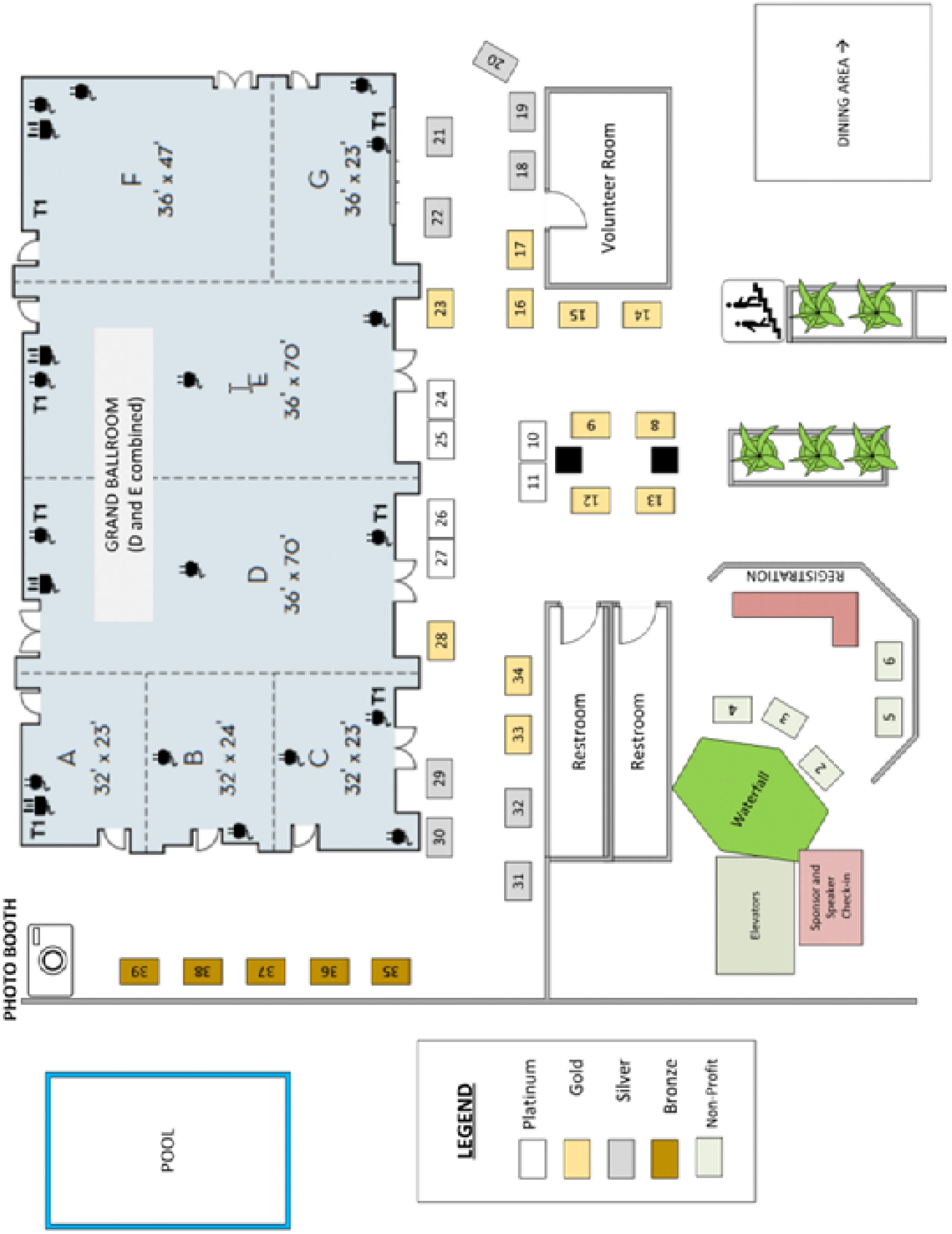
B-SIDES TAMPA

February 29, 2020

Embassy Suites - USF

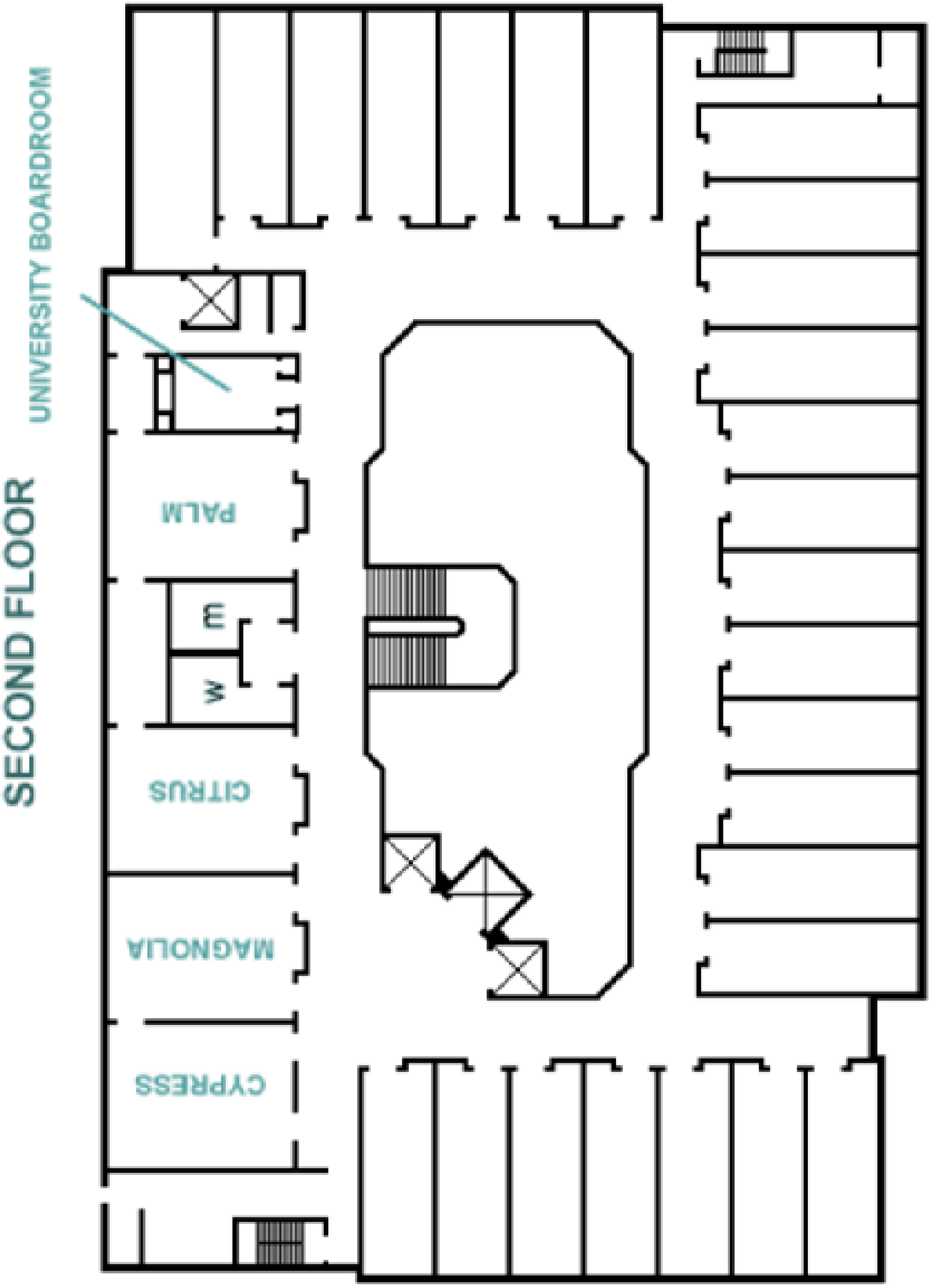
FLOOR 1_


GRAND BALLROOM
(D and E combined)
F
36' x 47'
G
36' x 23'
E
36' x 70'
D
36' x 70'
A
32' x 23'
B
32' x 24'
C
32' x 23'
T1
20
19
18
17
16
21
22
23
24
25
26
27
28
15
14
10
11
9
8
12
13
29
30
31
32
33
34
Volunteer Room
DINING AREA →
Restroom
Restroom
REGISTRATION
6
5
4
3
2
Waterfall
Elevators
Sponsor and Speaker Check-in
PHOTO BOOTH
39
38
37
36
35
POOL
LEGEND
Platinum
Gold
Silver
Bronze
Non-Profit

FLOOR 2_

EMBASSY SUITES HOTEL TAMPA - USF / NEAR BUSCH GARDENS

SECOND FLOOR



FRYDAY_

Palm Room

9 AM - 6 PM Brad Duncan: Malware Traffic Analysis

Magnolia Room

9 AM - 6 PM Kerry Hazeltone Cloud Forensic

Boardroom

1 PM - 4 PM Jenn S & Darren: BioHacking Workshop (tDCS)

Citrus Room

9 AM - 6 PM Joe Gray: OSINT (Open Source Intellegence)

Waterfall

6 PM - 9 PM Volunteer and Speaker Dinner

Hotel Administration Office

Noon - 6 PM Early Registration

SATURDAY_

B-SIDES TAMPA SPEAKER SCHEDULE_

8:30 - 10:00 **Opening Keynote NOT RECORDED**
Rachel Wilson From the NSA to Wall Street: A Cybersecurity Career Journey

Track A - NOT RECORDED

10:15 - 11:00 Mila Paul
How does blockchain secure Alice and Bob

11:15 - 12:00 Mike Orenchuk
Cyber security, compliance and changing the tone

12:15 - 1:00 Nathan Hamiel
Technical debt and tears: Attacking and defending AI

1:15 - 2:00 Filip Chytry
IoT vulnerabilities in Tampa Bay 2019

2:15 - 3:00 EVil Kat
IoT Device Security (Honeypots)

3:15 - 4:00 Ashley Newsome | Ayush Enkhtaivan
Critical Infrastructure: The future impact of Industry 4.0 on the Security of Healthcare

Track B

10:15 - 11:00 Allan Liska
Turn down for RaaS: Seperating hype from reality in the ransomware as a service market

11:15 - 12:00 Ben Rollin and Johnny Macluf
Sucess with Defense in depth. From the perspective of a Red Teamer

12:15 - 1:00 Julien Vehent
A DevSecOps approach to bringing security beyond the security team

1:15 - 2:00 David Switzer
RF for Red Team
Modern Day Vandals

2:15 - 3:00 Vanessa Ferguson
The Ethics of Data Collection

3:15 - 4:00 David Dillard
Practical crypto review for developers

Track C - NOT RECORDED
Cloud Track

10:15 - 11:00	Karen Gispanski - Cloud Security Alliance Shift Left
11:15 - 12:00	Ravi Devineni Automating Security Compliance at Scale
12:15 - 1:00	Michael Brooks Norbert Dereg GRC in the Cloud
1:15 - 2:00	Michael Melone Cloudy with a Chance of Adversaries - Common Mistakes in Cloud Security
2:15 - 3:00	Justin Leapline Security on Cloud 9
3:15 - 4:00	Robert Carvajal Controlling the Rain in Cloud

Track D

10:15 - 11:00	Alyssa Miller Losing our reality: Understanding and combating the deep fake threat
11:15 - 12:00	Casey Martin Network gravity: Exploring a enterprise network
12:15 - 1:00	Jeremy Rasmussen Post Quantum Crypto
1:15 - 2:00	Hardik Parekh - OWASP SAMM
2:15 - 3:00	Ira Winkler Stopping Cyberboom : Mitigating User error
3:15 - 4:00	Will Baggett Broken Arrow

Track E

10:15 - 11:00	Joff Thyer/Mike Felch Offensive Python for PenTester
11:15 - 12:00	William York | Thomas Slota | HTTP Covert channel using only HTML/CSS
12:15 - 1:00	Charles Herring Breaking NBAD and UEBA detection
1:15 - 2:00	Derek Banks | Beau Bullock | Ralph May How to ARM yourself
2:15 - 3:00	Jacob Baines Is that a WiFi sniffer in your pocket?
3:15 - 4:00	Chris Lyne / Nicholas Miles Extracting an ELF from an ESP32

Track F
CISO Track

10:15 - 11:00	Sallie Wright : IT 2020 Talent Trends - The Six Trends
11:15 - 12:00	Larry Whiteside : 21st Century CISO
12:15 - 1:00	Dave Summit : So you want to be a CISO!?
1:15 - 2:00	John Burger Optimizing Security Operations
2:15 - 3:00	CISO Panel Peter Rucys, Sherri Vollick, Deborah Steele, Sally Wright, Ryan Gutwin, Larry Whiteside Jr.,
3:15 - 4:00	CISO Panel Peter Rucys, Sherri Vollick, Deborah Steele, Sally Wright, Ryan Gutwin, Larry Whiteside Jr.,

Track G
Villages

10:15 - 4:00	Lock Pick Village / Tampa Hackerspace / Bio-Hacking Village / DC-813”

SECOND FLOOR

Palm Room
Career Workshops

10:15 - 12:00	Gina Yacone : Seat at the Table: Security Leadership Through Tabletop Exercises
12:15 - 2:00	**BREAK**
2:15 - 4:00	Resume Review and Career Coaching 2-4 PM

Citrus Room
Career Track

10:15 - 11:00	Kirsten Robin Renner Navigating to a better job in infosec
11:15 - 12:00	Leo Pate Offense From Defense - My Rocky Path to the Dark Side
12:15 - 1:00	**BREAK**
1:15 - 2:00	Recruiter Panel : How not to Gamble with Your Job Search
2:15 - 3:00	Laura Malave and Julia Meyer Prepare for Cybersecurity Industry certification success!

Magnolia Room

10:15 - 11:00	Alex Kirk : Using Bro/Zeek Data for IR and Threat Hunting
11:15 - 12:00	Erich Kron Cyber Defense In The Modern Org: 6 Low-Cost Tips To Secure Your Organization
12:15 - 1:00	Nikita Mazurov and Kenny Brown Tracking the Online Harassment Chain
1:15 - 2:00	Gideon Rasmussen Designing a 3rd party Risk Management Program
2:15 - 3:00	Anshu Gupta Mobile Application Security - What you need to know?
3:15 - 4:00	Kevin Kaminski Dude, Where's My Log? The Unknown Logging Gaps in Your Environment, Why You Didn't Detect that Pentest, and What to Do About It

Cypress Room
Workshops

10:15 - 11:00	Suzanne Ricci Enhancing Your Career in Cybersecurity
11:15 - 12:00	BREAK
12:15 - 2:00	Secure Code Warrior Tournament: The Ultimate Secure Coding Throw Down

USF Connect

10:15 - 4:00	All Day (10-4) for CTF

Hotel Administration Office

10:15 - 4:00	Mental Health Hackers

4:14 - 5:30

Closing Keynote
Rhett Greenhagen
Attacking the Data Before the Decision

PRESNTORS LIST_

From the NSA to Wall Street: A Cybersecurity Career Journey

Opening Keynote
8:30 - 10:00

Rachel Wilson

In her riveting keynote, Rachel will describe her career path as a cybersecurity professional and the lessons she learned along the way. She will detail the challenges and opportunities of transitioning from the closed world of NSA to the profit-driven world of Wall Street. She will explain the current cybersecurity threats facing companies and institutions from nation states like North Korea and Iran, from cyber organized crime syndicates, and from individual hackers looking to make money or create mayhem. With advanced hacking tools now widely available, Rachel will explain how cyber actors target companies, institutions and individuals in an opportunistic way and then work to monetize their access. Drawing from her experience at the NSA and in the financial sector, she will discuss what cybersecurity professionals need to be considering in the current cyber risk environment and describe the aspects of an effective corporate cyber resiliency strategy. From cyber governance and strategy, to cybersecurity technology investment, to the recruitment and retention of cybersecurity professionals, Rachel will cover the landscape of challenges facing today's cyber professional and provide practical, practitioner-level advice on how to build a cyber resilient organization.

Rachel Wilson spent 15 years at the National Security Agency (NSA) where she ran counterterrorism operations, worked cybersecurity threats to the 2012 summer Olympics in London, and spent five years leading NSA's cyber exploitation operations mission. As the senior committing official for NSA's hacking mission, she oversaw the planning and execution of thousand of cyber operations against America's adversaries. In the spring of 2017, Rachel became the first Head of Cybersecurity for Morgan Stanley Wealth Management. In this role, she leverages her experience in attacking and defending high-consequence systems to protect Morgan Stanley and its clients from cyber actors.

How does the blockchain secure Alain and Bob

Track A
10:15 - 11:00

Mila Paul

We keep hearing about how secure Blockchain is but why is it? Why is Blockchain considered a high integrity solution for data?

In a world of insecure networking protocols like BGP and TCP/IP, the Cypherpunks integrated cryptography to secure network transmission and speak freely on the internet. Despite aggressive pushback, their efforts included a solution to the global economy based on cryptography: electronic cash. A Centralized electronic cash solution beginning in 1980 led to the ultimate disruption by Satoshi Nakomoto's decentralized Bitcoin core in 2008 that became impossible to shut down. I will summarize the five cryptographic algorithms that make up Bitcoin core security and explore current picks for future blockchain algorithms in light of cryptanalysis and quantum cryptography to maintain our right to privacy and anonymity.

***Mila Paul** is adjunct faculty in Computer and Cyber Sciences and also has courses for certificates for secure web development and blockchain on Openclassrooms.com and Amesite.com. Her interest in cybersecurity began in her work as a defense contractor in the Middle East for twelve years. Now she enjoys teaching, blockchain startups and music production.*

Mike Orenchuk

Cyber Security, Compliance and changing the tone

Track A
11:15 - 12:00

Mike Orenchuk, former CIO of GuideWell Source, and executive at Blue Cross Blue Shield of Florida, is currently an executive security strategist for Vartai Security, who will account his experience of leading three of the largest processors of Medicare claims totaling over 100 billion in claims payments per year, through a rigorous undertaking to maintain and mature cybersecurity while adhering to the highest level of Federal requirements.

Michael Orenchuk is the executive security strategist for Vartai Security. He has over 35 years of broad IT experience in numerous senior leadership roles in healthcare, banking and telecommunications.
Mike was previously the CISO at Florida Blue and the CIO at GuideWell Source, a Medicare Administrative Contractor that processes 32% of the nation's Medicare Part A & B claims serving 401,000 Medicare providers. GuideWell Source has 3,000+ users in seven states processing 375 million claims per year worth $107 billion in claims payments per year.
At GuideWell Source Mike led the transformation of his company's Cybersecurity Program from last place nationally among all MAC contractors to first place for four consecutive years, as measured by an annual independent third party audit.
Mike is now dedicated to improving our client's Cybersecurity Programs as he did for his previous employers.

Nathan Hamiel

Technical Debt and Tears : Attacking and Defending AI

Track A
12:15 - 1:00

You can't go anywhere these days without being bombarded with the initials A.I. The marketing hype is high, and so are the promises. Industry reports, TV commercials, and countless other sources tell you if your company isn't using AI, you will lose out. The truth is, not everything is a good use case for AI, but we are getting it anyway. These systems hide invisible complexity that decreases visibility and increases technical debt, and this scenario isn't some far off problem for the future. Today, we have autonomous systems churning away, making critical decisions that we have no choice but to trust. A scary situation since these systems are fragile and fail in unexpected ways. Great for attackers, bad for security.

Many organizations are developing or purchasing solutions that use machine learning, deep learning, NLP, or similar discipline. It's also a safe bet that security isn't a consideration in their development. After all, software development and model development are different, and after some time, you might not be getting what you paid for. It's essential for security professionals to have a baseline understanding of these concepts so they can adequately defend them. In this presentation, we'll look at this new attack surface, how it can be attacked, as well as tools and techniques you can use to defend your autonomous systems. We may not be able to stop the onslaught of black boxes propagating through our organizations, but with the right amount of knowledge and preparation, we can lower the attack surface.

***Nathan Hamiel** is Head of Cybersecurity Research at Kudelski Security, an international security company providing innovative and tailored solutions to enterprises and public-sector clients. Nathan works in the innovation group defining the future of services and products for the company. A security veteran with a strong focus on software security,* *he has spent his nearly 20-year career helping customers around the world solve complex security challenges.*

Nathan is a regular public speaker and has presented his research at global security events, including Black Hat, DEF CON, HOPE, ShmooCon, SecTor, ToorCon, and many others. He is also a member of the Black Hat review board, where he evaluates research for inclusion in the various conferences around the world.

IoT Vulnerabilities in Tampa Bay

Track A
1:15 - 2:00

Filip Chytry

Possible live demonstration of device hacking using some of the latest vulnerabilities and devices. We can focus on the IoT problems within Tampa Bay as there are plenty of unprotected devices visible to attackers. The outcome should be general knowledge of the problem in here + how to protect your self and your home.

*As the threat intelligence director at Avast, **Filip** hacks and conducts experiments to illustrate the dangers of unsecured devices. He even crusades for cyber security in his free time, helping nonprofits stay safe in an insecure world.*

IoT Device Security (Honeypots)

Track A
2:15 - 3:00

Kat Fitzgerald

You've heard of IoT Security and probably even sat through a talk or two. This presentation brings a new level of applying IoT Honeypots to the mix of detection, defending and protecting unsecured IoT devices Using this technique, I recently caught an "appliance" scanning my home network. Luckily my honeypot detected it. Would you know if one of your appliances was actually trying to attack from within?

***Kat Fitzgerald** (@rnbwkat or evilkat@rnbwmail.com)*
@BsidesChicago / bsideschicago.org - Lead Organizer since 2017

First DEFCON was DC 3 (1995) with 16 speakers! In other words, I have been doing this for a very long time, with an emphasis on Security Operations, Incident Response and Purple Teams.

Based in Philidelphia and a natural creature of winter, you can typically find me sipping Casa Noble Anejo whilst simultaneously defending my systems using OSS, magic spells and Dancing Flamingos against a barrage of attackers. Honeypots are one of my favorite technologies, although they are now called "deceptive technologies" - and I find that they provide much more actual "threat intel" than most $ services.whilst simultaneously defending my systems using OSS, magic spells and Dancing Flamingos against a barrage of attackers. Honeypots are one of my favorite technologies, although they are now called "deceptive technologies" - and I find that they provide much more actual "threat intel" than most $ services.

Critical Infrastructure: The future impact of Industry 4.0 on the Security of Healthcare

Track A
3:15 - 4:00

Ashley Newsome

Ayush Enkhtaivan

As technology advances and becomes more integrated into health care, more data is collected. How that data is stored and used may vary slightly from institution to institution; and there are standards in place to maintain the security of the mass amounts of collected data. In 2003, the Federal Government established the Healthcare and Public Health (HPH) Sector as one of the critical infrastructure sectors in the United States, by doing so, it represents that its security the utmost importance to the national security, the economy, and public health and safety (dhs.gov). Critical Infrastructure describes the body of networks and the physical and cyber systems that are vital to the United State's economy and physical, and public health and safety.

With the advancements and integration of technology in critical infrastructure, the digitization of healthcare, the need for physical and cyber security, and the increase in big data, the development and move to industry 4.0 has increased. Industry 4.0, which ties together security (cyber and physical), big data, cyber physical systems, robotics, integration, IoT/ IIoT, cloud computing, and more.

The HPH sector requires resilience and security as it holds a significant position in national security, the economy, and public health and safety. Telehealth, robotics, IoT, mobile health systems and applications, among other data collecting and internet connected aspects of healthcare are involved in Industry 4.0. This paper explores healthcare as a critical infrastructure and how the movement of critical infrastructure to Industry 4.0 will affect the future and security of healthcare.

Ashley Newsome *is a senior at the University of Tampa (UT) majoring in Cyber Security and double minoring in Business Analytics and Management Information Systems (MIS). Throughout her academic career at UT, Ashley has conducted and presented three research projects discussing Botnets, SCADA systems, and now IoT and healthcare at various conferences. Her interest in research peaked during her 2.5-year experience as a student employee in UT's Information Technology department. Her experience and interest have led her to a career in a hybrid space of in Linux systems, application administration/dev-ops, and emerging technology, upon graduation*

Ayush Enkhtaivan *comes from Ulaanbaatar, Mongolia and she currently finishing up her M.S in Cybersecurity at The University of Tampa. Ayush holds an MBA in Finance from Gannon University and a B.E. from the University of International Business and Economics in Beijing, China. She has been previously employed by one of the Big 4 and has years of experience working in Marketing, Foreign Trade, and Finance, locally and internationally.*

Turn down for RaaS: Seperating hype from reality in the ransomware as a service market

Track B
10:15 - 11:00

Allan Liska

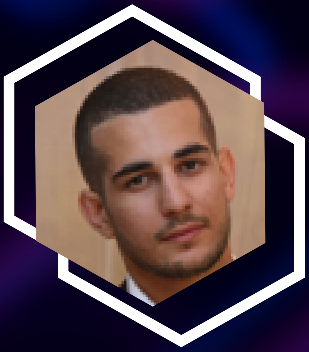
The open source Zeek network security monitor provides valuable data for incident responders and threat hunters alike. This talk will discuss how to use that data to lower the time necessary to find attackers on your network, as well as ways that advanced users can take Zeek's scripting language to create powerful, flexible detection logic that goes beyond traditional point-in-time IDS signatures.

Allan Liska is an intelligence analyst at Recorded Future. Allan has more than 15 years' experience in information security and has worked as both a blue teamer and a red teamer for the intelligence community and the private sector. Allan has helped countless organizations improve their security posture using more effective and integrated intelligence. Allan is also one of the organizers of BSides Bordeaux and has presented at security conferences around the world. He is the author of The Practice of Network Security, Building an Intelligence-Led Security Program, and Securing NTP: A Quickstart Guide and the co-author of DNS Security: Defending the Domain Name System and Ransomware: Defending Against Digital Extortion.

Sucess with Defense in Debth. FRom the perspective of a Red Teamer

Track B
11:15 - 12:00

Ben Rollin



Johnny Macluf

The commoditized use of the term "defense-in-depth" has brought a lack of understanding for how truly effective certain security controls can be when compared to expensive products which promise the world, and yet consistently fail to deliver. In this presentation we will provide a deeper look at fundamental controls that consistently limit Red Team penetration footholds and escalation attempts which are not based on fancy or expensive security products.

Networks should be thought of as onions in terms of the distribution of security controls in place to effectively combat cyber-threats. The use of stage 1, stage 2 and stage 3 proactive controls may be effectively circumvented by one attack method. This real-world fact requires organizations to employ different types of compensating controls, such as robust types of monitoring which fundamentally increase the likelihood that attacks will be detected or completely mitigated.

Some topics that will be covered to understand the layered defense model are
- The EDR and AV false sense of security. Secure your system as if there was no EDR or AV. - MITM network reconnaissance, preventing IPv4 and IPv6 relay attack.
- Using network segmentation as a literal "onion of defense".
- System Lifecycle challenges and addressing legacy operational states.
- Cloud migration challenges as companies require dual operational security methodologies.
- Active Directory security issues.
- Asset Management and Configuration Management.
- Using the principle of least function and least privilege throughout the SDLC.

Ben Rollin *is the founder of Vartai Security, LLC and has a decade of information security consulting experience focusing on technical IT Audit, risk assessments, web application security assessments and network penetration testing against large enterprise environments. Ben has worked as a consultant for a "Big 4" audit firm performing a wide range of information security consulting activities including IT controls audits, vulnerability and risk assessments, security program review, web application security assessments, and penetration testing. Ben has assisted state/local and federal government agencies such as the Department of Health and Human Services, the Department of Homeland Security, the United States Air Force, and the state of Maryland with complex information security needs. He also has aided private sector companies in a variety of industries (such as Finance, Healthcare, and Retail) with their information security and compliance programs.*

Ben has a Bachelors' Degree in Business Administration, as well as several industry certifications including Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Offensive Security Certified Expert (OSCE), Offensive Security Certified Professional (OSCP), eLearnSecurity Certified Professional Penetration Tester (eCPPT), eLearnSecurity Certified Web Application Penetration Tester (eWPT), and eLearnSecurity Advanced Web Application Penetration Tester (eWPTX). Ben is active in the information security community and has developed a number of hands-on technical training materials for online learning platforms targeting beginner to advanced level security practitioners globally. Ben has delivered hands-on training in a competition format both domestically and abroad, including an offensive security training exercise for the Greek Ministry of Defense in Athens, Greece. Most recently Ben has been involved as the key architect of the technical exercises for the EY Asia-Pacific Cyber Challenge, a two-day event in Hong Kong consisting of teams from universities from throughout the Asia-Pacific region. Ben has a strong interest in Active Directory security and focuses time on research in this area as well as remaining current with the latest tactics, techniques, and procedures (TTPs).

Johnny Macluf *is an ex-military Information Security Consultant with over a decade of experience and has performed multiple in-depth technical testing assessments. He has sound knowledge of network and application security, inter-networking and techniques, tactics and procedures of cyber-attacks. Johnny has assisted government agencies and a variety of private sector companies across varying industries in improving their security posture. Johnny is a specialist in red team operations but has also performed a wide range of information security assessments such as Vulnerability Assessments, Source Code Review, Network Penetration Testing, Web Application Testing, Incident Response, Reverse Engineering, and Architecture Review.*

Johnny has a master's degree in Software Engineering and holds several industry certifications such as Microsoft Certified Solutions Expert (MCSE), Cisco Certified Network Associate (CCNA), Checkpoint Certified Security Administrator (CCSA), Offensive Security Certified Expert (OSCE), Offensive Security Certified Professional (OSCP), eLearnSecurity Certified Professional Penetration Tester (eCPPT), and Certified Penetration Tester eXtreme (eCPTX).

Furthermore, Johnny has led and executed numerous red team operations as well as maturity assessments and social engineering engagements across the globe. In addition to his role as a red teamer, Johnny served as a guest lecturer for the Israeli government and universities as well as CheckPoint Israel. Outside of consulting, Johnny is heavily focused on Active Directory research and developing custom tools to benefit both red and blue team operations.

A DevSecOps approach to bringing security beyond the security team

Track B
12:15 - 1:00

Julien Vehent

What if operations teams defended their perimeters perfectly? What if developers always implemented the best security controls? What if product managers always made decisions based on a complete understanding of security risks? What if organizations were so good at security, that the security team no longer needed to exist? In this keynote, Julien explores the idea of using modern techniques, culture shifts and devops principles to grow a security-first culture in your organization. He reflects on years of maturing, improving and socializing the security strategy of Firefox at Mozilla, and shares examples and stories of bringing security beyond the security team.

***Julien** is responsible for the operational security of Firefox's backend infrastructure at Mozilla. He is the author of Securing DevOps, published at Manning Ed, and a developer of various defensive security tools. Julien can be found on twitter and github at @jvehent.*

RF for Red Team Modern Day Vandals

Track B
1:15 - 2:00

David Switzer

This would go over current Wifi attacks (both attacking clients and networks), as well as wireless attacks on mice/keyboards (both the old “”mousejack”” and more modern “Logitacker” style attacks), as well as monitoring other systems for physical attacks, such as IoT/smart devices, alarm systems and power meters.

- Wifi
- General overview
- Network attacks
- Client attacks
- PMKID cracking
- Mousejacking and derivatives
- IoT / Smart devices

- Popular Comm
- Cell
- Pagers
- Misc
- Alarm systems
- Power meters”

***David E. Switzer** has over 20 years of experience in systems and network security. Cert alphabet soup: GSE #136, G[cia|cih|awn|sec|stuff]), OSCE, CISSP and ITILv3 (keeps it gangsta). He currently is working on RF/IoT and ICS/SCADA projects for his employer, while off time amusements include RF, wireless networks, hardware hacking, and other expensive time sinks.*

The Ethics of Data Collection

Track B
2:15 - 3:00

Vanessa Ferguson

The financial and reputational harms associated with data breaches or unauthorized disclosures of consumers information can be fatal for small and medium-sized businesses. However, implementing ethical collection practices can build trust between the consumers and the company, thereby softening the damages associated with data breaches or unauthorized disclosures of consumer data. Using collection limitations and allowing consumers to provide their informed consent before collecting data are two of many ways to ensure a business is engaging in ethical data collection practices.

In this presentation, Vanessa will elaborate on the importance of engaging in ethical data collection practices and explain how to use collection limitations and obtain informed consent from your clients or customers.

Vanessa Ferguson *is an attorney and advocate for consumer privacy rights. She obtained her Bachelor's Degree from the University of South Florida St Petersburg and her Juris Doctor Degree from the University of Dayton School of Law. Ms. Ferguson is a Certified Information Privacy Technologist (CIPT) and can assist companies in the development, engineering, deployment, and auditing of their IoT products and services. Ms. Ferguson is also the managing director of Ferguson Legal, PLLC, a Florida law firm that focuses on data protection. Ms. Ferguson takes pride in providing affordable legal services to small and medium-sized businesses to ensure they can address their business needs and privacy concerns within their budget.*

Practical Crypto Review for Developers

Track B
3:15 - 4:00

David Dillard

Cryptography is hard. It's hard because there are often a number of mistakes a developer can make when writing cryptographic code, but there's no easy way for the developer to look at the ciphertext or use unit tests to know that he made any mistakes. As long as the data can be correctly decrypted the developer usually assumes everything is fine, when in fact there may be issues that a knowledgeable attacker could take advantage of to recover the plaintext data. The easiest way to find such issues is to review how the crypto was done, but what should someone look for in such a review?

This presentation will cover both common and not so common mistakes made with crypto I've encountered when performing crypto reviews and that have otherwise been made public, e.g. in news articles, blogs posts or CVEs. It will give attendees a number of practical things they can look for in performing crypto reviews of their own software. Examples of topics that will be covered include random number generation, the use of salts, salt generation, key generation, key derivation, IV generation, nonce generation and why developers should prefer AEAD ciphers.

David *has worked as a software professional for over 30 years. The first part of his career was spent developing mass storage software. During this time he represented several employers in storage related standards organizations, primarily the Storage Networking Industry Association (SNIA). For the last ten years he's been involved in application security, including five years in the product security group at Symantec. In his current position he focuses primarily on the management of third party software and cryptography.*

Shift Left

Track C
10:15 - 11:00

Karen Gispanski

Shift Left on Cloud Security

Organizations have adopted cloud computing to benefit from the promise of decreased cost, better scalability, and improve agility. Cloud service providers are expanding security features and protections, but security has and will continue to be the customer's responsibility to secure their data within the cloud environments.

We will discuss what is and what is not working for security operations teams in security cloud data, applications, and services in a shared responsibility model.

The top three areas of concern are:
Data loss and leakage
Unauthorized access through misuse or misconfiguration
Compliance and lack of visibility into infrastructure protections

How do we shift left on security postures and strategies to address deficiencies of legacy security tools to protect assets in the cloud environments?

__Karen Gispanski__ is the Global Business Information Security Officer at The Nielsen Company. She leads an executive committee to reduce Cyber Security risk through establishing a business risk program, standard operating practices and costs objectives. Karen is a thought leader that is called upon to analyze risks, while serving as a strategic business partner for technology and business teams.

Karen has held various security leadership roles, managing both employees and third party contractors across dispersed geographic locations. Her experience crosses multiple industries such as managed security services, financial, healthcare, manufacturing and consulting. Karen has successfully implemented and managed global enterprise solutions, built out security operations, incident responseteams, and e-discovery programs for Fortune 500 organizations. She is well-versed in security compliance and risk management programs and has facilitated credentials such as PCI, ISO 27001, and SOC 2 certifications.

Karen is committed to utilizing her expertise in Cyber Security and has served on boards for over seventeen years as a Cyber Security expert. Her board service includes: Cloud Security Alliance, Center for Cyber Safety and Education, Jacksonville Infragard Members Alliance and Jacksonville FBI Citizens Academy.

Automating Security Compliance at Scale

Track C
11:15 - 12:00

Ravi Devineni

Information security and compliance are becoming critical to businesses, especially after the Equifax breach. Financial services companies are no longer willing to compromise on security, especially when deploying services onto the cloud. In this talk, you'll learn a few techniques which we've implemented to automate compliance and use fast feedback loops to implement security as a part of CI/CD.

__Ravi Devineni__ is a Director of Engineering at Northwestern Mutual for a team responsible for DevOps and CI/CD tooling for the whole enterprise.

Previously Ravi worked at companies like Amplify/Oracle holding variety of roles including Developer, Architect, Database Administrator, Engineering Manager.

GRC in the Cloud

Track C
12:15 - 1:00

Michael Brooks

Joint presentation on GRC in the cloud and how effective and secure solutions can be implemented across multiple cloud environments to protect your data and enable your business.

Presentation objectives:

- Explain how an effective GRC framework can be implemented across cloud service providers (Azure, AWS, GCP)
- Explain how a solid GRC strategy can help secure cloud environments, reduce cyber risk and increase business performance
- Demonstrate proper GRC implementation within several different cloud environments (actual solutions)

Presentation Overview:
What is Cloud Security?
The Value of GRC
What right looks like
Lessons Learned
Tips to remember

Norbert Dereg

Michael Brooks *is a security and compliance executive with over 20 years of experience in developing, implementing, and operating cybersecurity programs for the Department of Defense and private sector clients in numerous industries. He is a retired Air Force officer with experience as both a Chief Information Officer and Chief Information Security Officer. Mike holds an MBA from American Military University and is also a credentialed Certified Information Systems Security Professional (CISSP) and Project Management Professional (PMP).*

Norbert Dereg *is a Cyber security professional with extensive background in the emerging world of Cloud Service Providers (CSPs). Norbert has taken his primary skills of being both an Architect & DevOps professional into the world of Cyber security where he is now creating and developing continuous compliance programs that include; drift-detection, self-healing and guardrails enforcement.*

Cloudy with a Chance of Adversaries – Common Mistakes in Cloud Security

Track C
1:15 - 2:00

Michael Melone

Migrating services to the cloud can provide a wealth of security benefits – if done correctly. Targeted attacks pose unique challenges from both a defensive forensic perspective if not designed correctly. Join Michael on a journey through some of the common mistakes encountered by the Microsoft Detection and Response Team (DaRT) team during targeted attack incident response investigation recovery.

Michael Melone *is a cybersecurity professional with over 20 years of experience. For the past seven years, Michael has been performing incident response and recovery consulting on DaRT – Microsoft's customer-facing targeted attack incident response team. In his time on DaRT, he has led the design and development of their internal threat hunting platform, designed the process used by Microsoft Services to recover customer enterprises after a targeted attack breach, and consulted for companies across the globe in most major industry verticals. Michael holds a Master of Science degree specializing in Information Assurance and Security as well as CISSP certification, and is the author of the book "Think Like a Hacker: A Sysadmin's Guide to Cybersecurity".*

Justin Leapline

Security on Cloud 9

Track C
2:15 - 3:00

Using cloud service providers has been a growing trend over the years, as most companies are leveraging their services to streamline their infrastructure needs. As this trend grows, many security professionals struggle to layer the organization’s compliance obligations and security needs into these environments effectively. Whether you need to comply with a standard (PCI, NIST, FFIEC, etc.) or protect your assets in the cloud, several controls need to be implemented and monitored for the desired appropriate levels. Then when you layer in various new delivery/ hosting models and development methodologies, it can turn complicated very fast.

During this talk, we are going to be exploring the various activities needed to be done to implement excellent security practices and appropriate oversight into this environment, including:

* How to clearly define responsibilities between the cloud service provider and your organization.
* Understand the different hosting models (IaaS, PaaS, Serverless, etc.) and how that affects your oversight responsibilities.
* Discuss the impact of using different technologies (containers/serverless) and processes (DevOps, CI/CD).
* Implementing segmentation controls with container technologies (Docker/Kubernetes).
* How automate and effectively monitor your compliance status in the cloud.

Justin *has over twenty years of experience in system administration, software development, and information security. His core skills include regulatory and contractual compliance, program management, payment card standards, and general governance practices and frameworks. He is the founder of episki, a cloud-based governance tool geared to help smaller organizations manage their security programs, an IANS faculty member, and serves as a Principal Consultant at TrustedSec.*

Before his current roles, Justin consulted with Fortune 1000 companies in information systems, audit, governance, and information security. He has led the governance and security practices for prominent eCommerce and large financial services companies. Additionally, Justin has spoken at conferences concerning risk management, payment card industry (PCI), security leadership, and general information security practices.

Robert Carvajal

Controlling the Rain in Cloud

Track C
3:15 - 4:00

The cloud is our new reality and the traditional security perimeter is gone. Our job as security professionals is to evolve and adapt to the changing landscape. Shadow IT operations are becoming more rampant; leveraging the cloud as an enabler. We will discuss the common threat vectors for the cloud, and best practices to secure cloud data, applications, and services.
-- Identity and Access Management (IAM)
-- Networking Services (Network Security Groups and Load Balancers)
-- Shadow IT
How do you leverage years of IT practices and security principles to secure the cloud? Are there parallels to transition existing knowledge to accomplish the same objectives? What are the key differences? Part of this presentation will include reviewing slides of a solution capable of monitoring/enforcing Cloud Security and Governance.

Robert Carvajal *is a Cybersecurity veteran with over 15 years experience in Cybersecurity. He is currently the Director of Threat and Vulnerability Management at The Nielsen Company; which specializes in Big Data collection of how people consume media, and how they purchase consumer goods. He currently leads a geographically disparate team that works on securing Mergers and Acquisitions, leading tabletop exercises and purple/red team engagements, and is responsible for overall Attack Surface Reduction; which includes Cyber Threat Intelligence and Vulnerability Management. He started his career in Cybersecurity working at the University of Miami where he was responsible for implementing enterprise security controls across Endpoint, Network, and Data vertices. He designed and managed traditional solutions such as FW, IPS, VPN, Anti-Virus, and network based physical security devices. Additionally, he led incident response activities that included forensic investigations and e-Discovery; engaging with General Counsel and local law enforcement.*

He went on to work for an MSSP provider that served several Fortune 500 companies. This role expanded his exposure to multiple industries with different regulatory compliance requirements including: PCI, HIPAA, FISMA, and SOX. He led and assisted in the accreditation of PCI, SOC, and ISO certifications. He designed product services, operations SOPs, and incident response processes while managing multiple SOC locations that encompassed security administrators, engineers, and incident response analysts that were responsible for delivering services. Before joining Nielsen, Robert led the creation of a sustainable SIEM content development program and ongoing tuning processes, as well as Threat Intelligence integrations within multiple SIEM platforms to provide high-fidelity alerts to clients. Robert’s experience in cloud started years ago when deploying and migrating security solutions in the cloud for customers. His role at Nielsen has shifted his focus from deploying and configuring in the cloud to implementing standards, monitoring compliance, and remediating issues in cloud security best practices. Robert Carvajal graduated from Northeastern University with a Bachelor’s of Science degree in Criminal Justice. He obtained and has maintained his CISSP certification since 2007.

Loosing our Reality: Understanding and combating the deep fake threat

Track D
10:15 - 11:00

Alyssa Miller

As a result of continuing advancements in AI, deep fake media has become increasingly convincing and easy to produce. Experts have warned of the impact this could have on elections and personal security. However, the threats that deep fakes pose to businesses and global markets are receiving less attention and are therefore not as well understood.

This session will analyze both the societal as well as the business threats that we as security experts must consider. Threat vectors in terms of election and market manipulation, insider trading, extortion and theft of intellectual property will be presented and analyzed. Psychological research into the effects of disinformation campaigns will also be leveraged to provide further context regarding the full potential impact of these threats.

However, while the erosion of our ability to trust what's real can seem scary, researchers have been working to counteract these threats. Various low-tech as well as AI based solutions are being developed to help detect deep fake media. These will be analyzed to show their promise as well as their limitations. Additionally, research into possible countermeasures to help prevent deep fake creation will also be analyzed.

Alyssa Miller *is a hacker, security evangelist, cyber security professional and public speaker with almost 15 years of experience in the security industry. She has always had a passion for deconstructing technology, particularly since buying her first computer at the age of 12 teaching herself BASIC programming. In her career, Alyssa has performed all forms of security assessments but given her developer background, she had a dedication to application security. She currently specializes in working with business and security leaders to design and deploy effective security programs that strengthen enterprise security strategy.*
Alyssa is also committed to evangelizing security. Not only does she speak internationally at various industry, vendor and corporate events, Alyssa also engages in the community through her online content, media appearances, and security community activism. Her journey through security was recently featured in an article by Cybercrime Magazine. She's also been recognized in Peerlyst's e-Book "50 Influential Penetration Testers". Alyssa is treasurer and member of the board for Women of Security (WoSEC) and is an Application Security Advocate for London-based Snyk Ltd.

Network gravity: Exploiring a enterprise network

Track D
11:15 - 12:00

Casey Martin

Enterprise networks are often complex, hard to understand, and worst of all - undocumented. Few organizations have network diagrams and asset management systems and even fewer organizations have those that are effective and up to date.

Leveraging an organization's SIEM or logging solution, network diagrams and asset inventories can be extrapolated from this data through the 'gravity' of the network. Similar to our solar system and galaxy, even if you cannot confirm or physically see an object, you can measure the forces of gravity it exerts on the observable objects around it that we do know about. For example, unconfirmed endpoints can be enumerated by the authentication activity they register on known domain controllers. The inferred list of endpoints and their network addresses can begin to map out logical networks. The unpolished list of logical networks can be mapped against known egress points to identify physical networks and potentially identify undiscovered egress points and the technologies that exist at the egress points.

As more objects are extrapolated and inferred, the more accurate the model of your enterprise network will become.

Through this iterative and repeatable process, network diagrams and asset inventories can be drafted, further explored, refined, and ultimately managed. Even the weakest of observable forces can create fingerprints that security professionals can leverage to more effectively become guardians of the galaxy.

Casey Martin *is an information security professional with a curiosity for enabling blue team operations. Casey has operated in all technical aspects of security operations as well as leading the customer enablement effort as the Director of Security Operations for some of the worlds most trusted brands. In his current role, Casey leads the Threat Management function at his organization which engages him in innovative functions such as SOC research and development, threat intelligence, and red team operations. Prior to moving to Tampa, Casey held security roles in the energy and educational sectors which was made possible through his education at the Rochester Institute of Technology.*

Post-Quantum Cryptography for Dummies

Track D
12:15 - 1:00

Jeremy Rasmussen

Quantum computing allows complex problems to be solved exponentially quicker than what is currently available with classical computing. For several years now, we have been warned that a quantum computing breakthrough is just around the corner. Now, with Google’s recent “quantum supremacy” announcement, researchers have shown that it’s possible to solve a complex mathematical calculation in about 3 minutes for which a supercomputer would take 10,000 years. So, are we on the verge of a Y2K-like event involving quantum computers breaking all of our popular public-key cryptographic systems, such as RSA, which form the basis of many of our authentication, key exchange/distribution, VPN, and even blockchain systems? Mathematicians and computer scientists are on the clock now to do the following: - Quickly improve the efficiency of post-quantum cryptography. Build confidence and consensus in the methods of post-quantum cryptography. Improve the usability of post-quantum cryptography in widely-deployed crypto systems.
In this talk, we’ll review basic concepts of cryptography, complexity theory, and quantum computing. We’ll then delve into the next generation of cryptographic algorithms that appear to have attributes resisting quantum-computing attacks. Such algorithms include hash-based cryptography, code-based cryptography, lattice-based cryptography, and multivariate cryptography. My intent is to put these in laypeople’s terms as much as possible. Finally, we will discuss practical application of these concepts in the next generation of crypto systems. This talk will not address quantum cryptography, which is a different subject altogether.

Jeremy Rasmussen *is CTO/CISO of Abacode, a company that provides managed cybersecurity & compliance advisory services to businesses across all industries. He is also an adjunct professor at the University of South Florida and founder of the USF Whitehatters Computer Security Club (WCSC). Since 2000, he has taught courses in cryptography & network security, ethical hacking, digital forensics & investigations, and mobile & wireless security. For 25+ years, he has performed R&D of cyber solutions for government and commercial customers. Jeremy is a CISSP (No. 11762) and CEH. He was named 2017 Tampa Bay Technology Leader of the Year.*

OWASP SAMM

Track D
1:15 - 2:00

Hardik Parekh

OWASP SAMM (https://owaspsamm.org) is the prime maturity model for software assurance that provides an effective and measurable way for all types of organizations to analyze and improve their software security posture. Building security into the software development and management practices of a company can be a daunting task. There are many elements to the equation: company risk profile, organizational structure, different stakeholders, technology stacks, tools and processes, and so forth. Implementing software assurance will have a significant impact on the organization.

OWASP Software Assurance Maturity Model (SAMM) gives you an effective and measurable way for all types of organizations to analyze and improve their software security posture in 3 levels of maturity - thus creating a step-by-step software assurance navigation plan. It enables you to formulate and implement a strategy for software security that is tailored to the risk profile of your organization. In this talk, we give an overview of the new release of the SAMM model. After 10 years since its first conception, it was important to align it with today's development practices. We will cover a number of topics in the talk: (i) the core structure of the model, which was redesigned and extended to align with modern development practices, (ii) the measurement model which was setup to cover both coverage and quality and (iii) the new security practice streams where the SAMM activities are grouped in maturity levels. We will demonstrate the new SAMM2 toolbox to measure the maturity of an example DevOps team and how you can create a roadmap of activities.v

***Hardik Parekh** is recognized thought leader and executive in security/privacy domain with contributions to SANS CWE Top 25, OWASP SAMM, BSIMM 1.0 to BSIMM 9; and SAFECode. Hardik is part of the core team which developed OWASP SAMM 2.0.*

Hardik has 16+ years of security leadership experience with a track record of developing and maturing security programs in consumer and enterprise companies RSA/EMC, Intuit, Amazon, and Splunk. Hardik has built security programs in dynamic, fast-paced environments while leading highly technical globally distributed security teams focused on application security, hardware security, security operations, threat and vulnerability management, security architecture, AWS security, and tools development.

Hardik has transformed DevOps organization to DevSecOps by integrating security engineering tools in CICD pipeline and delivered security at scale and speed in the journey to AWS migration.
Hardik was invited to speak at Global AppSec conference 2019.
Hardik also serves on advisory board of several security start ups and CompTIA.

Stopping Cyberboom: Mitiaging User error

Track D
2:15 - 3:00

Ira Winkler

The most devastating attacks predominantly begin with some form of user action. A user clicks on a phishing message. A user goes to a malicious website. A user puts a malicious USB drive on their system. Etc. The commonly recommended solution is more and better awareness, which doesn't account at all for malicious users. This is like saying that if a canary die in a coal mine, you need to find healthier canaries.

The fundamental problem is not a lack of awareness, but that users have the ability to initiate a loss. What is therefore required is a methodology that involves analyzing where the ability to initiate the loss comes from, stopping the initiation of the loss, and then mitigating the potential loss before it is initiated. This is what counterterrorism, safety, and accounting practitioners do in their professions. It is time for the cybersecurity profession to realize that a user action, error or not, is just the proximity of where the loss becomes visible. Addressing the proximity of the loss does not address the root cause of the loss, or the failure to mitigate that loss.

This presentation adopts counterterrorism principle and will walk attendees through a comprehensive program to determine the source of losses, and determining how to prevent, detect, and respond to potential losses. Case studies will be included.

Ira Winkler, *CISSP, is the Lead Security Principal for Trustwave and Author of Advanced Persistent Security, and the forthcoming book, You Can Stop Stupid. He is considered one of the world's most influential security professionals and was named "The Awareness Crusader" by CSO magazine in receiving their CSO COMPASS Award. He has designed and implemented and supported security awareness programs at organizations of all sizes, in all industries, around the world. Ira began his career at the National Security Agency, where he served in various roles as an Intelligence and Computer Systems Analyst. He has since served in other positions supporting the cybersecurity programs in organizations of all sizes.*

Broken Arrow

Track D
3:15 - 4:00

Will Baggett

Friends and family often look us as members of the InfoSec community for guidance. "Fix my computer" has become "fix my situation." I will discuss applying InfoSec principles and also forensic principles to assisting domestic abuse victims cutting the electronic cord to their abuser. Members of the audience will receive methods to provide triage for the victim and granular examples of how social engineering can lead to the unwitting installation of monitoring software. I will discuss applying the counterintelligence mindset to the domestic situation- what can be gathered, what sources and methods can be used against a person in their own house and how to detect the threats. The talk will discuss the use of social media to detect physical surveillance, technical countermeasures for surveillance devices, lessons learned with forensics...and the ways to protect oneself against leaving data behind. As a certified fraud examiner, I discuss implied consent and implied trust for online finances and the need to cull access lists.

Former CIA SME for iOS and Mac Forensics, NATO SOF cyber trainer and volunteer of many BSides conferences. I have presented to NATO HQS, DefCon 2019, BSides Las Vegas, and BSides Detroit. I am a senior cybersecurity consultant at Revolutionary Security and a forensic analyst for Operation Safe Escape.

Joff Thyer

Mike Felch

Offensive Python for Pentesters

Track E
10:15 - 11:00

This talk will focus on the many different ways that a penetration tester, or Red Teamer can leverage the Python programming language during offensive operations. Python is a rich and powerful programming language which above all else allows a competent developer to very quickly write new tools that might start as a Proof of Concept, but soon become an invaluable addition to the Red Teamer's tool-belt. Having the skills to both generate new tools, and modify existing tools on the fly is critically important to agility during testing engagement. Everything from utility processing of data, network protocol, API interaction, and exploit development can be rapidly developed due to the high functionality level and intuitive nature of Python.

Joff Thyer *has been a penetration tester and security analyst with Black Hills Information Security since 2013. Prior to joining the InfoSec world, he had a long career in the IT industry as a systems administrator and an enterprise network architect. He has an Associate's in Computer Science, a B.S. in Mathematics, and an M.S. in Computer Science, as well as several certifications (listed below). The best part of a penetration test for Joff is developing sophisticated malware that tackles defensive solutions, ultimately delivering exciting wins for company engagements. He has extensive experience covering intrusion prevention/detection systems, infrastructure defense, vulnerability analysis, defense bypass, source code analysis, and exploit research. When Joff isn't working or co-hosting the Security Weekly podcast, he enjoys making music and woodworking.*

Michael Felch *joined Black Hills Information Security in 2017 and is a Senior Penetration Tester and Red Team Leader. Since beginning his career in IT as a Linux Administrator he has evolved along with the technology to hold offensive security, software development, and hardware/ software security research roles.*

William York

HTTP Covert channel using only HTML/CSS

Track E
11:15 - 12:00

A covert channel is a secretive communication channel that can bypass traditional security measures. They provide a means of communicating through mechanisms that are not intended for communication. In this paper, we propose a covert channel that utilizes only HTML and the CSS hover feature to transmit messages. To do this, we create a website with our covert channel on a web page and develop a tool that converts a plain ASCII message to hex, and based on the CSS hover locations, control the mouse to move to the hover locations. A manual implementation of this was explored. However, the manual transmission had a larger margin for error compared to program-driven mouse control. The covert channel takes advantage of the fact that this is a new CSS only mouse-tracking technique using the hover feature, which can bypass common tracking protections. The covert channel is hidden to blend in with the background of any given web page. Our results show that we can reliably transmit a message at a rate of 13 bytes per second utilizing the mouse control transmission tool.

William York *is a student at RIT finishing my Bachelors degree in Computer Science and a Masters in Computer Security, graduating May 2020. Have done four work tours with the Department of Defense as a Software Engineer.*

HTTP Covert channel using only HTML/CSS

Track E
11:15 - 12:00

Thomas Slota

Thomas Slota *received a Bachelor’s Degree from Rochester Institute of Technology in Computing Security in the Spring of 2019. Completed 3 Internships at Leidos Corporation focusing on Software Defined Networking. Currently I am a first year Computing Security Masters student at Rochester Institute of Technology with a focus in Malware.*

Breaking NBAD and UEBA detection

Track E
12:15 - 1:00

Charles Herring

Network Behavior Anomaly Detection (NBAD) and User and Entity Behavior Analytics (UEBA) are heralded as machine learning fueled messiahs for finding advanced attacks. The data collection and processing methodologies of these approaches create a series of new exploitable vectors that can allow attackers to navigate network and systems undetected. In this session, methods for poisoning data, transforming calculations and preventing alerts will be examined. Proof of concept Python code will be demonstrated and made available. Approaches to harden against these attacks will also be discussed as well as outlining needed changes in detection standards.

Charles’ *dedication to maturing the craft of InfoSec is built on a diverse career path across the industry. He started his career in InfoSec in the US Navy in 2002 serving as the Network Security Officer at the US Naval Postgraduate School. After leaving active duty, he was a contributing product reviewer for InfoWorld magazine focusing on network security products. Charles spent 7 years running Herring Consulting, a company dedicated to process orchestration, data sharing, and marketing. In 2012, Charles joined the Lancope team as a pre-sales engineer, promoted to Consulting Security Architect and later as Strategic Account Manager following the acquisition of Lancope by Cisco. In 2014, Charles partnered with veterans of the military, law enforcement and cybersecurity to research new approaches to improve the craft of cybersecurity operations. In 2016, that research resulted in the forming of WitFoo. When not working with cybersecurity heroes, Charles enjoys SCUBA divining with his wife, Mai.*

How to ARM yourself

Track E
1:15 - 2:00

Beau Bullock

You’re on your first physical pentest, you’ve gained access to the data center, now what do you do? One of the best options for to demonstrate how physical security failings can bleed over into the digital breach world is to use a Pentest Dropbox - a small IOT physical digital implant device that can be used as an attack platform against the client’s infrastructure. You could buy an expensive prebuilt device and they have their place. But that’s not the best you can do, hacker. Come learn how we built a variety of custom Pentest Dropbox and IOT devices to help us out on our engagements. We will include parts lists, build instructions, software choices, and custom scripts that you can use to build your own evil IOT devices.

How to ARM yourself

Track E
1:15 - 2:00

Derek Banks

__Beau Bullock__ is a Senior Security Analyst and Penetration Tester and has been with Black Hills Information Security since 2014. Beau has a multitude of security certifications and maintains his extensive skills by routinely taking training, learning as much as he can from his peers, and researching topics that he lacks knowledge in. He is a constant contributor to the infosec community by authoring open-source tools, writing blogs, and frequently speaking at conferences and on webcasts.

__Derek Banks__ has been a security analyst and penetration tester for Black Hills Information Security since 2014, but he has been a part of the IT industry for his entire career. Since graduating college with a BS in Computer Information Systems, Derek has explored many different Information Technology jobs, from working at a help desk to being a network and systems administrator. He has experience in forensics, incident response, creating custom host and network-based monitoring solutions, penetration testing, vulnerability analysis, and threat modeling. Derek's favorite aspects of working at BHIS include learning from his coworkers and helping customers better their security posture. When he isn't participating in CtF competitions or red team engagements, Derek enjoys spending time with his family, staying physically fit, and playing the bass guitar.

Ralph May

__Ralph May__ has six years of professional experience in information security and over 10 years in Information Technology (IT). Ralph has conducted security assessments that include components such as physical security, social engineering, internal/external network and application penetration testing, wireless assessments and Advance Persistent Threat (APT) actor simulations. Ralph currently leads the A&P breach team which focuses on advanced treat actor simulations and breach war games. Ralph is active in the security community and has spoken at multiple security conferences including Blackhat. Ralph is an Army veteran serving various levels within the federal government as both a service member and contractor.

Is that a WiFi sniffer in your pocket?

Track E
2:15 - 3:00

Jacob Baines

Wardriving and warwalking have long been a favorite pastime of hackers. But the concerned stares and furrowed brows that follow you down the street when your laptop is in hand and your antennas are flying proudly can be disconcerting. To avoid this unwanted attention, I decided I needed a WiFi sniffer that could easily fit in my pocket. A tool that I could tuck away, but also had a display if I wanted to use it. Of course, it would also have to let me control the monitored channel, capture EAPOL packets, write pcaps, and log GPS locations.

After looking around, I found no such device seemed to exist. So I made my own. In this talk, I'll share my Raspberry Pi Zero build out and show you how to cheaply make your own pocket sized WiFi sniffer.

__Jacob__ is the founding member of Tenable's Zero Day Research team. He spends most of his research time on routers and custom protocols. Sometimes he even finds bugs.

Chris Lyne

Extracting an ELF from an ESP32

Track E
3:15 - 4:00

The Espressif ESP32 is a system on a chip (SoC) engineered for mobile devices, wearable electronics and IoT applications. It provides Wi-Fi and Bluetooth LE which makes it great for products needing wireless capabilities. While researching a consumer product, we discovered an ESP32 being used to provide Wi-Fi connectivity to the device. We found that there was limited tooling available to facilitate the reverse engineering process of an ESP32 firmware image. So, we decided to create tooling of our own. We will talk about how we went about creating our tooling to extract an ELF file from an ESP32 flash dump. With excruciating amounts of detail, we will discuss the binary format of ESP32 firmware images as well as the process of converting it to an ELF file. By the end of the talk, you will know how to go from flash dump all the way to control flow graph in IDA.

Chris *enjoys dissecting complex applications and lives for the hunt. Despite having deep roots in software development, his true passion is security. An avid learner, Chris is continuously evolving his skills, capabilities and methodologies. Chris believes any problem can be solved with knowledge, intelligent decisions, and sheer grit.*

Nicholas Miles

Nick *joined Tenable as a Research Manager in 2011. He has written hundreds of Nessus plugins and developed several core libraries used in the Nessus engine. He now leads the company’s Zero Day Research team. In his free time, Nick likes model aircraft, metalworking and breaking out his telescope on clear nights.*

IT 2020 Talent Trends – The Six Trends

Track F
(CISO Track)
10:15 - 11:00

Sallie Wright

The ware for talent is here, and organizations are losing the battle. With IT unemployment at record lows, IT departments must find new ways to set themselves apart to stay competitive. This presentation will highlight the six IT talent management trends, including new strategies and tools to explore.

Sallie Wright *– Chief Information Officer BIO She. brings over 30 years of experience in information technology leadership. She is currently the CIO & Executive Counselor for Info-Tech Research Group where she is a CIO’s CIO. Prior to joining Info-Tech she was the CIO for Fulton County Government where she oversaw the IT Department of Georgia’s largest county and provided guidance for technology decisions. She previously served as Deputy Chief Information Officer for Georgia State University and held executive roles at the University of Alabama at Birmingham, the University of North Carolina and within the private sector. Her specialty areas include IT strategic planning, enterprise infrastructure, and information technology security and privacy.*

Sallie Wright is an active member of the technology community within the Atlanta region. She was a top 5 finalist for 2018 Georgia CIO of the Year for the Public/Non-Profit Sector as well as the 2018 Atlanta Technology Professionals Leadership Impact Award. She serves on multiple well respected boards and committees notably, Atlanta Technology Professionals Executive Advisory Board, Technology Association of Georgia Public Diversity and Inclusion Board, Georgia State University Graduate School Mentoring Program, Georgia Piedmont Technical College Computer Information Systems Advisory Committee, Power My Learning Greater Atlanta Regional Board and CISO Executive Council. In 2018 she also served on Georgia State University Robinson School of Business CIS Board, Kettering Executive Women Board of Directors, Governors Computer Information

Systems Technology Advisory Committee, and Governors IT Task Force. Ms. Wright is also a member of the Georgia CIO Leadership Association (GCLA) and a mentor for students of the Georgia State University Robinson School of Business since 2013. Following her induction to the Pink Tech Hall of Fame in 2015, she was nominated CIO of the Year in 2016 and 2017.

Sallie holds a master's degree in management, a bachelor's of science in business administration, and is a CISSP.

Larry Whiteside

21st Century CISO

Track F (CISO Track)
11:15 - 12:00

Debunking the fiction versus reality of the CISO role.

Larry Whiteside Jr. *is the founder and CEO at Whiteside Security and Trusted Advisor, Cybersecurity at Presidio. He has 25+ years experience in building and running cybersecurity programs, holding positions as Chief Security Officer and Chief Information Security Officer in multiple industries including DoD, Federal Government, Financial Services, Healthcare, and Critical Infrastructure.*

Since 2009, Larry has advised several corporate security executives and companies across the cybersecurity industry on how to make Cyber Security a number one objective to their business. He has helped CEOs and board members of private cybersecurity companies achieve their goals in sales, marketing, and customer retention.

Larry is a Co-Founder and VP, and on the Board of Directors at the International Consortium of Minority Cybersecurity Professionals (ICMCP), a 501(c)3 non-profit association that is dedicated to the academic and professional success of female and minority cyber security students and professionals.

A thought leader in the industry with extensive experience presenting at conferences such as the Gartner Security Summit, RSA Conference and SC World Congress, Larry has been featured in many articles relating to information security and risk management.
Larry received his Bachelor of Science degree in computer science at Huston-Tillotson University.

Dave Summit

So you want to be a CISO!?

Track F (CISO Track)
12:15 - 1:00

A recent ISC2 survey stated that 65% of Cyber security professionals struggle to define their career paths. This is not surprising, given the wide range of areas that makes up the cyber field. For those who are exploring or are entering management with the intent of becoming a Chief Information Security Officer, this topic will explore the pros and cons. The CISO can take a lot of bumps and bruises along the way to often unrecognized victories. Taking blame for issues, uncooperative users and leaders, and when things go wrong, unfortunate negative attention. But the rewards can be worth it. This session will be a candid discussion of topics from successes to failures, necessary skills, the "what-to-do" and "what-not-to-do" will be shared. If you think you have what it takes or don't know what it takes but are interested in CISO career path, this would be a good session to attend.

Dave *is the Chief Information Security Officer at the H. Lee Moffitt Cancer Center and Research Institute in Tampa, Florida. His passion for technology and cyber security continues through his 35 years of experience in information technology. Dave's experience crosses federal and private sectors. A 21 year federal career with the Department of Defense preceded his entry into Healthcare security,* *in which he has been actively engaged in for the past 10 years. Dave earned his undergraduate degree in Information Systems Management from the University of South Florida and his Masters in Information Security with a Digital Forensics concentration from Norwich University. He is as a fellow with the Institute of Critical Infrastructure Technology (ICIT) a national cyber security think tank, a member on the Forbes Technology Council and serves as an adviser to the Center for Cyber Safety and Education. For the past two years, Dave has been identified as one of the "Hospital and Health System CISOs to know" by Becker's Hospital review. Awards include 2017 ISE Southeast Executive of the Year finalist, 2017 ISE Southeast People's Choice award and 2019 ISE Southeast Executive of the Year nominee. More recently, he has had the honor of providing congressional testimony over the security implications to healthcare operations with phone spoofing and robocalls.*

Dave speaks at various Cyber Security events throughout the country on topics ranging from building security teams and cyber awareness to roles and responsibilities of CISOs as well as providing recommendations and insights into cyber threats and incident response.

Optimizing Security Operations

Track F
(CISO Track)
1:15 - 2:00

John Burger

Barely a few decades old, the information security profession is nascent when compared to many other professions such as the legal or medical professions, both with origins tracing back to ancient Greco-Roman empires. Centuries old, these professions have not only established standard norms of behavior and performance, they have also matured a standard taxonomy which has been essential for the evolution of these professions, as progress cannot be achieved without a "common understanding". In contrast, very few standard terms of reference have been defined within our security profession. The purpose of this brief is to propose a standard taxonomy of key terms and best practices workflow to optimize modern Security Operations Centers (SOCs). Using standard terms, it will cover topics such as False positive management, tuning and setting targets relative to risk, Introduce the concept of Anomalous Safe Alerts and setting targets relative to risk, Typical false negative (unseen attack) scenarios and root causes, Optimizing the balance between alert types, True Positive Impact Analysis and Incident Response. The goal is to achieve a common understanding of terms and best practices to facilitate SOC program maturity. Moreover, strategically, as the pace of threat innovation has continued to accelerate, it is equally imperative that we endeavor to speed the progress of our profession in like fashion.

COL (retired) ***John Burger serves*** *ReliaQuest as the Chief Information Security Officer (CISO) and Head of IT Infrastructure. Prior to joining ReliaQuest, he served 27 years in multiple assignments including the CISO at the United States Central Command from 2010-2012. As the CISO, he directed the efforts of four (4) advanced HUNT teams, integrated with the National Security agency, to protect and defend a global network of over 1+ million devices in the middle east supports Operation Iraqi Freedom and the War on Terror. In 2012, he was selected as the Chief of Cyber Warfare (Joint Cyber Center), where he directed the cyber-attacks in Afghanistan, Iraq, and the planning for offensive cyber operations against Iran.*

CISO Panel

Track F
(CISO Track)
2:15 - 4:00

Deborah Steele

A panel discussion which invites you to learn how the role of Chief Information Security Officer (CISO) has changed in the age of data breaches and high-profile cyber-attacks. The panel discussion will include several well-known CISOs for an interactive panel conversation where they will discuss various topics, such as :

- **How the role of CISO has changed over time.**
- **Top challenges for CISOs**
- **Dealing with stress and pressure associated with the role**
- **What keeps CISOs up at night**
- **much more**

Deborah Steele: *I am the VP of Information Technology and Cyber Security at Fox News Network. I've been with Foxnews since its inception in 1996. Prior to this I attended The Copper Union for the Advancement of Science and Art and then went on to get a master's in criminal justice with the specialization in cybercrime. I've held just about every job within IT. I've led the company's Information Technology Infrastructure organization where I was responsible for developing and maintaining network, computing, server, storage, collaboration and infrastructure solutions across the enterprise. In this role I provide leadership for the continued development of an innovative, robust, and secure information technology environment. I've been involved in every aspect of IT with focus around building and supporting our broadcast operation. I am member of WITI and was appointed to USF's Cybersecurity Certificate Program Advisory Committee.*

Peter Rucys

Hello, I am ***Pete Rucys****, CISO for Tampa General Hospital, driven by curiosity, due diligence, and continuous education. I started my career in IT after serving in the US Air Force, where the area of Information Assurance was beginning to gain ground and grab my attention. While living in Chicago, I worked for American National Can, Axiom, and RR Donnelly & Sons as a network engineer. The focus of security in organizations at the time was in its infancy, because of this I was able to learn how important core security principles were vital to doing business and how real the threats were. I migrated to Tampa, FL; employed by JP Morgan and eventually the Air Force, again, in the capacity of a Computer Network Defense Manager. There it became real, very quickly. I was able to visually see the threats, visualize the big picture of security, and learn from some of the best our country has to offer. I brought these tools to Tampa General Hospital, hired as the first dedicated network security engineer the organization has ever had. Through supportive leadership, my predecessor and I were able to start a security program from the ground up, implementing controls I had learned from my previous employments. Not only is this program protecting the hospital, it is protecting a community that is dependent on the expert care that TGH provides. The satisfaction that I receive from my work that is protecting one of the largest hospitals in Florida is immeasurable.*

Ryan Gutwein

Ryan *is an information security risk leader that works as a Security Director For Ignyte and provides high-level consulting to DoD and Defense Health Agency (DHA). As a senior level risk manager, Ryan manages and automates several types of risk assessments leveraging latest technologies and tools. Ryan has served as a security officer for many organizations and is currently a board member of ISACA (Tampa). Ryan's experience is formally supplemented by several industry certifications and extensive experience working in complex environments like defense.*

Sherri Vollick

CISO Panel

Track F (CISO Track)
2:15 - 4:00

Sherri *has over 19 years of experience in Risk Management and Security Operations in professional services firms. She is responsible for the development, execution, management and delivery of her firm's information security and governance program, overseeing all aspects of information security, including program development, security operations, physical security, vendor risk management, business continuity and incident response.*

Gina Yacone

Seat at the Table: Security Leadership Through Tabletop Exercises

Palm Room (Workshop)
10:15 - 12:00

Imagine that your organization is infected with ransomware what do you do? From a critical breach to a minor incident, your organization's success lies in the speed of detection, effectiveness in containment, and accuracy of remediation. As an IT and security professional, you are on the front line. How should you prepare?

Tabletop exercises are an effective mechanism to shape, enhance and test the awareness of decision makers, and the gamification of the exercise yields a higher level of engagement of participants. Participants of this session will:
- Learn the key components of an effective tabletop exercise.
- Understand the tabletop exercise process through the perspective of all participants (from the facilitator to shareholder).
- Appreciate why tabletop exercises increase operational resilience, and improve security effectiveness and efficiency.
- Learn how to create a high ROI by conducting tabletop exercises.
- Work through a few tabletop exercises to learn how to be a facilitator.

Learning Objectives:
1. Learn the key components of an effective tabletop exercise.
2. Understand the tabletop exercise process through the perspective of all participants (from the facilitator to shareholder).
3. Appreciate why tabletop exercises increase operational resilience and improve security effectiveness and efficiency.
4. Learn how to create a high ROI by conducting tabletop exercises.
5. Work through a few tabletop exercises to learn how to be a facilitator.
6. Learn to create an incident response kit.
7. Determine what pieces to the puzzle are missing in a faux company's processes.
8. Become a Dungeon Master!

Gina Yacone *is a cybersecurity consultant and vCISO with Agio. Gina is an information security strategist and speaker with a unique technical vision and business acumen. She is responsible for educating organizations about the ever-changing cybersecurity landscape and helping them build a dynamic cybersecurity program. She loves focusing on the unique challenges today's organizations face.*

Gina is an active member in the local North Carolina chapters of ISSA, ISC2, Security + Beers, DefCon919 and OakCity Lock Sports. Gina sits on the board for Women in Cybersecurity (WiCyS) North Carolina, Tweens & Technology, BsidesRDU as well as the Information Services Advisory Board for the Town of Cary.

Kirsten Renner

Navigating to a better job InfoSec

Citrus Room
(Career Track)
10:15 - 11:00

In a sea of job postings, recruiters and hiring managers, how can you be your own best advocate to land the right next role for yourself?

How will you search, network, apply and interview?

I will offer my opinion based on decades of experience, having conducted thousands of interviews and placed many information security professionals.

First we'll discuss:
- The best searching and networking techniques (where do I look, who do I connect with and how)
- Then the most effective resume writing (how should I format, why is no one responding, what about keywords)
- And finally interviewing techniques, to include salary negotiations! (what research to do and questions to ask, how to answer questions, do I tell you my current salary, do I deserve a sign-on bonus, what's the going range)

***Kirsten** is the Sr Director of Recruiting at Novetta, an advanced analytics and full spectrum cyber security company. She studied HR Management at University of Maryland. After a short while working as a software developer, then help desk manager, she combined her love for technology and HR by becoming a Technical Recruiter and has been doing so for over 20 years. For the last decade, Kirsten has been primarily supporting the Information Security field, and is best known in the community for her volunteer activities especially her involvement in the Car Hacking Village from its inception!*

Leo Pate

Offense From Defense : My Rocky Path to the Dark Side

Citrus Room
(Career Track)
11:15 - 12:00

Many security professionals live in one of two worlds; offense or defense. While there is a rise of offense and defense collaboration, more often than not, these two worlds are often silo'd. This talk will focus on how I made the jump from IT to defensive security, to offensive security and the lessons learned along the way. By citing real case studies over the past 11 years, I will show how IT, coding, defense and offense security §are all woven together and how skills in one, sharpens the others.

***Leo Pate** is an Application Security Consultant at nVisium and a former Cyber Warfare Officer within the South Carolina National Guard. Leo's expertise in information security, analysis and R&D comes from 12 years experience in a wide-variety of information technology and business roles to include security systems administrator, security consultant and other information security specific functions. Leo is also a technical mentor for NodeCarolinas, a non-profit organization focusing on teaching information technology, application and network security, digital forensics and response and open-source intelligence to the communities of North and South Carolina.*

Laura Malave

Julia Meyer

Prepare for Cybersecurity Industry certification success!

Citus Room
(Career Track)
2:15 - 3:00

Prepare for Cybersecurity Industry certification success! Save yourself from being overwhelmed. Learn proven strategies college students use to get ready for an industry certification and succeed.

Cybersecurity industry certifications such as CompTIA Security+ are important for validating technical skills, helping students, career changers, and veterans gain entry-level positions, and helping industry professionals position themselves for the next level in their careers. This presentation is designed for students, working professionals, veterans, and career changers interested in learning about current entry and mid-level Cybersecurity Industry certifications and best practices for certification success.

Participants will learn strategies for increased success in Cybersecurity Industry Certifications. Strategies used to prepare students will be shared as many of these same strategies are also applicable to working professional seeking to self-study for industry certifications for career growth. Tools and techniques to be shared include the results and recommendations of Test Prep technical tools and books, and support activities/systems such as CTFs and cybersecurity competitions. Common Cybersecurity Industry Certification study challenges such as time management skills, student study skills, and tips for successful studying will also be addressed. We will also provide an overview of current entry and mid-level Cybersecurity industry certifications such as: CompTIA Security+, EC-Council Certified Ethical Hacker, and Cisco CCNA Cybersecurity Operati

Laura Malavé *has a Master of Science in Computer Science from the University of South Florida. She has over 15 years of Computer & Information Technology College teaching experience.*
Laura joining St. Petersburg College in July 2015 as Academic Chair for the Midtown and Downtown campuses, leading the Certificate and Associates in Cybersecurity. Prior to SPC, she taught at Hillsborough Community College and Keiser University Tampa Campus.
Laura has numerous industry certifications including: GIAC GSEC, CompTIA CySA+, Security+, Network+, A+, EC-Council Certified Ethical Hacker, MOS, and MTAs, and is a member of the SANS Advisor Board.
Laura is is an active member of ISC2 Tampa Bay, and a volunteer and committee team lead for the BSides Tampa Conference.
Laura is the advisor to the SPC Cybersecurity club, TitanSec, in which students actively participates in online, and local Capture the Flag competitions, and attend local conferences and industry events.
Laura received the 2016 League of Innovation Excellence Awards in Teaching and Learning in the category of: Innovation in the Use of Technology. She has been awarded three grants: NSF-ATE Grant Application Co-PI, Biomedical Engineering & Cybersecurity, SPC Innovation Grant 2016, Digital Forensics & Cybersecurity Lab, and SPC Titan Achievement Grant, TitanSec Cybersecurity Escape Room. She led the initiative to have the SPC Associates Degree in Cybersecurity to be designated as an NSA Cybersecurity Center of Academic Excellence in Two-Year Education (October 2019). She has served as a Cybersecurity subject matter expert for regional newspaper articles, and television.
She is also a member of the HSI, Homeland Security Investigations, 2018 Citizens Academy, and the FBI Fall 2019 Citizens Academy.

Julia *is a sunshine state native, who was ready for something completely different after 10-years in corporate hospitality and administrative management. That led her back to her alma mater, St. Petersburg College. Now having worked exclusively with Career & Technical Education students for the last five years, she has used her experience in operations and education in sustainability management, to create supportive processes within the colleges growing industry certification program. She takes pride in holistically leading her students to success. When she is not helping them land jobs before graduation by getting certified, she is at home with her fiancé tending to her (many) plants and animals*

Alex Kirk

Using Bro/Zeek Data for IR and Threat Hunting

Magnolia Room
10:15 - 11:00

The open source Zeek network security monitor provides valuable data for incident responders and threat hunters alike. This talk will discuss how to use that data to lower the time necessary to find attackers on your network, as well as ways that advanced users can take Zeek's scripting language to create powerful, flexible detection logic that goes beyond traditional point-in-time IDS signatures.

***Alex** is a veteran open source security evangelist with a deep engineering background. In 10 years with Sourcefire Research (VRT), he wrote the team's first malware sandbox and established its global customer outreach and intelligence sharing program. He has spoken at conferences across the globe on topics from "Malware Mythbusting" to "Using Bro/Zeek Data for IR and Threat Hunting", and was a contributing author for "Practical Intrusion Analysis", and oft-used textbook for university courses on IDS.*

Erich Kron

Cyber Defense In The Modern Org: 6 Low-Cost Tips To Secure Your Organization

Magnolia Room
11:15 - 12:00

Cybersecurity is often expensive, time-consuming and can have catastrophic consequences if done wrong. From scams designed to steal money to attacks designed to disrupt business and bring production to a halt, attackers have been upping their game continuously.

In the meantime, the security vendor's marketing departments relentlessly try to sell the latest and greatest "solution" to our problems with catchy ideas and the latest trends and buzzwords. Do we really need AI-enabled, ML-enhanced, multi-disciplinary, automated threat hunting cloud-connected, quantum controlled, blockchain-processing toasters in our organizations? Marketing departments sure think so. Sadly, all of this buzzword bingo has drawn attention away from securing the basics in favor of more technology, which requires more trained cybersecurity professionals to manage and really don't reduce our risk in any meaningful way.

This session will focus on 6 low-cost, but vital fundamental security principles that are being overlooked, resulting in significant breaches and disruption in small, medium and global organizations alike.

***Erich Kron**, Security Awareness Advocate at KnowBe4, is a veteran information security professional with over 20 years' experience in the medical, aerospace manufacturing and defense fields. He is the former security manager for the US Army's 2nd Regional Cyber Center-Western Hemisphere and holds CISSP, CISSP-ISSAP, MCITP and ITIL v3 certifications, among others. Erich has worked with information security professionals around the world to provide the tools, training and educational opportunities to succeed in Information Security.*

Kenneth Brown

Nakita Mazurov

Tracking the Online Harassment Chain

Magnolia Room
12:15 - 1:00

The concepts of the kill chain and the deception chain are well known in information security. There is, however, an increasingly-sophisticated online harassment chain which encompasses an array of digital attacks targeting an ever-broadening number of individuals and organizations that IT security professionals need to be aware of. This talk will explore the various tactics deployed in cyber harassment campaigns, and will further provide guidance on minimizing the impact of the attacks through prudent, preemptive cyber defense measures. The presentation will cover in detail the various techniques used throughout the cyber harassment life cycle, and will in turn discuss how each stage can be mitigated and guarded against, protecting both individual and organizational targets from online harassment. Learn how cyber attackers operate and how to safeguard yourself and your organization against them.

Kenneth Brown*, CISSP, is a Federal Project Manager at VMware, USA, specializing in automation and operations management.*

Nikita Mazurov*, PhD, is a researcher focusing on privacy issues revolving around data archival, watermarking technologies, and open source investigations.*

Gideon Rasmussen

Designing a 3rd party Risk Management Program

Magnolia Room
1:15 - 2:00

Provides practical advice to design a TPRM program. Details the end-to-end process: identify, risk rank, assess, risk treatment, monitor and oversight and; escalations. Includes options based on risk tolerance and available funding:

- Provides security requirements for vendor contract templates.
- Describes how to identify new and existing vendors through existing Supply Chain Management processes and in organizations where it is necessary to leverage financial systems. Includes examples where vendors may slip through the cracks.
- Addresses a risk-based approach to tier vendors for assessment when confidentiality and business criticality information is available. Otherwise, includes alternatives such as risky vendor categories and tiering questions.
- Assessment options include on-site assessment, questionnaires, artifact reviews, vulnerability scans and acceptance of independent assessments and; certifications.
- Describes risk treatment: tracking remediation to closure, policy exceptions and risk register entries.
- Provides recommendations to reduce residual risk when vendor service is discontinued.
- Addresses program architecture: welcome packet, process diagram, procedures manual, message templates, system of record, reporting, metrics, etc.
- Includes tips to develop a roadmap to mature the program over three years.
- Provides examples that can be leveraged in small, medium and large organizations. Includes real world challenges with recommendations for processes.

__Gideon Rasmussen__ is an Information Security Consultant with 20 years of experience in corporate and military organizations. Gideon has designed and led programs including Information Security (as a CISO), PCI - Payment Card Security, Supplier Assessment, Application Security and Information Risk Management. Gideon has authored over 30 information security articles. He is a veteran of the United States Air Force, a graduate of the FBI Citizens Academy and a recipient of the Microsoft Most Valuable Professional award. Gideon has also completed the Bataan Memorial Death March (4 occurrences).

Anshu Gupta

Mobile Application Security - What you need to know?

Magnolia Room
2:15 - 3:00

As users move to the world of Mobile Apps, it becomes important to understand the security and privacy risks around Mobile Apps and the technical mitigations available to developers and security professionals to mitigate these risks.
This session will delve into security and privacy issues like third party SDK security, cryptographic storage, IP protection among others. We will also talk about about some of the security risks and best practices around mobile application security development.

Audience Takeaways
Mobile Application Security
Security & Privacy Risks of Mobile Apps
App Level Security Model of iOS and Android. OS/Platform level security issues and protections available
Application/Code level security mitigations that developers can use with code examples
Mobile specific privacy issues and available technical mitigations
Mobile third party SDK level security issues

__Anshu Gupta__ is a senior level security practitioner who has Fortune 500 security consulting experience at Ernst & Young and KPMG where he worked at companies like Microsoft, Salesforce, Oracle, Cisco, McAfee, Adobe, Yahoo, GAP, Kaiser among others. He then moved on to get startup experience at Coupa Software (now a public company), HelloSign (acquired by DropBox) where he was the first security hire and had to build the whole security program from scratch and hired the information security team as well. He is currently serving as the Head of Security Engineering at an innovative Fintech startup. Anshu has a Masters degree in Computer Science and holds the CISM, CISA and CIPP certifications among others.

Kevin Kaminski

Dude, Where's My Log? The Unknown Logging Gaps in Your Environment, Why You Didn't Detect that Pentest, and What to Do About It

Magnolia Room
3:15 - 4:00

Failure to log everything needed for maximum visibility in your environment can leave huge gaps in your ability to remediate threats. But running an enterprise-level logging program can be difficult: how do you know if you're logging everything necessary to detect threats? Are all of your technologies configured to send the right logs? Are they all sending to a logging platform? In this session we will help you answer these and other critical questions of your logging program, which will ultimately help you remediate issues and better use log analysis to mitigate threats.

Kevin Kaminski *is currently the Threat Management R&D Lead at ReliaQuest. He has worked in the security operations space for seven years and worn many different hats throughout the SOC. He has experience in analysis and many different logging platforms, and specializes in threat detection, research, and content development. Kevin works with companies to optimize their logging infrastructure and platforms to improve their security posture and response to threats.*

Suzanne Ricci

Enhancing Your Career in Cybersecurity

Cypress Room
(Workshop)
10:15 - 11:00

In a sea of job postings, recruiters and hiring managers, how can you be your own best advocate to land the right next role for yourself?

How will you search, network, apply and interview?
I will offer my opinion based on decades of experience, having conducted thousands of interviews and placed many information security professionals.

First we'll discuss:
- The best searching and networking techniques (where do I look, who do I connect with and how)
- Then the most effective resume writing (how should I format, why is no one responding, what about keywords)
- And finally interviewing techniques, to include salary negotiations! (what research to do and questions to ask, how to answer To obtain success in today's workforce requires careful career planning. This interactive workshop will guide participants through career planning, enhancing and cultivating a successful career in Cybersecurity.

In this workshop participants will learn:
-- The SWOT technique to planning a cybersecurity career.
-- Enhancing your career with Cybersecurity certifications.
-- Cultivating career success through networking - a focused step by step how-to guide
-- Standing out as a SME in Cybersecurity

This interactive workshop is jam packed with how to's and action items. Participants leave with a completed workbook and detailed action plans.
questions, do I tell you my current salary, do I deserve a sign-on bonus, what's the going range)

Suzanne Ricci *is the Chief Success Officer at Computer Coach IT Training Center. She has spent 20 years career coaching 1000's of IT professionals in Tampa Bay. Getting her start as a web designer, she quickly learned what it takes to be successful in an IT career and today she passionately shares her "tried and true" advice with anyone who needs help. She is the Founder of Tampa Bay Tech Career Advice Meetup, LinkedIn Local Tampa Bay, is a Board member of WITI Tampa Bay and is active in several nonprofit, IT-focused, organizations in Tampa Bay. www.linkedin.com/in/SuzanneRicci*

Secure Code Warrior

Cypress Room
(Workshop)
12:15 - 2:00

Daniel Lewin

Secure Code Warrior's live tournaments allow students to practice, test and prove their web application security knowledge of the OWASP Top 10 and ultimately learn more about secure coding.

Players will be presented with a series of vulnerable code challenges that will ask them to identify the problem, locate the insecure code, and fix the vulnerability. Select from various software languages to complete the tournament, including: Java EE, Java Spring, C# MVC, C# WebForms, Ruby on Rails, Python Django, Scala Play &amp; Node.js.
As students attempt challenges, they can choose to watch instructional videos or read more to learn about how to overcome or fix the vulnerability. The faster and more accurately they complete the challenges, the higher their score. This live tournament setting motivates students in friendly competition, where the top Secure Code Warrior is crowned champion at the end of the session.

*Facilitator **Daniel Lewin** for Alicia Gordon, Secure code warrior*

Attacking the data before the decision

Closing
Keynote
4:14 - 5:30

Rhett Greenhagen

Machine learning and artificial intelligence are emerging as leading technologies when it comes to how data is ingested into graph database management systems such as Neo4j, MongoDB, Cassandra, ArangoDB, Orient DB, Titan, JanusGraph, etc.. One way to manipulate this data leverages said technologies: adversarial modeling/machine learning. And, yes, the bad guys know about it.
In this talk, I'll share examples of how nation-state actors and cybercriminals are using this method – and how you can defend yourself. Did you know, for example, that cybercriminals work closely with fraud rings to mitigate fraud detection algorithms? Learning how these attacks unfold is critical to preventing them.

Attendees will walk away with the knowledge of how malicious hackers can use both simple and advanced attack methods – and armed with the knowledge to protect themselves, too.

***Rhett Greenhagen** is a Senior Security Associate at Bishop Fox, where he is a member of the research and development team. Rhett has over a decade of red teaming and network security experience. His focuses encompass open source intelligence, cyber counterintelligence, profiling, exploitation, and malware analysis in addition to technical research. An accomplished speaker, Rhett has spoken at numerous conferences, such as Black Hat USA and DEF CON on a variety of security and related topics.*

OUR SPONSORS_

OFFICIAL (ISC)² CHAPTER

TAMPA BAY

RELIAQUEST

Checkmarx

REDSEAL

sslstore™

exabeam

CYBERSECJOBS

ClearedJobs Net

PRIVASEA

PROTECTION COAST TO COAST

TrustedSec

CRITICALSTART

VIPERLINE™

SOLUTIONS

EVT

ENTERPRISEVISIONTECHNOLOGIES

BLACK HILLS

Information Security

• 2008 •

Gigamon®

CROWDSTRIKE

ABACODE

proofpoint.

COMPUQUIP

CYBERSECURITY

AMGEN

Secureworks®