Speaker Name	Title	Title/Synopsis	Track	Time
Marcus Carey	"If you click this link, I will kill you!"	Information warfare used to be reserved for the government — it was prohibitively expensive. But now, it's easy to do with a little code, APIs, and the cloud. There are several APIs that are intended for web developers (traditionally for advertisements) that can be leveraged to track people down to their exact geolocation. Additionally, free web platforms allow attackers to quickly deploy malicious web content and vanish without a trace. This talk will provide tips for carrying out information warfare on a budget in order to help the audience understand the techniques, tactics, and procedures attackers often use. It will also give the audience a better understanding of how they can protect their own identities online.	All Conference	9:00 AM
Andy Thompson - Cyberark	"Addressing Insider Threat"	This talk discusses corporate espionage, sabotage, and insider threat in todays IT landscape. This talk discusses what technical controls apply to addressing insider threat and how others simply don't work. Topics will include: DLP, Account Deactivation, Separation of Duties, Least Privilege/Application Control, Encryption, SLDC/Change Control Backup & Recovery, Credential Management, and Behavioral Analytics	All Conference	10:00 AM
Dr Jerald Dawkins	"From the Basement to the Boardroom – How Information Security Has Changed Over the Last Ten Years and Where It Is Going"	To understand where we are going, you must understand where we have been. Information security has been a roller coaster ride over the past decade. During this talk, Dr. Dawkins will present his experience on how technology, compliance, and security has changed across multiple industries. He will provide an interesting, retrospective analysis to better equip our InfoSec community for the future – a future where information security has broader visibility and impact not only in technology but in the boardroom.	All Conference	11:00 AM
Ian Anderson / Jason Nations	"Social Engineering a SCADA Security Program".	The premise of the presentation is… What are some tips and tricks that security teams can deploy to reduce the friction of standing up or maintaining a SCADA security program.	Conference Center A	1:00 PM
Donovan Farrow	"Hacking the Humans"	Every day we hear about the latest virus attacks, DDoS, or malware outbreaks. What about the human? Do we not play a huge role in these types of data attacks? Hackers today are easily subverting humans with common techniques.	Conference Center A	3:00 PM

Bob Simpson	"Old Tools to Fight New Enemies"	A decade ago, Kris Lamb, a security leader at IBM stated “The network boundaries are dissolving”, and TechRepublic published an article stating, “Perimeter security simply doesn’t cut it anymore.” Ten years later, those words have never been truer. Attack mechanisms are spread across more devices than ever, and can hop from one platform to another, and enter our network in new ways every day. Luckily, through the concept of cyber hygiene, we are finally making sense of how to cope in this new world. This talk will discuss techniques that have been around for years, but are particularly effective against todays threats. For example, Private VLANs for preventing an intruder from pivoting inside your network. Also, easy file permissions that can stop ransomware in its tracks, or router filters that will black hole your enemies and stop C&C from taking charge. Putting all these decade-old tools to use can help us defeat malware that hasn’t even been invented yet. A. Shifting Mindset a. Ubiquitous Attack Mechanisms b. Cyber Hygiene is Absolutely Required c. Nothing is Perfect d. Prepare for the Worst B. Attacks Happen a. Where is Your Perimeter b. Where is Your DMZ c. The New Defense in Depth C. Real Life Defense	Conference Center A	2:00 PM
Craig Buchanan	"Video Surveillance in the modern age"	Ten years ago IP cameras were just being introduced in the surveillance space. Many organizations were still using VHS tape as a recording medium. This presentation will look at the evolution of cameras and storage technologies. We will discuss the power of digital cameras and the ability to store recordings. We will discuss the benefits and consequences of upgrades with a sober look at the economic and security consequences. We will wrap up with a glimpse of what the near future (months) hold in the area of surveillance.	Conference Center B	12:30

Gordon Rudd	"CISO Skill Set: The Tools and Techniques You Need to Succeed"	The purpose of this session is stretching the average life expectancy of the CISO beyond 2.1 years. Today's CISO is a hybrid: part technician; part manager; part leader; and part visionary. This session will focus on the concrete skills those who believe they are CISO material will need to master. If you are a CISO, this session will give you tools to help you do your job better/cheaper/faster than the competition. We'll focus on: assessing the information security department's operational readiness; skill sets; people, processes and technology; and communicating with upper management and your board. We'll also take a hard look at what to do when things don't go as planned. Join us and learn to thrive, not just survive, as a CISO. NOTE: In-conference workshops this year have limited seating and require preregistration. Learning Objectives: * Assess an information security department, the people in it and the organization it serves. Develop organization specific tools to accurately determine the capabilities and operational readiness of the department. Develop organization specific tools to accurately determine the capabilities and operational readiness of the department. * Plan the work and work the plan. Create strategic and tactical plans that work for their information security department; measure the information security departments progress toward the objectives/milestones detailed in the plan; differentiate between processes, projects, programs and reality; and move from analysis paralysis to action. Create the people, processes and technology roadmap for the information security department. * Demonstrate why the programs, processes and projects in place will keep the organization as secure as possible in the world we live in today. Move beyond guessing and get down to reality; parse the mountains of information coming in and create threat intelligence that is actionable	Conference Center B	1:00 PM

Paolo Dal Checco	"Bitcoin"	BITCOIN FORENSICS AND INTELLIGENCE Bitcoin is the most popular cryptocurrency, employed by people and companies all over the world, slipping through highs and lows, freedom and obstruction. As with every technology, there's a dark side, which in this case is represented by dark markets, anonymous transactions and wallets used by criminals to carry on illicit activities and launder money. The speech will introduce the audience to the problems concerning Bitcoin pseudo-anonymity and illustrate some practical methods for investigating bitcoin addresses and transactions. By joining OSINT, bitcoin forensics and bitcoin intelligence methods and techniques, researchers will sometimes be able to identify wallets and track money. In some cases, with the help of advanced tools and techniques, there are chances to identify the owner of addresses or the place where transactions were issued and even de-anonymise mixer transactions or jumps between different cryptocurrencies. OSINT TECHNIQUES TO DETECT AND PREVENT BUSINESS EMAIL COMPROMISE ATTACKS Also known as BEC Scam, CEO Fraud or Man in The Mail, this kind of attack can take a variety of forms. In just about every case, the scammers target employees with access to company finances and trick them into making wire transfers to bank accounts thought to belong to trusted partners, while actually the money ends up in accounts controlled by the criminals. A common scheme involves the criminal group gaining access to a company's network through a spear-phishing attack and the use of malware, which leaves traces in many forms and places. By analysing open source data with OSINT techniques, its sometimes possible to detect ongoing BEC attacks and warn (future) victims about the risk they are running. The challenging part is explaining victims what is happening in the early stage of scam when they still don't realize their role in the fraud scheme.	Conference Center B	2:00 PM

Ed Eckenstein	"How to Reignite Your Professional Passion, When Work is Sucking the Joy out of Your Life…"	Somewhere deep down you're passionate about what you do. That passion used to be central to not just your career path but to your LIFE. Your work was important to you. Your work defined you. And your work was something you were excited to dig into every single day. Until you weren't. At some point along the way, the stress, anxiety, and constant hurdles of your day-to-day made it a lot harder to love what you do. Instead of pouring your passion into your latest project, your time and talent is being sucked into an endless black hole -- a black hole defined by… ● Constant late night and weekend troubleshooting sessions, that are never on the calendar ● The latest "code red" project that's dumped on your desk -- right on top of the other urgent to-dos… ● A total lack of management support ● Colleagues who make MORE work for you ● Organizational politics that define who gets what and who does what day in and day out ● A constant lack of recognition for your work -- the work you're producing at all costs, even though you're hanging on by a thread You could look for another job, but who's to say these challenges won't be waiting for you there? Besides, that's going to take more time -- time you don't have. While you're working through your options, the stress of your workday keeps closing in on you -- it's the insomnia, the weight gain, the depression, the high blood pressure… Overcoming the Challenges, No Matter How Big Sound familiar? You're not alone. This has, increasingly, become the reality for many tech insiders, innovators and entrepreneurs -- but it doesn't have to be this way. ● What if you could learn to be happier in your job right now -- happy like you USED TO BE. ● What if you could handle challenges with less stress -- and be more resilient to stress when it does happen? ● What if you could learn a better way to react to the ups and downs of this industry, so you could work anywhere, anytime and handle whatever is thrown your way.	Conference Center B	4:00 PM
Danny J. Slusarchuk	"HIPAA Security top 10 for small healthcare"	Most people don't know where to start so they just bury their head in the sand. That's why we have insurance they say. Would you send your Grandma to a clinic if you even remotely thought her "protected health information" would be compromised? This talk is a day one, start here for you to begin the journey that is part of providing positive patient outcomes. A sprinkling of fail stories too.	Conference Center C	12:30 PM
Optiv	"Day in the life of a Pentester"	Optiv returns this year with their ever popular discussion panel. This year panels looks at what goes into a successful pentester career. Careful consideration is given to specific skils for the individual as well as needed team integration requirements.	Conference Center C	1:00 PM
Ed Eckenstein	"The Career Success Maze: Breaching the Walls		Conference Center C	2:00 PM

NCC Group	"The Evolution of Industrial Networks and the Convergence of OT and IT"	During this panel, industry veterans will discuss how managing and protecting Process Control Networks has evolved in the past couple of decades. The delineation between what belonged to OT and what belonged to IT was once clear. That line continues to blur as Industrial networks interface with business networks more and more often. The panelists come from a variety of technical backgrounds and will offer a diverse view on the challenges and potential solutions related to InfoSec in ICS. Specific topics include: · How are Industrial network designs changing? What is the new state-of-the-art? · How does the Industrial Internet of Things factor into these design decisions? · What is the valuation of Certifications in the Control System and IoT field? · How do organizations handle vulnerability management in L3 networks? · What standards are useful to adopt considering limited regulation and how will this drive the desire to be "compliant" versus the need to be "secure?" The target audience includes those that are responsible for managing or securing ICS networks, or those that do so on behalf of their clients. The panelists' goal is to provide attendees insight into emerging trends in InfoSec and to enable them to more effectively protect their organizations	Conference Center C	3:00 PM
Sean Satterlee	"The last 12 months…"		Conference Center C	4:00 PM
Cory Sutliff	"Leveraging Artificial Intelligence/Machine Learning to Stop Malware and CyberCriminals"	Artificial Intelligence (AI) and Machine Learning (ML) capabilities are rapidly changing the world of computing, from self-driving cars and IBM Watson playing Chess to supporting mission-critical applications. In this informative review of AI, Cylance Security Engineer Cory Sutliff will trace the rapid evolution of AI, identify sectors of early adoption, and its recent application to cybersecurity. He will review how and why the velocity of AI evolution is accelerating in recent years, plus provide valuable insights and case studies of AI in cybersecurity stopping malware attacks.	Room 109 / 110	12:30 PM
Chris Yates	"Tough passwords? We don't need no stinking tough passwords!"	Everyone knows by now that the guidance we've been giving for years is that passwords should be complex, long, and should be changed frequently. The National Institute of Standards (NIST) is the organization that publishes guidance for password complexity, which is the basis for not only best practices guidance used worldwide, but has been incorporated into compliance frameworks that many organizations are legally required to comply with. However, recent studies on how people comply with ever increasing password complexity requirements reveals that instead of increasing the security of passwords, people make password choices that decrease their security, even though their passwords are in compliance with the password guidelines and standard practices. Based on this information, NIST has published new guidance on the complexity of passwords that significantly changes the standards for password complexity. This presentation will discuss password policy evolution, and provide some context for the new guidance from NIST.	Room 111	12:30 PM

Trent Greenwood	"Your organization is a crime scene"	Your perimeter has moved and is no longer where it has traditionally been. This leads to breaches because it is a weak point in your organization. When you have a breach, your organization is now a crime scene. So understanding the consequences, having a strategy and implementing the right tools will all help with your crime scene. In this talk we will discuss what the consequences of a breach have to your organization. We will touch on how your perimeter as you know it has changed and where it now is and what is your strategy. Lastly what you should consider in implementing tools to help.	Room 109 / 110	1:30 PM
Geoff Wilson	"There Will Be Breaches: How to Equip Our Organizations for the Decade Ahead"	In this talk we will review some notable and some lesser known information security breaches from the last 10 years. By understanding root causes and underlying security control failures, we can distill the lessons learned to create more breach-resilient organizations. We don't know what the next 10 years will hold, but one thing is for sure: There Will Be Breaches. The best time to prepare for an incident is before it occurs. Let's invest some time today to enhance our preparedness and planning.	Room 109 / 110	2:00 PM
Pedro A. Serrano	"Your first and last line of defense"	The Description: A quick look at the most important security issues that every company should be educating their users today 1. You are the Target a. Stop, Look, Think b. How much data are you sharing? 2. Social Media a. Time to check your settings 3. Protect you PC a. Pedro's 5 rules for home PC 4. Your Digital ID	Room 109 / 110	3:00 PM
John Spaid	"Save Your Sole: Network Footprinting and Hardening with Shodan, Kali, Nexpose, and more!"	In the age of the APT, insider threat is all the rage. But while many organizations spend their security budgets on advanced tools they'll never fully utilize, they neglect basic security principals, such as, "don't allow SMB traffic to/from the Internet," or, "use TLS on login pages." It takes a major incident to draw attention back to these issues, and when questions start pouring in from management, none of your fancy widgets can answer any of them. In this talk, I will explain the application of some free and free-ish tools you can use to profile your public network footprint and walk you through the process of doing network reconnaissance the same way an external attacker would.	Room 111	1:00 PM

Brett Edgar	"A Pragmatic Approach to People-Centric Security"	PEOPLE-CENTRIC SECURITY (PCS) WHAT IT IS… (Definition: People-Centric Security) • The premise of PCS is that employees have certain rights. However, these are linked to specific responsibilities. • This compact of rights and responsibilities creates a collective codependency among employees, exploiting existing social capital within the enterprise. • PCS principles presume an emphasis on detective and reactive controls, and transparent preventative controls, over the use of intrusive preventative controls. • PCS favors the maximization of a trust space within which individual autonomy and initiative is encouraged. • PCS presupposes an open, trust-based corporate culture, and associated executive awareness and support. • PCS principles presume that individuals have the appropriate knowledge to understand their rights, responsibilities and associated decisions.	Conference Center A	12:30 PM
Nathan Sweaney			Conference Center B	3:00 PM