CornCon 7: Quad Cities Cybersecurity Conference
Speaker & Activity Schedule
[Click here for Full 2-Day Schedule]

Day 1 • Friday, September 10, 2021

8:00 AM

Registration Opens

8:30AM

(Track 1)

Introduction: Welcome to CornCon 7 Day 1

John Johnson & Shad Roberts, with
VIP Guest: Bob Gallagher, Bettendorf Mayor

9:00 AM

Expo & Villages Open

(Track 1) Tim Callahan, CSO, AFLAC

From Compliance to Resiliency: Evolution of Information Security (v)

Abstract: Information security has come a long way and regulatory compliance requirements change rapidly. It is well recognized that maintaining compliance is not enough to protect your business from the ever-evolving threat landscape. In this session, we will examine the

codependency of Compliance, Security, Maturity, Defensibility and Resiliency and deep dive into what makes a business cyber-resilient.

Bio: Tim Callahan joined Aflac in 2014, bringing more than 30 years of experience in information and physical security, business resiliency and risk management. He was promoted to his current role in January 2016, where he is responsible for directing Aflac's global security strategy and leading the information security, business continuity and disaster recovery functions across the company to prioritize security initiatives and allocate resources based on appropriate risk assessments.

(Track 2) Tim Schulz, Adversary Emulation Lead, SCYTHE

Adding Purple to your Team Color Wheel: Purple Maturity Model

Abstract: Purple teaming is the new kid on the block, straddling the fence between red and blue teams, except this new kid doesn't know what to be when they grow up. As processes and fields mature, standards of operation become the new normal. Blue teams have the multi-level security operations center (SOC) maturity model and hunting maturity model (HMM) to provide a clear path of capability building. Red teams have the Ethical Hacking Maturity Model, and can leverage frameworks like ATT&CK and David Bianco's Pyramid of Pain to match emulation with their capability level. When it comes to purple, there is currently no such model for determining the maturity or capability level. This talk will present an approach to maturing a new purple team from scratch, allowing anyone to chart the path for an internal capability. We will use a multi-level approach to identify the skill sets, people, and processes needed to build a strong purple team. Audiences can expect to walk away with an understanding of where their organization sits in the Purple Team Maturity Model, and what skills their current blue and red teams can leverage to strengthen the organization's purple capabilities.

Bio: Tim Schulz is SCYTHE's Adversary Emulation Lead and has been helping organizations build and train teams to understand and emulate cyber threats for the last six years while working at multiple FFRDCs. He is the author of the Purple Maturity Model and has given talks on Adaptive Emulation with ATT&CK and Technical Leadership.
https://www.linkedin.com/in/tim-schulz/

10:00 AM

(Track 1) Scott Schober, CEO, Berkeley Varitronics Systems

Staying Safe from Skimmers and Scammers

Abstract: If the audience pays with Credit Card or Debit Card they will get a wakeup call as to how prevalent skimming technology is stealing their card information without them knowing it. I will also review how it is packaged and sold on the Dark Web.

Bio: https://linkedin.com/in/snschober

Scott Schober is the President and CEO of Berkeley Varitronics Systems, a 48-year-old, New Jersey-based provider of advanced, world-class wireless test and security solutions. He is the

author of three best-selling security books: Hacked Again, Cybersecurity is Everybody's Business, and Senior Cyber.

Scott is a highly sought-after author and expert for live security events, media appearances, and commentary on the topics of ransomware, wireless threats, drone surveillance and hacking, cybersecurity for consumers, and small business. He is often seen on ABC News, Bloomberg TV, Al Jazeera America, CBS This Morning News, CNN, Fox Business, and many more networks. Scott also serves as the CSO and Chief Media Commentator for Cybersecurity Ventures and sits on several cyber advisory boards for various companies.

(Track 2) Ian Garrett, CEO Phalanx

Hybrid Work Security: Hot Desks are in the Hot Seat

Abstract: No prior knowledge required.

Bio: Ian Garrett, CEO and co-founder of Phalanx, was a former Army Cyber officer focused in offensive operations. His military experience combined with his PhD research set the stage what became the data security company Phalanx. https://www.linkedin.com/in/ianygarrett/

11:00 AM

(Track 1) GRIMM CyPhy Team (Panel)

Conversations with a Tractor Hacker (v)

Abstract: This conversational, not presentational. Interactive with audience. Bring your questions.

Bio: "GRIMM's CyPhy™ (Cyber-Physical) team firmly believes that citizen safety and cybersecurity are intrinsically linked when it comes to embedded systems. Typically, vulnerabilities are most prevalent at the intersection of hardware, software, and firmware. To account for this, the GRIMM team performs end-to-end vulnerability assessments of "systems-within-systems"". Assessments are routinely made in areas of Critical Infrastructure and Industrial Control Systems (ICS), the Internet of Things (IoT), medical IT devices, and connected mobility (e.g., transportation systems, automotive, aviation, and agriculture)."

(Track 2) Kraig Faulkner, Lead Sales Engineer, Cybereason

Ransomware Decoded: Understanding & Preventing Modern Ransomware Attacks

Abstract: It's no secret that Ransomware presents an increasing danger to organizations--there has been a 105% increase in ransomware attacks since the beginning of COVID-19 alone, with 73% of those attacks being effective. Is your organization invested in the right defenses so that it does not fall victim to this costly and dangerous attack?

Bio: *Kraig Faulkner is responsible for helping clients reduce critical risk and enabling successful technology-driven outcomes for Cybereason. As a leader with expertise in threat*

defense across an array of industries, he brings a devout passion for assessing business risk and protecting enterprises from advanced attacks. Kraig understands the consequences associated with leaving data unprotected in an ever-evolving technology-driven world and constantly evangelizes alignment between cross-functional teams to protect sensitive assets – from endpoints to everywhere.

12:00 PM

(Track 1) Adam Kujawa, Director, Malwarebytes Labs

State of Ransomware: The survival guide to living in a ransom-world (v)

Abstract: An overview of the current state of ransomware, followed by predictions based on analyst data and observations on the next phase for ransom actors.

Bio: With over 16 years of experience working with Government Agencies, Private Companies and Educational Organizations, Adam has analyzed threats from across the world. In addition, Adam has taught, published and presented content on malware analysis, threat defense and recovery. https://www.linkedin.com/in/%F0%9F%90%A7-adam-kujawa-78255316/

(Track 2) John Bambenek, Threat Intelligence Advisor, Netenrich

Embrace the Suck: The Devolving Threat Landscape and What to do About It

Abstract: Every year it seems the pace of breaches gets worse. This talk will discuss the threat landscape as it exists today and why we haven't been making any real progress to stem the tide of breaches and major cybersecurity incidents.

Bio: John Bambenek is a threat intelligence advisor for Netenrich and finishing his PhD in cybersecurity machine learning at the University of Illinois Urbana-Champaign. He has over 20 years in the industry and runs several large threat research groups tracking cybercriminal campaigns.

1:00 PM

(Track 1) Bryson Bort, SCYTHE

Throwing the Elephant: How to Hack Leadership

Abstract: Security is defined by the threat, there is no objective measure of it that exists on its own today. So, how can we really do this? If you're a small organization, you've got enough problems keeping users happy so how do you step into the world of threat modeling and emulation? If you're a larger organization, how do you effectively do it at scale? I'll cover the What's In It For Me? for executive/organizational buy-in, how to get started from tooling, process, and baby steps, and how to detection engineer so you can improve as you go. If you're red, blue, or other, there will be something to take away to make you and your org better.

Bio: Bryson is the Founder of SCYTHE, a start-up building a next generation attack emulation platform, and GRIMM, a cybersecurity consultancy, and Co-Founder of the ICS Village, a non-profit advancing awareness of industrial control system security. He is a Senior Fellow for Cybersecurity and National Security at R Street and the National Security Institute and an Advisor to the Army Cyber Institute. https://www.linkedin.com/in/brysonbort/

(Track 2) Kate Kuehn, SVP, vArmour

Visibility Can't Be Zero When Talking Trust

Abstract: In this session, Kate Kuehn will dive deeper into the current market conditions that are propelling the adoption of ZT, review the Best Practices to avoid the non-starters that can create headaches for organizations looking to implement ZT, and understand how organizations can be most effective when considering a ZT Architecture.

Bio: https://www.linkedin.com/in/ian-robertson-4282684/

2:00 PM

(Track 1) Marci McCarthy, CEO/President, T.E.N.

Harness Emotional Intelligence to Stay Connected in a Post-Pandemic World

Abstract: Research has clearly shown that a person can have the best training in the world; a sharp, analytical mind; and an endless supply of good ideas, but these alone will not make them a great leader. While these factors are all important, to be an effective leader, one must also possess a high degree of Emotional Intelligence (EI). This is especially true for information and cybersecurity professionals. Harnessing Emotional Intelligence ensures effective communication between InfoSec executives and their security teams as well as communication between security executives, stakeholders, teammates, lines of business leaders, customers and board members. Strong working relationships and interpersonal skills are the keys to success in every area of human activity, especially for a cybersecurity professional looking to enhance their leadership skills and bring out the best in their teams. However, the past two years have also proven that leaders will need to take their Emotional Intelligence to the next level. We now exist in a post-pandemic world with hybrid work environments, which requires us to communicate in different ways and detect new social cues from our business peers, partners and employees through both in-person and digital means. Join Marci McCarthy as she discusses how you can best utilize Emotional Intelligence to adapt to any situation, improve flexibility and intuition in the workplace and become a better leader who builds successful teams—whether you and your team are working in an office or from home.

Bio: With more than 20 years of business management and entrepreneurial experience, Marci McCarthy founded T.E.N.'s flagship program, the Information Security Executive® of the Year (ISE®) Program Series, which is lauded by the IT industry as the premier recognition and networking program for security professionals in the U.S. and Canada. McCarthy has been a guest lecturer, speaker, and moderator at national conferences such as the ISE® Executive Forum and Award Program Series, ISSA Local Chapter and International Conferences, and

more, speaking on cybersecurity, women in technology/security/business, STEAM, entrepreneurism, and leadership topics.

LinkedIn: https://www.linkedin.com/in/marcimccarthy

(Track 2) Travis Hartman, Brigade Commander, 359th Theater Tactical Signal Brigade & President, IWC Labs

Hide your code! Hide your files! AIs are coming for you!

Abstract: Can humans hope to keep up if an AI wants to propagate attacks from your HVAC to your payroll? In this session we go over the current capabilities of AIs in attack and defense on networks. We will cover the current state of AIs in attack and defense and the mechanisms researchers are using to manipulate the AIs themselves. (Note that the conflation of AIs and machine learning may occur during parts of this presentation solely to annoy fellow researchers). *As a bonus - no skills in Python or advanced statistical knowledge required for this to make sense.*

Bio: Brigade Commander, 359th Theater Tactical Signal Brigade & President, IWC Labs and Ph.D. candidate in Artificial Intelligence at Capitol Technology University.
https://www.linkedin.com/in/travisahartman/

(Track 3) ICS Tabletop Exercise (Scythe)

Abstract: Join us in a tabletop exercise where you play the role of the expert called into assess the unexpected shutdown of a power plant. You will be led through a series of real world malicious activities and be asked to offer your analysis. Can you get operations going again?

3:00 PM

(Track 1) Richard Rushing, CISO, Motorola Mobility

Cybersecurity Maturity – is it Mission Impossible, Wargames, or Top Gun

Abstract: Cybersecurity Attacks are ever-increasing. Ransomware is shutting organizations around the globe. Cybersecurity or Information Security has been around since the computer was invented and progressed into foundations around many aspects of our lives. So when does Cybersecurity mature? Just what is Cybersecurity Maturity about? Does it mean that my Cybersecurity program can start “shaving now” and see R-rated Movies, or could buy alcohol now? This humor-filled view of Maturity as it relates to the 80’s Classics movies and clear analogies for Cybersecurity Maturity.

Bio: https://www.linkedin.com/in/richardrushing/

(Track 2) John Bonar, Security Engineer, Collins

Risk Management Framework or How I Learned to Stop Worrying and Love the NIST SP 800 series

Abstract: Struggling to blend multiple compliance requirements for your Enterprise, or looking for help on trying to develop or improve your existing security plans. The presentation will provide a survey of some of the resources available to the public from NIST in the SP 800 series and other organizations such as DCSA.

Bio: With nearly 20 years of IT experience and punching the nerd card with various hobbies and passions. A current graduate student in the Cyber Defense Masters of Science program after graduating from Dakota State University Summa Cum Laude with a BS in Cyber Operations and holds a CISSP and Security+ certifications. John works daily with Information Systems that must comply with 800-171 and 800-53 requirements.
https://www.linkedin.com/in/jbonar

4:00 PM

(Track 1) Keenan Skelly, CEO, Shadowbyte

Portal to the Upside Down: Cyber Criminals at Play

Abstract: Get lost in the Upside Down, where cyber criminals roam freely between our world and their own. These demogorgon (criminals) act with confidence, knowing they are untouchable due to National and International legal loopholes. We will explore the exploits and interconnectivity between a several of these actors; and highlight the need for National and International Norms involving extradition of known cyber threat actors.

Bio: Disruptor. Hot sauce maker. Bomb slayer. Tight-roller of Jeans. Hunter of Cyber Mind Flayers.

(Track 2) Caroline Wong, Chief Strategy Officer, Cobalt.io

The Future of Cloud-Native Security (v)

Abstract: In recent years, we have witnessed an explosive uptick in cloud-native security implementations for their myriad of benefits. As modern development processes speed up, organizations have recognized the urgent need for integrated security.

In this talk, Caroline will share her observations on how companies must change the way they build security into their cloud-native projects and forecast what's next for cloud-native security. She will discuss how, when it comes to the future of cloud-native security, organizations must double down on people and process innovation to overcome the misconceptions, education gaps and common mistakes we see when it comes to the cloud. Cloud native is here; it is scaling, and it is not going anywhere. The more we can see the reality and necessity of what security must become, the better we will all be in the long run.

Bio: Caroline Wong is the Chief Strategy Officer at Cobalt. As CSO, Caroline leads the Security, Community, and People teams at Cobalt. She brings a proven background in

communications, cybersecurity, and experience delivering global programs to the role.
LinkedIn: https://www.linkedin.com/in/carolinewmwong/

5:00 PM

Expo & Villages Close

(Track 1) John Johnson & Shad Roberts
Day 1 Closing Ceremony, Awards & Door Prizes

6:30 to 10 PM

(Track 1)

- **Music, Networking, Cash Bar**
- **8-10 PM Hacker Jeopardy**
- **10 PM Venue Closes**

Day 2 • Saturday, September 11, 2021

8:00 AM

Registration Opens

8:45 AM

(Track 1)

Introduction: Welcome to CornCon 7 Day 2

John Johnson & Shad Roberts, with
VIP Guest: Chris Cournoyer, Iowa State Senator

9:00 AM

Expo & Villages Open

(Track 1) Richard Thieme, Author/Speaker, Thiemeworks

The More Things Change: The Necessity for Thinking like a Hacker, Thinking Critically, and above all, Thinking (Reprising DEFCON 1 talk) (v)

Bio: Richard Thieme is an author and professional speaker focused on the challenges posed by new technologies and the future, how to redesign ourselves to meet these challenges, and creativity in response to radical change and identify shift. His column, "Islands in the Clickstream," was distributed to subscribers in sixty countries before collection as a book in 2004. When a friend at the National Security Agency said after they worked together on ethics and intelligence issues, "The only way you can tell the truth is through fiction," he returned to writing short stories, 19 of which are collected in “Mind Games.” A novel FOAM will be available this month (October 2015). He is also co-author of the critically extolled “UFOs and Government: A Historical Inquiry,” a 5-year research project using material exclusively from government documents and other primary sources, now in 65 university libraries

His work has been taught at universities in Europe, Australia, Canada, and the United States, and he has guest lectured at numerous universities, including Purdue University (CERIAS), the Technology, Literacy and Culture Distinguished Speakers Series of the University of Texas, the “Design Matters” lecture series at the University of Calgary, and as a Distinguished Lecturer in Telecommunications Systems at Murray State University. He addressed the reinvention of “Europe” as a “cognitive artifact” for curators and artists at Museum Sztuki in Lodz, Poland, keynoted CONFidence in Krakow 2015, and keynoted “The Real Truth: A World’s Fair” at Raven Row Gallery, London, He has spoken for the National Security Agency, the FBI, the Secret Service, the US Department of the Treasury, and Los Alamos National Labs and has keynoted “hacker” conventions around the world. He spoke in 2021 at Def Con.

(Track 2) Douglas Brush, Global Advisory CISO, Splunk

You Don’t Have to Be Crazy to Work Here: An Honest Talk About Mental Health

Abstract: Cybersecurity professionals spend most of their day focused on the health and wellbeing of the environments in their care. However, the cost of reducing risk and keeping our networks safe often comes at the price of our professionals’ mental health. Many InfoSec professionals burn out, suffer from anxiety and depression, and turn to unhealthy coping mechanisms, which further exacerbate underlying psychological and physical health issues. This talk will alleviate the stigma around mental health and stress the importance of open and frank dialogs about this critical issue impacting our community. I will share my journey, reverse engineer the stigma of mental health in business, and look at ways to hack mental health in productive and meaningful ways.

Bio: https://cybersecurityinterviews.com/douglas-a-brush-speaker-bio/

(Track 3) ICS Tabletop Exercise (Scythe)

Abstract: Join us in a tabletop exercise where you play the role of the expert called into assess the unexpected shutdown of a power plant. You will be led through a series of real world malicious activities and be asked to offer your analysis. Can you get operations going again?

10:00 AM

(Track 1) Kate B., CEO, Cybermaniacs!

A fireside chat with Kate Kuehn on a new way to train employees – Cyber Education

Abstract: Creating secure humans through innovative use of technology and puppets. Making the world a happier, safer place.

Bio: Kate Kuehn https://www.linkedin.com/in/katekuehn/
Kathryn Brett Goldman https://www.linkedin.com/in/kathrynbrettgoldman/

(Track 2) Sick.Codes, Security Researcher

The Agricultural Data Arms Race: Exploiting a Tractor Load of Vulnerabilities in the Global Food Chain (v)

Abstract: How I hacked the entire American Food Supply Chain over the course of 3 months, assembled a team of hacker strangers, and how we used a "full house" of exploits on almost every aspect of the agriculture industry. See the process in which it happened, the private exploits we used, the vectors we attacked from, and how it could happen again, or be happening right now. How the ongoing analytics arms race affects everyone, and how Tractor companies have metastasized into Tech companies, with little to no cyber defenses in place. Learn how farms are not like they used to be; telemetry, crop & yield analytics, and more telemetry.

Bio: Responsible Security Researcher: https://sick.codes/vdp

11:00 AM

(Track 1) Winn Schwartau, Chief Visionary Officer, SAC Labs!

Defending Security is Probabilistic, Not Deterministic: Get Over It (v)
Audience participation involved!

Abstract: Since the inception of computer/data/cyber/network security some fifty years ago, one recurring question has beset our industry: “How do we secure it?” By its very nature, this question has propagated a harmful meme, by implying that a binary deterministic answer is possible. “How can we defend against unknown vulnerabilities and hacks?” is perhaps a more realistic question.

Bio: Winn has lived Security since 1983, and now says, “I think, maybe, I’m just starting to understand it.” His predictions about the internet & security have been scarily spot on. He coined the term “Electronic Pearl Harbor” while testifying before Congress in 1991 and showed the world how and why massive identify theft, cyber-espionage, nation- state hacking and cyber-terrorism would be an integral part of our future. He was named the “Civilian Architect of Information Warfare,” by Admiral Tyrrell of the British MoD. His new book, “Analogue Network Security” is a mathematically based approach to provable security where his goal is to provide tools and methods to “fix security and the internet”.

Distinguished Fellow: Ponemon Institute Top-20 industry pioneers: SC Magazine. Top 25 Most Influential: Security Magazine Top 5 Security Thinkers: SC Magazine. Power Thinker and one of the 50 most powerful people: Network World. Top Rated (4.85) RSA Speaker Author: Pearl Harbor Dot Com (Die Hard IV), 3 volumes of "Information Warfare," "CyberShock", "Internet and Computer Ethics for Kids", "Time Based Security" (More on his web site.) Founder: www.TheSecurityAwarenessCompany.Com Founder: www.InfowarCon.Com Executive Producer: "Hackers Are People Too"

(Track 2) Professor Gene Spafford, Purdue Univ.

One View of Cyber Past and Future (v)

Abstract: I have been involved in computing for almost 50 years, and in cyber security for over 40 of those years. In this talk, I'll recount a little of how I got started in computing, and how I became interested in cybersecurity. I'll also explain a little about the cybersecurity challenges with illustrations of the past, and projections into the future. This won't be an expansive view of the field, but rather a personal view, shaped by my experience as a researcher and teacher.

Bio: Eugene H. Spafford is one of the most recognized esteemed leaders in the field of computing. His research and development work, including work with his students, underlies cyber security mechanisms in use on millions of systems in use today, including work in firewalls, intrusion detection, vulnerability scanners, integrity monitoring, forensics, and security architectures.

12:00 PM

(Track 1) Richard Greenberg, CEO, Security Advisors

Breaches are Everywhere. What's a Good Security Leader to Do? (v)

Abstract: Breaches are on the news seemingly weekly, as organizations are struggling to secure their data. In this talk, Richard will share strategies to combat the rise of cybercrime, and how to make your networks more secure. He will discuss administrative, technical, and physical security controls. Phishing attacks are proliferating and seemingly at will compromising our workforce. Ransomware has taken several victims and payment demands are escalating. All organizations seem to have become prime targets. Have you built a sustainable and dynamic Information Security Program? Have you shared this with upper management and gotten their buy-in and support?

Have you initiated a balanced Security Awareness Program? Are you regularly running scans of both your network and your applications? Are you monitoring your network to detect unusual activity? What about when that dreaded intrusion into your network occurs? Do you know what to do? Are you testing and evaluating your security controls on a regular basis? How often do you test your Disaster Recovery Plan and your Incident Response Plan? Do you have the right people on your IR team? We are entrusted with highly sensitive data. We must utilize best practices and ensure we have a comprehensive Cyber Security Program. Come learn if you are doing this and ensure that you indeed are properly protecting your confidential information. Don't allow your organization to become the next victim of a breach.

Bio: https://www.linkedin.com/in/richardagreenberg/

(Track 2) Casey Ellis, Founder/Chairman/CTO Bugcrowd

The Unlikely Romance (v)

Abstract: A primer on how hackers and organizations are working together, and what that looks like in 2021

Bio: https://www.linkedin.com/in/caseyjohnellis/

1:00 PM

(Track 1) Richard Marshall, Chairman, Citurion Group

Cyber Security: Fact or Fiction

Abstract: What are realistic expectations

Bio: Dr. Marshall offers 20 plus years of broad executive leadership experience as a former member of the Senior Executive Service in the federal government having served in the Department of Defense, National Security Agency (legal architect of nation's first cyber warfare exercise), the White House (Comprehensive National Cyber Security Initiative), the Department of Commerce (Critical Infrastructure Assurance Office), and the Department of Homeland Security (Director of Global Cyber Security Management).
Since retiring from federal service (as a SES level two, the equivalent of a two star general) he has broadened his executive experience by serving on various boards of directors, CEO of tech startups, Executive Director of a non-profit research center, and Special Cyber Advisor to the government of Moldova.

(Track 2) Mark Jaster, CEO, 418 Intelligence Corp.

Phinding Phish … and other Games on the way to Work (v)

Abstract: In the first half of 2021, following a successful DHS supported pilot last year, we proved that a gamified threat hunting and collaboration platform could deliver a live real-world threat hunting experience to cyber threat analyst interns from rural Kentucky that landed over 80% of them full-time high-paying remote cyber security analyst jobs on their first interviews. We will present an overview of the technologies that comprise the systems and discuss their potential uses in analyst skill development and on-demand threat hunting while demonstrating the user experience of the analyst platform live.

Bio: Mark Jaster is the Founder & CEO of 418 Intelligence. Mark is an entrepreneur and technology strategy expert with over 30 years of deep expertise in developing technology for complex problems that drive growth. https://www.linkedin.com/in/mjaster/

(Track 3) Dr. Phil Polstra, Professor, Bloomsburg University

Getting started in ARM reverse engineering (TUTORIAL)

Abstract: This talk will introduce the ARM platform and what you need to know for reverse engineering on this platform. Basic Assembly language is helpful, but not required.

Bio: Phil was born at an early age. He cleaned out his savings as a boy in order to buy a TI99-4A computer for the sum of $450. Two years later he learned 6502 assembly and has been hacking computers and electronics ever since. Dr. Phil currently works as a professor at Bloomsburg University of Pennsylvania. His research focus over the last few years has been on the use of microcontrollers and small embedded computers for forensics and pentesting. https://www.linkedin.com/in/philip-polstra-2b87037/

2:00 PM

(Track 1) Michael Daugherty, CEO, LabMD

Cybercriminals, Politicians and Bureaucrats: What could possibly go wrong?

Abstract: Mike Daugherty is the CEO of LabMD, a cancer testing laboratory and Founder of The Cyber Education Foundation. A graduate of The University of Michigan, Mike was a surgical healthcare entrepreneur for over twenty years marketing implantable medical devices. In 1996 he founded LabMD. He has spent most of the last decade defending his company against charges that it had deficient cybersecurity practices. (https://www.bloomberg.com/features/2016-labmd-ftc-tiversa/)

The early years of his entering and fighting Washington, DC, are recorded in his book, “The Devil Inside the Beltway”. In so doing, he has become the only litigant to challenge the basic authority that underlies more than 200 enforcement actions relating to cybersecurity and online privacy that the FTC has brought over the past 15 years. Every one of the 200+ litigants before him – including some of the largest companies in the world – have settled with the FTC, creating an unquestioned and untested belief that the FTC has broad authority to regulate in these areas. On June 6, 2018, he prevailed. In so doing, he toppled key pillars of the FTC’s cybersecurity and online privacy edifice, successfully exposing and challenging The Administrative State. Mike is committed to our Founding Fathers’ principles regarding the separation of powers, so he demands fair notice, due process and accountability. Mike seeks to educate and demonstrate how these principles are sorely lacking in DC today.

https://www.newyorker.com/magazine/2019/11/04/a-cybersecurity-firms-sharp-rise-and-stunning-collapse

Bio: Mike Daugherty is the CEO of LabMD, a cancer testing laboratory and Founder of The Cyber Education Foundation. A graduate of The University of Michigan, Mike was a surgical healthcare entrepreneur for over twenty years marketing implantable medical devices. In 1996 he founded LabMD. He has spent most of the last decade defending his company against charges that it had deficient cybersecurity practices. https://corncon.net/michael-daugherty-ceo-labmd-2/

(Track 2) George Simmonds, Founder, ICISI

Performance-Based Tactics in Cybersecurity Through Persistent Threat Emulation

Abstract: Threat emulation should be realistic and the basis of cyber defense across all critical infrastructure sectors.

Bio: Mr. Simonds specializes in cybersecurity and the protection of our nation's critical infrastructure from cyber-based threats. He is the Executive Director of ICISI and consultant for Fortune 500 companies and governments around the world. (https://www.linkedin.com/in/george-simonds-a660191/)

3:00 PM

(Track 1) Ian Robertson, SVP Advanced Technologies, NCC Group and Javed Samuel, VP, NCC Cryptography Services Division (v)

Castles Built on Sand - a pen-testers view on integrations

Abstract: This talk will review the foundations of cryptographic vulnerabilities as applicable to open-source software from a penetration tester's perspective over multiple public cryptography audit reports. It will discuss what attacks in the past took advantage of these cryptography vulnerabilities and what the consequences were. The talk will also examine ways that open-source software has been updated over time to mitigate these cryptography flaws and how successful these mitigations may have been. Finally, some thoughts on possible areas that could be the focus for future cryptography vulnerabilities in open-source applications will be presented.

Also some embedded systems shenanigans.

Bios:
https://www.linkedin.com/in/ian-robertson-4282684/ As Senior Vice President of Advanced Technologies, Evolving and Specialist Practices, Ian Robertson oversees the boutique service offerings for NCC Group. This includes cryptography, full-spectrum attack, hardware and embedded systems, operational technologies, connected vehicles and telecommunications. Previous to NCC Group, Ian held senior leadership positions at Sony Pictures, Motorola (under Google) and BlackBerry. He is well known for having founded the security research and response team for Research in Motion and building highly effective security organizations.

Javed Samuel is the Vice President of NCC Group's specialized Cryptography Services Division. Javed and his team specialize on novel cryptographic implementation and design assessments across a range of areas such as open-source cryptography projects, embedded devices, post-quantum cryptography, block-chain ecosystems, smart contract execution environments, authentication mechanisms, encryption tools and custom protocol reviews. We also devote significant time to cryptography research across multiple areas and regularly present at various security conferences. Prior to NCC Group, Javed worked as a developer with Oracle's Database Security group. Javed obtained an MEng and BSc in Computer Science MIT. His MEng thesis was in geometric algorithms: Lower bounds for Embedding the Earth Mover Distance Metric into Normed Spaces. He obtained a Rhodes Scholarship and

completed an MSc in Applied and Computational Mathematics at Oxford University. His thesis was on analyzing a mathematical model of the spread of computer viruses: The Fitness Network: Properties and Epidemic Dynamics.

(Track 2) Aaron Warner, CEO, ProCircular (Moderator)

Panelists:

- **Auditor Joel Miller from Linn County**
- **Gabe Kimbrough, CISO @ MercyCR**
- **and Jon Neff, CIO at Kirkwood**

Panel: Targeted Industries: Election Security, Higher Ed & Healthcare Cybersecurity in Practice

Abstract: While all businesses are faced with increased cybersecurity threats, such as ransomware, small to medium-sized businesses often face resource and budget limitations. The panel will be joining Aaron R. Warner, Founder/CEO of ProCircular. This panel will take questions, discuss the most recent threats, and how they effectively defend against and respond to cybersecurity threats without breaking the bank.

Bio: Mr. Warner's decades of global IT and cybersecurity expertise, an MBA from the University of Iowa, CISSP, Certified CISO, and Security+ certifications underline the organization's commitment to aligning cybersecurity, compliance and their clients' company strategy.

(Track 3) X31phix

Getting started in ARM reverse engineering (TUTORIAL)

Abstract: To ensure proper formatting, I uploaded the txt file to my Gitlab: https://gitlab.com/xe1phix/ParrotSecWiki/-/blob/InfoSecTalk/Xe1phix-InfoSec-Talk-Materials/Secure-Linux-Networking-v2-%5BCornCon-2021%5D/Secure-Linux-Networking-v2-%5BCFP%5D/Xe1phix-Securing-Linux-Networking-v2-CFP-CornCon-2021-%5Bv9.6.45%5D.txt

Bio: "Xe1phix is a dual certified Linux Systems Administrator (LPIC-1, Linux+) with over 9 years experience in GNU/Linux systems. He is currently studying for his LPIC-2. He excels especially in system hardening, malware analysis, and memory forensics. He works for an ISP as a network administrator. Xd1phix also provides community support for the Parrot Linux project." https://www.linkedin.com/in/mark-curry-linux-infosec-professional/

4:00 PM

(Track 1) Ira Winkler, CISO, Skyline Technology Solutions

A Multilayered Approach to Stopping Ransomware

Abstract: This presentation will look at the ransomware lifecycle and discusses how ransomware originates, is distributed, activated, and can be consistently mitigated before

damage occurs. Mitigation can happen at all levels of the attack. In the end, as I always say, behind very stupid user is a stupider security professional.

Bio: Ira is considered one of the world's most influential security professionals. He began his career at the National Security Agency (NSA), and has since served in other positions supporting the cybersecurity and risk management programs in organizations of all sizes. He has written widely on, and speaks around the world about, cybersecurity, risk management, loss mitigation, and the human aspects of security and technology. His latest book "You Can Stop Stupid" will be released in December and is available for order at https://tiny.cc/stupidbook. https://www.linkedin.com/in/irawinkler/

(Track 2) Jason Barnes, Sr. Mgr, Netskope Security Operations

Building a Future-Proof SOC

Abstract: *SaaS is the future of security. The office is everywhere. Automate everything. Until the day we reach the AI singularity, security operations is still all about enabling, motivating, and engaging with your people. SASE can help. The value of SASE includes shifting the responsibilities of certain services to the cloud, which frees up time for SOC analysts to focus on different tasks. SASE technology also solves some challenges that SOCs deal with, reducing or even outright eliminating some risk that today's SOCs must account for.*

Bio: https://www.linkedin.com/in/thejasonbarnes/

5:00 PM

Expo & Villages Close

(Track 1) John Johnson & Shad Roberts
Day 2 Closing Ceremony, Awards & Door Prizes

6:30 to 10 PM

(Track 1)

- **6:30 -10 PM "The Bill Murray After Party"**
- **Music, Networking, Open Bar & Snacks**
- **10 PM Venue Closes – See you in 2022!**