8:30 – 9:00 am  Registration / Check-in

9:00 – 9:10 am  Opening Remarks

9:10 – 10:00 am  Morning Keynote Speaker
                   Kip Peters - Leadership Partner for Security & Risk Management, Gartner

Ethics in IT

Kip Peters will provide a thought-provoking presentation on Ethics in IT. He will deliver an overview of ethics, morality, and ethical styles, and discuss the ethical implications of technology and IT at work and at home. Through examples, ethical dilemmas, and difficult questions, Peters will heighten your awareness of technology-related ethics, equip you to identify true ethical dilemmas, and leave you with several ethical decision-making approaches.

Bio:

Kip Peters is a Leadership Partner for Security & Risk Management with Gartner, the world’s leading IT research and advisory company. He has over twenty-five years of Information Technology (IT) leadership experience in the financial services, state government, and military sectors. While the bulk of his experience is in information security, he has led virtually all aspects of IT during his career.

Mr. Peters has served as the inaugural chief information security officer in multiple organizations, including the state government of Iowa, has been a security consultant, and was an Air Force Information Assurance Officer. He is also a Graduate Lecturer at Iowa State University, teaching “Legal & Ethical Issues in Information Assurance” since 2008. He has a B.S. in Computer Science and an M.S. in Information Assurance, both from Iowa State University.

10:00 – 10:10 am  Break
10:10 – 11:00 am
Matt Curtin – CISSP and Founder, Interhack

Our Insecure Infrastructure
After ten years of state laws requiring disclosure of data breaches, ongoing efforts to establish security standards, and attention by government and industry, security failures continue to dominate the discussion of computing. Why is security so difficult, and how do we recover? We’ll discuss principles of cybersecurity presented forty years ago and how they still apply today—and why it’s imperative that we stop ignoring those lessons.

Bio:
Matt is a computer expert, leading Interhack’s Cyber security team. Through projects and managed services, Interhack helps organizations to prepare for, respond to, and recover from high-impact incidents like data breaches, trade secret misappropriation, and business litigation. Matt has appeared as an expert witness in civil, criminal, administrative, and military adjudication. Matt is also a Sr. Lecturer in the Department of Computer Science and Engineering at The Ohio State University, where he began teaching in 1999.

11:00 – 11:30 am Cybersecurity Updates

Brian L. Quinn - Chief of Operations, STACC Statewide Terrorism Analysis and Crime Center

Statewide Terrorism Analysis and Crime Center (STACC)

Brian Quinn is the Chief of Operations for the Ohio Homeland Security’s Primary Fusion Center, the Statewide Terrorism Analysis & Crime Center (STACC). The STACC’s role is to support local, state, and federal agencies as they investigate terrorism and other criminal activity by fusing information to begin the intelligence cycle.

Chief Quinn retired after serving 10 years as the Chief of Police for the Upper Arlington Division of Police in January 2016. He earned his undergraduate degree in Criminal Justice from Bowling Green State University and a Master’s Degree from Tiffin University. He joined the Upper Arlington Police Division in 1988.

Chief Quinn is a graduate of the 208th Session of Federal Bureau of Investigation National Academy in March 2002 and of the Naval Postgraduate School’s Fusion Center Leaders Program in March 2017. He was named the 7th Upper Arlington Chief of Police on November 28, 2005. He is a Past President of the FBI National Academy having served on the Executive Board for the Ohio Chapter for seven years, served on the Executive Board for the Ohio Association of Chiefs of Police as the District One Representative until his retirement and other boards throughout his career.
He serves as a lead consultant for police promotional assessments for OACP Advisory Services. Chief Quinn has served as an Adjunct Professor at several universities.

Mark Bell - Cyber Security Outreach Coordinator, Ohio Adjutant General’s Department

Ohio Cyber Collaboration Committee (OC3)
Mark primarily works with a wide range of partners throughout Ohio, organized into the Ohio Cyber Collaboration Committee (OC3,) to improve the cyber security posture of the state through education and workforce development, the creation of a Cyber Range in Ohio, the development of cyber response teams for Ohio, and the sharing of best cyber practices and policies throughout the state.

In addition to his work at the Ohio National Guard, Mark continues to serve in the US Army Reserve as the Command Sergeant Major of a Military Police Battalion located in Columbus, Ohio.

11:30 – 11:40 am Break

11:40 – 12:30 Split Session

Main Room       Jonathan Skaggs – Intelligence Analysis, FBI

Cybersecurity Threats

Make-up of the FBI and current cyber trends, including some best practices and lessons learned.

Johnathan is an Intelligence Analysis with the Cincinnati Division of the Federal Bureau of Investigation. He has been with the bureau for over 7 years

🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩🧩

Breakout Room

Phil – Infrastructure Specialist, State of Ohio

Past the Perimeter: What ya gonna do when a breach happens to you?

When looking at any news coverage today one will not have to look hard before hearing about a story of some type of hack, or other type of breach. These types of incidents are especially troubling when they involve government systems, due to the nature of the data stored within government systems. As these incidents continue to increase and evolve, the traditional approach to cyber defense has had to adapt to deal with these threats. With the ever-advancing nature of cyber threats, an agency can no longer afford to rely solely on a perimeter based approach to cyber security, and assume that nothing will gain access. As part of any incident response, a digital forensic examination must be conducted to analyze the incident, and determine how the incident can be prevented in the future. Accordingly, the purpose of this presentation is to discuss the incident response process, how forensic examination applies to the process, and the steps that are taken to forensically examine any incident, and the resulting analysis that is provided.
Phillip Hinders is currently assigned to the Office of Information Security and Privacy as a Forensic Specialist. During his tenure, Mr. Hinders has worked to continue the development of the Office of Information Security and Privacy by performing forensic analysis, providing guidance, and by developing policies that guide the forensic examination process. Prior to joining the Office of Information Security and Privacy, Mr. Hinders spent six years in Law enforcement where he learned skills that are still being applied in his current assignment. During his service, Mr. Hinders was also assigned to teach newly appointed police recruits in law and procedure in the academy as well as in the field as a Field Training Officer.

Mr. Hinders currently hold a Master’s of Science degree in Cyber Security with a concentration in Digital Forensics from Utica College in Utica, New York. As part of his studies Mr. Hinders completed advanced research in applying current legal standards to the qualifications of forensic examiners as legal expert witnesses. This research is entitled “Judicial Adaptation to the Digital Revolution,” and was published in 2016. Mr. Hinders also holds a Bachelor’s of Science degree in Criminal Justice from Radford University in Radford, Virginia.

12:30 – 1:40 pm Lunch Break
1:40 – 2:30 pm Afternoon Keynote Speaker
Rafeeq U Rehman - Business Innovation Consultant, Verizon

Verizon 2017 Data Breach Investigation Report

The Verizon Data Breach Investigations Report (DBIR), in its tenth year, is an unparalleled source of information on cybersecurity threats. Join this session to understand key findings of DBIR 2017:

• Cybercrime can come in any shape or size, and not always the form you’d expect — we explain how cybercriminals seek to compromise your systems.
• Each industry faces a distinctive pattern of threats — discover the biggest risks facing your business.
• Yet again, the overwhelming majority of incidents fall into one of our nine attack patterns — we show you how these can help you mitigate the risks of a breach.

Bio:

Rafeeq Rehman is business innovation consultant providing advice to Verizon corporate customers on matters of information security, IT risk management, and digital transformation. He believes in evidence-based information security as an enabling force and a competitive advantage in the fast changing field of technology. Rafeeq is author of multiple books on information security, operating systems and software development. He holds M.Sc. degree in electrical and computer engineering numerous certifications in the field of information security.

2:30 – 2:40 pm Break
Cloud Security CASB’s Explained

Cloud access security brokers (CASBs) are the most logical solution to address security and compliance requirements in cloud and hybrid environments. CASBs enforce or provide security policies such as authentication and authorization, device profiling, encryption, activity monitoring, alerting, and more. The primary CASB use case has changed from discovering unsanctioned applications (shadow IT) to providing visibility, threat protection and data protection for sanctioned cloud applications.

During this session, you will learn:
1) What is a CASB and how does it work?
2) The primary use cases for a CASB and how they’ve changed over time
3) Key decision points my organization needs to consider when evaluating CASB for my Cloud/Hybrid architecture

Bio:

Mitch Palski is a well-rounded Cloud technologist with a focus in non-profit industries such as S&L government, higher education, and healthcare. He has a strong and experienced background working with customers to identify needs, clearly define use cases, and deliver creative solutions to their problems. At Skyhigh, Mitch has turned his attention to helping his customers find a comfortable path to the Cloud through Cloud Access Security Broker (CASB) technology.

Mitch is focused on educating his customers about how bringing visibility, threat protection, compliance, and data security tools into their Hybrid Technology portfolio will mitigate risk, ensure business continuity, and encourage a secure environment for innovation to flourish. Mitch has a deep background in traditional application development security best practices – especially in the areas of Role-based Access Control (RBAC), Mobile Device Management (MDM), and User and Entity Behavior Analytics (UEBA). He studies emerging cyber security and trends by following populate InfoSec blogs and podcasts (ex: CyberWire, Wired’s Threat Level, Roger McClinton, Dark Reading), being active in AWS User Groups, and closely following news from the Center for Internet Security (CIS).
Past the Perimeter: What ya gonna do when a breach happens to you?

When looking at any news coverage today one will not have to look hard before hearing about a story of some type of hack, or other type of breach. These types of incidents are especially troubling when they involve government systems, due to the nature of the data stored within government systems. As these incidents continue to increase and evolve, the traditional approach to cyber defense has had to adapt to deal with these threats. With the ever-advancing nature of cyber threats, an agency can no longer afford to rely solely on a perimeter based approach to cyber security, and assume that nothing will gain access. As part of any incident response, a digital forensic examination must be conducted to analyze the incident, and determine how the incident can be prevented in the future. Accordingly, the purpose of this presentation is to discuss the incident response process, how forensic examination applies to the process, and the steps that are taken to forensically examine any incident, and the resulting analysis that is provided.

BIO:

Phillip Hinders is currently assigned to the Office of Information Security and Privacy as a Forensic Specialist. During his tenure, Mr. Hinders has worked to continue the development of the Office of Information Security and Privacy by performing forensic analysis, providing guidance, and by developing policies that guide the forensic examination process. Prior to joining the Office of Information Security and Privacy, Mr. Hinders spent six years in Law enforcement where he learned skills that are still being applied in his current assignment. During his service, Mr. Hinders was also assigned to teach newly appointed police recruits in law and procedure in the academy as well as in the field as a Field Training Officer.

Mr. Hinders currently hold a Master’s of Science degree in Cyber Security with a concentration in Digital Forensics from Utica College in Utica, New York. As part of his studies Mr. Hinders completed advanced research in applying current legal standards to the qualifications of forensic examiners as legal expert witnesses. This research is entitled “Judicial Adaptation to the Digital Revolution,” and was published in 2016. Mr. Hinders also holds a Bachelor’s of Science degree in Criminal Justice from Radford University in Radford, Virginia.
Building the Human DMZ

Productive hours are leaking from your organization faster than personal information leaves Yahoo! and Equifax. According to a 2017 study, the average worker is only productive for 2.53 hours per day. While a cyber security professional's day is often full of unplanned work, some activities like excessive meetings, email, phone calls, and walk-ups are unnecessary. What if the same network security strategies and concepts you use each day to defend your DMZ servers could also be used to protect yourself from distractions that wreck your ability to get things done?

In this entertaining presentation, Cyber security expert and productivity coach, Simon J. Herring, will show you how to build your personal DMZ by:

• Identifying and reducing the “yes-flows” — dangerous paths of over commitment that leave you spread thin and overwhelmed.
• Virtualizing your expertise and knowledge, effectively isolating yourself from direct access and persistent interruption (without having to work from home each day).
• Establishing a “least privilege” approach to email, meetings, & walk-up distractions while still being a team player.

Hackers have all the time and focus they need to unleash global havoc. You don’t. If you’re looking for a way to reclaim at least 10 hours of productive time each week then Building the Human DMZ is for you!

Bio:

Simon Herring is an independent cyber security consultant and productivity coach with nearly 25 years of experience. He equips front-line information warriors at billion dollar companies with common sense tips, tricks, and tactics for doing more with less in a world of increasing threats. Through assessments, workshops, and one-on-one coaching, Simon helps executives, managers, and IT teams discover what's holding them back and how to achieve security success. Simon loves security, but people are his passion. You'll enjoy his stories, deep technical expertise, and his dream of building better security professionals. You can reach him at simon@ubersecure.com