionals, other DHS resources include a Workforce Framework-aligned catalog tool to locate available cybersecurity courses across the country; a free online cybersecurity training environment for all federal, state, and local government employees and veterans; and taking cybersecurity classes at a DHS-NSA designated top school to earn a degree. Join this session to learn how you can use these resources to build (and keep) your cybersecurity team.
Noel Kyle: Program Lead for Cybersecurity Education and Awareness, DHS

Shining a Light on the Dark Web
10/11/2017, 3:30 pm - 4:15 pm, Nautilus 2
Track: Securing the End Users
The Dark Web has made it to mainstream in fictional TV shows like CSI Cyber and NCIS. But, the Dark Web is far from fiction. Powered by virtual currencies and the barter system, the Dark Web can enable a criminal to conduct anonymous business, and all at your expense. Most of the items available on the Dark Web consist of information. Credit cards, personal information and even ways to target individuals and companies are readily available. While the Internet breaks down borders and makes the planet a smaller place, it also enables criminals to reach victims while relaxing on the couch, often on the other side of the world. In some countries, the activity may not even be illegal and criminals enjoy little risk of getting caught or facing the consequences. The Dark Web presents challenges for the investigator, but the first step is understanding what can be found. Only then can we shed light on how to access the information.
Cary Moore, CISSP, CFE: Associate Partner, IBM Red Cell Team

SIEM Regrets? Get the Most Out of Your Investment
10/11/2017, 3:30 pm - 4:15 pm, Nautilus 3
Track: Infrastructure
This session will provide real-world experience and tangible information on actions you can take when your SIEM solution fails to provide the level of visibility needed to respond to network threats. SIEM vendors have sold thousands of tools to organizations over the past few years and most of these implementations are not deemed successful by the CIO. So, what are some companies doing differently to make them more successful than others? We will cover the top three reasons a SIEM project fails to meet expectations: 1.\tLack of people 2.\tLack of process 3.\tAppropriate use cases. Brad Taylor, CEO of managed security service provider Proficio, will describe how to fix these issues. He will also review the metrics you should expect from a SIEM solution, and how to measure successful SIEM operations. He will also review new SIEM concepts and how to utilize them, including: machine learning, user and entity behavior analytics, threat intelligence, threat hunting, and orchestrated incident response.
Brad: Taylor, Proficio, @BradleyHTaylor

Hunting-as-a-Service: What It Is and Why You Need It

10/11/2017, 3:30 pm - 4:15 pm, Nautilus 4

Track: Incident Response

Because the security industry has the attention of the connected world right now, there is a great deal of posturing among solutions providers who lay claims to the latest and greatest technologies to ensure security. They create buzz through a mix of overstated guarantees and outright fear, uncertainty, and doubt. Despite the uncertainty, there is a recognizable shift pertaining to new processes and technologies that stand out. Monitoring incoming traffic on the network via next-gen firewalls and appliances, as well as endpoint agents that go deeper into client systems, have made a case for moving completely away from signature-based and stand-alone-technology protection. There's a risk void that hunting-as-a-service seeks to fill, by providing more focused detection capabilities and response protocol for anomalous and dangerous system activity. Join security expert Ron Pelletier as he explores the evolution of threat detection and hunting services, with special emphasis on the added value of human intelligence in a technology-driven discipline.

Ron Pelletier: Co-Founder, Partner, Pondurance