DAY 1 • FRIDAY SEPTEMBER 30, 2022

8 AM • REGISTRATION OPENS • RIVERCENTER / 136 E 3rd St, Davenport, IA 52801.

9AM • INTRODUCTION / Welcome to CornCon 8 • TRACK 1 / MISSISSIPPI HALL

9:10AM EXPO HALL OPENS • TRACK 1 / MISSISSIPPI HALL

9:10AM PRESENTATIONS

TRACK 1 • *Adversary ROI* / Defenders have to deal with a plethora of different adversaries - from script kiddies to nation states with a variety of motivations. Throwing your hands up and saying "we'll just defend ourselves and the adversary doesn't matter" doesn't work, as our limited resources aren't adequate to create perfect security. Learn how understanding potential adversaries and their motivations can help optimize your security program.

- DAVID ETUE, CEO, Nisos https://www.linkedin.com/in/davidetue/ • @djetue

TRACK 2 • *Threat Model Trick or Treat? (Accelerating secure design)* / Threat models seem to be having a “moment”. OWASP and NIST have recently highlighted the urgent need for

threat modelling. Articles, books, presentations abound. But even those who have skill are often daunted by recurring, typical challenges. Some of the problems appear as initiatives begin, while others are a sign of program maturity. There are solutions! Indeed, some common mistakes make things worse versus the hard-learned "tricks" that ease the way towards effective and comprehensive threat modelling. Brook S.E. Schoenfield will outline the issues that come up in almost every effort and their field-tested solutions. Watch out! Some of Brook's "tricks" may contradict accepted "wisdom"! A few "treats" are guaranteed.

- BROOK S.E. SCHOENFIELD, Principal Software Security Strategist & Chief Security Architect, True Positives LLC & Resilient Software Security LLC https://www.linkedin.com/in/brookschoenfield/ • @BrkSchoenfield

10AM FOOD & DRINK CONCESSIONS OPEN

10AM PRESENTATIONS

TRACK 1 • *Financial Industry Panel*

- AARON LINT, Security Lead, Anchorage Digital https://www.linkedin.com/in/lintile/ • @lintile
- GARY HAYSLIP, CISO, Softbank https://www.linkedin.com/in/ghayslip/ • @ghayslip
- JAVIER GONZALEZ, CISO, Barclays Mexico https://www.linkedin.com.in/cyberjago • @ @Cyber_JAGO
- TELLIS WILLIAMS, CISO, Dream Exchange https://www.linkedin.com/in/tellis-williams-9a8a501/ • @tellis_williams

TRACK 2 • *Registering Enterprise Risk* / We've heard talks about what metrics to use or how to present them. Turns out, risk presentation format doesn't matter! Come to this talk to hear about research in this space and recommendations for a better Board discussion.

- EDWARD MARCHEWKA, VP of IT, Gift of Hope Organ & Tissue Donor Network https://www.linkedin.com/in/emarchewka/ • @EJMarchewka

TRACK 3 • *The Impact of Ransomware* / SPONSORED BY RUBRIK

- TOM WILCOX, Former CTO/CISO, Involta https://www.linkedin.com/in/towilcox/

11AM PRESENTATIONS

TRACK 1 • *Board Level and Executive Reporting – How the Proposed SEC Cybersecurity Guidelines will Impact Us*

- DEMETRIOS LAZARIKOS (LAZ), Co-Founder and President, Blue Lava
  https://www.linkedin.com/in/iamlaz/

TRACK 2 • *M365 Threat Hunting – Discovering Microsoft Cloud Vulnerabilities* / 90% of organizations rely in some way on the Microsoft cloud for their operations. Whether for email, document sharing or collaboration, M365 has become a critical part of our daily business lives. Aaron Turner will provide an overview of how to approach threat hunting in this complex environment.

- AARON TURNER, CTO, Vectra AI
  https://www.linkedin.com/in/aaronrturner/ • @aaronrturner

12PM PRESENTATIONS

TRACK 1 • *Threat Management Panel / SPONSORED BY CYBEREASON*

- KRAIG FAULKNER, Associate Director, Sales Engineering, Cybereason
  https://www.linkedin.com/in/kraigfaulkner/
- JEFF LENNINGER, Sales Engineer, Cybereason
  https://www.linkedin.com/in/jlenninger/
- ANDY NELLER, Deputy CISO, Wellmark Blue Cross and Blue Shield
  https://www.linkedin.com/in/andyneller/
- BRANDON POTTER, CTO, ProCircular
  https://www.linkedin.com/in/brandonapotter/

TRACK 2 • *A Modern Approach to Pentesting Zero Trust Environments* / Zero Trust is the new buzzword. But when you get past all the marketing fluff, you're left with a network architecture in conflict with traditional pen testing methodologies. We must do better! The goal is to assess business risk based on actual threats and missing, weak, or failed security controls. In this talk we'll explore the fundamental pieces of the Zero Trust model and discuss a modernized approach for analyzing potential threats and simulating attacks that validate business risk to the organization by coordinating offensive and defensive efforts.

- NATHAN SWEANEY, Principal Security Consultant, Secure Ideas
  https://www.linkedin.com/in/nathansweaney/ • @sweaney

1PM PRESENTATIONS

TRACK 1 • *Community Building in Trusted Circles* / We rely on technology and tools to assist is us with our work keeping our organizations safe. But beyond the tools are the people. This talk will discuss building communities and trusted circles in sharing organizations. Getting people to share intelligence and work with peers on larger issues facing their industry vertices.

- CHERIE BURGETT, Director, Cyber Intelligence Operations, Mining & Metals ISAC https://www.linkedin.com/in/cherieburgett/

TRACK 2 • *Oh the passwords you'll crack: An Absurdist Look at Why Enterprises Still Suck at Identity and Access Management* / In this talk, we'll look at how the modern discipline of Identity and Access Management's failure modes continue to be exacerbated by cognitive biases in user populations, and how legacy protocols and backwards compatibility in infrastructure render reasonable efforts to solve the issue moot. And we're bringing memes!

- BOBBY KUZMA, Director of Offensive Cyber Operations, ProCircular https://www.linkedin.com/in/bobbykuzma/ • @BobbyKuzma

TRACK 3 • *Gazing into the Crystal Ball – The Fog of Cyberwarfare Escalations* / Every new technology presents the possibility of new weapons, and for every new weapon, there's a soldier hoping it will yield the ultimate advantage, although few ever do. The nature of war is never gonna change. But the character of war is changing before our eyes–with the introduction of a lot of technology, a lot of societal changes with urbanization, and a wide variety of other factors. In order to have a robust discussion about how emerging technologies may affect the proliferation of modern cyberwar, it is vital to understand these technologies. In this session, ISR techniques (intelligence, surveillance, reconnaissance), and counter-drone security serve as productive examples of technologies that we have witnessed in recent conflicts playing the role of a potential tool of exploit and will be greatly escalated in the future as well. This session provides the background and context required to assess potential challenges to this emerging cyber threat. As will be discussed with case studies, advancements in these areas are especially relevant because they have made it increasingly easy for Infosys to leverage these technologies to achieve its objectives and threaten the global IT/ICS ecosystem.

- HARSHIT AGRAWAL, RF Security Researcher, Boston University https://www.linkedin.com/in/harshitnic/ • @harshitnic

2PM PRESENTATIONS

TRACK 1 • *The Fast and Furious of Cybersecurity: The FTC and FBI Cooked the Books*/ My experiences with law enforcement corruption and why it should matter to all of us.

- MICHAEL J. DAUGHERTY, CEO, LabMD & Founder, The Justice Society https://www.linkedin.com/in/michael-j-daugherty-7a500819/ • @DaughertyMJ

TRACK 2 • *Threat Hunting in Practice: How to Protect Critical Assets Through Systematic Proactive Threat Hunting* / Today's organizations face unprecedented challenges in battling cyber threats. Between increasingly sophisticated cybercriminals, rapidly expanding digital assets and attack surfaces, and a legal landscape that threatens to punish those companies that fail to adequately protect their customers' privacy rights, it's not hard to see why cybersecurity professionals are buckling under the mounting pressure. Within this complex new cyber threat battleground, organizations cannot afford to continue relying on passive, reactive defense, and instead, must leverage the tools and methodologies to facilitate a truly proactive and preemptive cyber defensive program.

- MICHAEL-ANGELO ZUMMO, SR., Threat Intelligence Specialist, Cybersixgill https://www.linkedin.com/in/michael-angelo-zummo-usmc-m-s-8666a7aa/

TRACK 3 • *Predicting which CVEs will next appear on CISA's 'exploited in the wild' list* / Dan will present the challenges of predicting 'exploited in the wild', our prediction model from a high-level perspective, the details of the data backing our model, and a detailed discussion of how well our model performed against the CISA list of CVEs currently being published. Background in CVEs, 'exploited in the wild' concepts are needed to understand talk, some knowledge of machine learning and prediction would be helpful but not required.

- DAN CORLETTE, Head of Research, Northstar

3PM PRESENTATIONS

TRACK 1 • *Why We Hack Tractors* / John Deere's perspective on product security

- DAVE BAILEY, Sr. Staff Embedded Security Engineer, John Deere https://www.linkedin.com/in/dave-bailey-96493161/ • @daveisu
- AMELIA WIETTING, Senior Security Engineer, John Deere https://www.linkedin.com/in/wietting/ • @aask42

TRACK 2 • *Performing Risk Assessments on a Shoestring* / Risk assessment is essential for protecting critical systems, but process can be daunting. The NIST Cyber Security Framework (CSF) provides a straightforward process for starting down the path of evolving risk assessment. This session will provide a starting point using a standard process without incurring extensive costs.

- KEN ROWE, President, InfraGard Springfield Members Alliance https://www.linkedin.com/in/ken-rowe-security40-61801/

4PM PRESENTATIONS

TRACK 1 • *The Risks of Jailbreaking Your Tractor*

- SICK CODES, Security Researcher https://www.linkedin.com/in/sickcodes/ • @sickcodes

TRACK 2 • *Securing Your Work from Home Environment*

- FRED KWONG, VP and CISO, DeVry University https://www.linkedin.com/in/fredkwong/ • @ftkwong

5PM – 6:30PM • HACKER JEOPARDY IN TRACK 1 (Sign up at Registration)

DAY 2 • SATURDAY OCTOBER 1, 2022

8 AM • REGISTRATION OPENS • RIVERCENTER / 136 E 3rd St, Davenport, IA 52801.

9AM • INTRODUCTION / Welcome to CornCon 8 • TRACK 1 / MISSISSIPPI HALL

9:10AM EXPO HALL OPENS • TRACK 1 / MISSISSIPPI HALL

9:10AM PRESENTATIONS

TRACK 1 • *My first hack was in 1958 (Then a career in Rock 'n' Roll taught me about security)/* Seriously. My first hack was in 1958, and it was all my mother's fault. Or perhaps I should also blame my father. They were both engineers and I got their DNA. As a kid I hacked phones… cuz, well, using telephones were expensive! (Cardboard was also an important hacking tool.) At age 6 I made a decent living cuz I could fix tube TVs. True!

In roughly 1970 (thanks to NYU) we moved on to hacking Hollerith (punch) cards to avoid paying for telephone and our utilities, and of course, shenanigans.

As a recording studio designer and builder, we dumpster dived for technology from AT&T. We never threw anything out and learned how to repurpose tech from the 1940s.

As a rock'n'roll engineer, I learned to live with constant systems epic failures. Anything that could break would break before a live TV event or a massive concert. Talk about lessons in Disaster Recovery and Incident Response.

This story-laden talk is chock full of pictures a from the past, covers my hacking path as a kid then as a necessary part of survival in the entertainment industry. "The Show MUST Go On!"
Come on down for a wild ride and see how 64 years of my hard lessons learned can give you an entirely different view of Hacking, D, & IR, and how and why I have embraced failure for both of my careers!

- WINN SCHWARTAU
  https://www.linkedin.com/in/winnschwartau/ • @winnschwartau

TRACK 2 • *Security Architecture Paradigm & Associated Baggage /* This is a presentation and discussion about what is Security Architecture, the various Certifications, a few frameworks and a little bit about one of the certificate bodies' approach.

Then thrown in is a discussion about the various baggage enterprises usually have that can make building a secure architecture much easier. For example, what are the GRC components and how do they tie together with the Security Architecture foundational elements to enable AGILE secure architectures.

- BRUCE NORQUIST, Product Security, A Large Financial Organization
  https://www.linkedin.com/in/brucenorquist/ • @bruce_norquist

10AM FOOD & DRINK CONCESSIONS OPEN

10AM PRESENTATIONS

TRACK 1 • *The Evolution of the CISO – How to make the transition from technical to transformational* / In today's dynamic environment, the role of the CISO can be compared to a Swiss Army knife. You have to have a firm understanding of technology, compliance, and emerging trends, enable strong communication ties between a number of disparate departments, foster strong leadership, and most importantly be able to translate complex cybersecurity topics to a language that a Board and Executive Team can comprehend. The culmination of all these skills is to enable key stakeholders to make critical strategic decisions for the enterprise, and then lead the program to enact them. In this session we will consider the current state of the role of the CISO, and the journey from being predominantly technical to understanding the business acumen necessary to make the leap to being a transformational business leader. We will examine from a professional development perspective, how to assess and understand the cybersecurity maturity of an organization from a business lens, and how a Board views risk to create a correlation of initiatives.

- KATE KUEHN, SVP, vArmour
  https://www.linkedin.com/in/katekuehn/ • @KateKuehn

TRACK 2 • *How we do security reviews at Slack* / The Security Review activity that includes Design Reviews and Code Reviews/Pentest is an important aspect of Security Program, but it's costly in terms of engineering efforts, and takes too much time to finish! Come and learn how we improved collaboration with developers and made the process easy to adopt using a Slack Bot App, JIRA workflow.

- ATULKUMAR GAIKWAD, Staff Software Engineer, Salesforce
  https://www.linkedin.com/in/21451186

TRACK 3 • *Forensics Workshop* / 2-Hour Session

- DR. PHIL POLSTRA, Professor, Bloomsburg University of Pennsylvania
  https://www.linkedin.com/in/philip-polstra-2b87037/

11AM PRESENTATIONS

TRACK 1 • *Welcome to the Dark Side, we own EVERYONE'S Cookies... /* Our record (Feb 2022) for breaking into a fully patched, XDR, UBA, NGFW, ABC, AI, ML target was 2 minutes and 6 seconds... Our record for breaking through your web application with its containers, dockers, WAF's and MFA's.... about 5 minutes and that's only because we got lost in the Amazon along the way...

So, now we've burst your bubble and introduced you to reality what CAN you do? What SHOULD you be doing? AND how can you reduce risks in the digital realm? WHERE is it most

effective to build out security AND what the hell DO you do to make sure when I'm inside you know I'm there AND can do something about it BEFORE I wander off with all YOUR data, leaving behind a nice set of ransomed systems with an I-love-you note for $10m

- CHRIS 'SIDRAGON' ROBERTS, CISO/Geek/Hacker, Boom Supersonic https://www.linkedin.com/in/sidragon1/ • @Sidragon1

TRACK 2 • *Big Trouble in Little SOC -- Of Dragons and Fire Extinguishers/* This talk focuses on how to build a model that intersects your threats/adversaries, your assets, your security capabilities, and resources to build you some priorities -- where you should focus SOC work, and where you should be closing gaps.

- RAFAL "Wh1t3Rabbit" LOS, Head of Services GTM, ExtraHop https://www.linkedin.com/in/rmlos/ • @wh1t3rabbit

12PM PRESENTATIONS

TRACK 1 • *The Top 5 Cloud Native Risks*

- BOB WEST, CISO, Prisma Cloud, Palo Alto https://www.linkedin.com/in/bowest/ • @rkw59

TRACK 2 • *Detection Is Your Superpower /* Protecting a network against a hacker means that you had to be on your game 100%, but the hacker only needed to be right once to get in. But wait! With detection the tables are turned, and they're on your territory. If an attacker interacts with your network, they absolutely must generate artifacts related to the interaction. Detection becomes your advantage, as the attacker has to avoid leaving a mark and all you have to do is watch and wait.

- STEL VALAVANIS, CEO, onShore Security https://www.linkedin.com/in/stelvalavanis/ • @stelvalavanis

1PM PRESENTATIONS

TRACK 1 • *(Incident Response Panel)* ***How do you prepare for the 100 year "cyber" flood that now happens every year? /*** Cyber professionals must prepare for the unpredictable event that is beyond what is normally expected of a situation and has potentially severe consequences. Career military operators in kinetic and cyber operations, and world-class security professionals will share the challenges and successes that helped shape the security posture of large ultra-large-scale organizations. This talk will focus on planning, training,

organizational culture, and the best practices that are actionable in assisting organizations and CISO prepare for their Black Swan event.

- RICHARD HL MARSHALL, ESQ., Chairman of the Board, Cinturion Group https://www.linkedin.com/in/rmarshall141699/
- RICHARD RUSHING, CISO, Motorola Mobility https://www.linkedin.com/in/richardrushing/ • @SecRich
- J.C. VEGA, CISO/US Army Colonel (Ret) https://www.linkedin.com/in/jcvega-cyber-colonel/ • @teamvega

TRACK 2 • *Consumer Electronic Security Systems: Not that secure… still* / Our homes provide a place to store our personal belongings and secure them against theft. That's one of the reasons why we have locks and security devices. Since these are protecting our belongings, and our families, these should be secure from most people being able to break in and act in a criminal manner. Many of the Professional Security Systems are exceptionally vulnerable to very simple attacks. The presentation will show how to render moot these professional security systems using four different sample systems and $110 of equipment easily purchased online. The procedure is so easy, even a caveman can do it. Also, we re-tested an updated system for one manufacture, which was still a failure. The manufacturers have been contacted several times as part of the responsible disclosure protocol.

- CHARLES PARKER II, Sr. Information Systems Security Researcher, Stephenson Technologies Corp.

TRACK 3 • *Your Cybersecurity Career, Matched & Mapped* / This demo will provide you with the keys to a successful cybersecurity career. You'll be provided the opportunity to find your best matched cybersecurity work role based on your interests and personality traits. You'll learn about the four core elements of a successful cybersecurity career which are: Certifications, Experience, Training, and Education.

This presentation will show you, your personalized cybersecurity career pathway which is a systematic way of when and which type of certifications, experience, training, and education to pursue throughout your career based on your matched role. This demo will include showing you where to search and apply for jobs on platforms where recruiters are hiring as the pathways are mapped to LinkedIn, Indeed, and ZipRecruiter. This session will also show you how your matched role maps to the NIST NICE Framework.

After this talk audience members will understand that there is a place for everyone on the cybersecurity team and learn that you don't have to know how to code or be good at math to have a successful cybersecurity career.

Link to how mycyberpath.com works: https://youtu.be/b8rE3UzhuNc

- JASON SHOCKEY, Founder & CEO, My Cyber Path
  https://www.linkedin.com/in/jason-shockey/

2PM PRESENTATIONS

TRACK 1 • *TBD*

- Rich Lindberg, CISO, JAMS
  https://www.linkedin.com/in/skippy/

TRACK 2 • *Do we live in a simulation? Could we tell? Could we hack it?* / Some posit that we all live in a simulation. The Matrix, of sorts. It would need to be a massively complex system with incalculable resources. But, is it possible? Being that we are inside this system, is there any way to tell if it is a simulation? Could we detect a glitch? If this is a simulation, then the code would be the laws of nature, as scientists attempt to find 'theory of everything'. It will take a physicist to decompile the source code of the universe!

- DR. JOHN D. JOHNSON, President, Docent Institute
  https://www.linkedin.com/in/nullsession/ • @johndjohnson
- PARKER SCHMITT, CEO, NetThunder
  https://www.linkedin.com/in/parker-schmitt-netthunder/ • @parkerschmitt

TRACK 3 • *Intro to Bluetooth Low Energy Hacking* / This talk will introduce the audience to the world of Bluetooth Low Energy (BLE) security from an IoT pentester's perspective. The number of IoT devices using BLE is exploding due to its low power consumption and support on all modern mobile devices. We will give an overview of the BLE protocol and the history of BLE encryption. Then, we will discuss different methods of capturing BLE communications and connecting and interacting with BLE devices. Finally, we will demonstrate reading data from a BLE heart rate monitor. **This session may exceed 1 hour.**

- MATT BROWN, Sr. Security Analyst, Independent Security Evaluators (ISE)
  https://www.linkedin.com/in/matt-brown-149198237 • @nmatt0

3PM PRESENTATIONS

TRACK 1 • *The Cat in the IRC Chat – Intersection of OPSEC & Deception* / Both OPSEC and deception are absolutely essential. Always look for opportunities to balance these two

disciplines by weaving together their capabilities, thereby obfuscating the truth and controlling the narrative.

- DR. GREGORY CARPENTER, CSO, KnowledgeBridge International https://www.linkedin.com/in/dr-g-carpenter-cism-imagineer/ • @gscarp12

TRACK 2 • *Equity and Diversity in Cybersecurity* / Even with a decade of work, the numbers are still dismal. Twenty-four percent of all cybersecurity employees are women, thirteen percent Black, and five percent Hispanic. The odds are even bleaker for women of color. What is being done, and what can be done to resolve this gap and fill the increasing number of open jobs in the cyber fields?

- ROBERTA OSMERS, Associate Professor, Lead Faculty EICC Cyber Center https://www.linkedin.com/in/roberta-osmers-8627763/ • @robbi61

4PM PRESENTATIONS

TRACK 1 • Creative *Security Awareness in the Enterprise*

- KATHRYN BRETT GOLDMAN, CEO, Cybermaniacs https://www.linkedin.com/in/kathrynbrettgoldman/

TRACK 2 • *TBD*

- TBD

5PM CLOSING CEREMONY AND DOOR PRIZES • TRACK 1

6:30PM to Midnight

"The Bill Murray After Party"

Open to all ticket holders, kids & adults. Bring your badge! Unlimited free tokens, pizza & open bar! @ Analog Arcade Bar, 302 N Brady St., Davenport, IA (2 blocks from RiverCenter)

Co-Sponsored by: Cybereason