PROGRAM
2017

BSIDES NASHVILLE

BsidesNash.org
@BsidesNash

BSides Mid-TN, Inc. is proud to present :

BSides Nashville 2017

Welcome to BSides Nashville for 2017!

On behalf of the Organizing Committee, volunteers, speakers and sponsors we are pleased you are here.

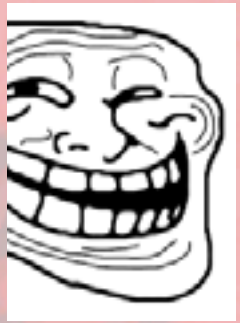
Can you believe it has been 4 years? It has been a fun ride and we are amazed and overwhelmed by your support.

We would like to thank our sponsors. Without their generosity, this conference (and many others) would not exist. Each of our sponsors bring resources and enthusiasm to this event. A special thank you goes out to Lipscomb's College of Computing and Technology for providing the perfect space and atmosphere, for a fourth year. We are all students of the security craft, and we welcome the new students and the more experienced to help us in our learning.

We have intentionally avoided tight schedules and we want all of you to relax, share, and connect. We believe that the real value of a BSides conference is the community. You don't get to socialize when you race from room to room, trying to find a seat. So, find your slow, southern drawl (we'll let y'all borrow one) and relax. Go check out the Phish Bowl. Minecraft is back as are some new fun things for kids of all ages. Brought to you by people of the community, we give them the space, they give us their creativity, so check out their hard work.

Once again we are excited to bring you great speakers from around the US and many from Tennessee and nearby Kentucky. Please show your appreciation, as they are volunteers and came at their own expense to share their knowledge.

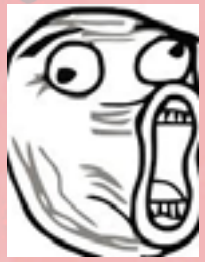
KEYNOTE SPEAKER:

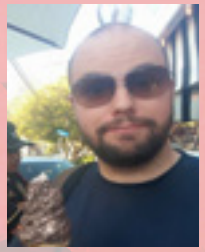


Amanda Berlin

Amanda Berlin is an Information Security Architect and infosec groupie. She has spent over a decade in different areas of technology and sectors providing infrastructure support, triage, and design. Amanda is an avid volunteer and has also presented at a large number of conventions, meetings and industry events. Some examples of these are: DerbyCon, CircleCityCon, GrrCon, and DEFCON.

She is currently working on co-authoring a Blue Team best practices book titled "The Defensive Security Handbook" as well working on a barrage of other projects. While she doesn't have the credentials or notoriety that others might have, she hopes to make up for it with her wit, sense of humor, and knack for catching on quick to new technologies. A solid 5/10 for looks, 6/10 for tech, and 5/7 for humor.





Adam John

AJ has been around this infosec and IT thing for closing on 20 years. Amazed that he's both still "sane" and still employed, he has experienced life from the trenches of the lowly IT tech to explaining to Federal CISOs and big company shops what they really should do, and help them get there (if they listen). AJ made a point to be unconventional in the various corporate levels that he's lived in, and it has taught him a lot of what works, what is BS, and what politics can do to a person and an organization. And various stuff and nonsense in my LinkedIn profile.

Armin Smailhodzic

Bosnian born, German raised, American educated Information Security Professional. Avid traveler/explorer, food and workout enthusiast, and PC gamer.

Ben Actis

Based in San Francisco, Ben Actis is currently a Sr. Security Research Engineer/Grand General of GIFs at Synack, specializing in Mobile & IoT Security, as well as reverse engineering. Prior to Synack, Ben worked a combined 6 years at Lookout and MITRE in various roles with focuses on research & response, mobile reverse engineering and network analytics – most famous for his primary research surrounding shedun/humming bad and xcode ghost. Ben has also taught introductory college courses, such as "intro to x86" and "intro to flow analysis" – both available on opensecuritytraining.info. When not reversing or participating in bug bounty programs, you'll find Ben searching for Pokemon, taking Krav Maga, and trolling on Twitter and Slack channels.

Ben Shipley

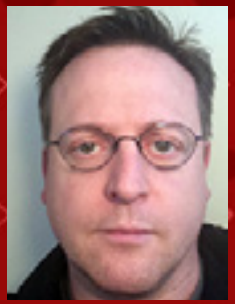
Ben Shipley is an undergrad majoring in Information Technology with a focus in Information Security & Assurance. He currently works in Incident Response for a confidential, globally recognized Security Solutions Provider. He is also passionate about consumer-data privacy, threat-intelligence, as well as foreign affairs.

Brent White

Brent is an Sr. Security Consultant within NTT Security, is the founding member of the Nashville Def Con group (DC615), and is also a supervisor for the Def Con conference "Groups" program. He has held the role of Web/Project Manager and IT Security Director at the headquarters of a global franchise company as well as Web Manager and information security positions for multiple television personalities and television shows on The Travel Channel. He has also been interviewed on the popular web series, "Hak5" with Darren Kitchen, BBC News, and on Microsoft's "Roadtrip Nation" television series. His experience includes Internal/External Penetration, Wireless, Application and Physical Security assessments, Social Engineering, and more. Brent has also spoken at numerous security conferences, including ISSA International, DEF CON, DerbyCon, SaintCon, PhreakNic, SkyDogCon, NolaCon, B-Sides Nashville, B-Sides Charleston, Techno Security Con, TakeDownCon and Appalachian Institute of Digital Evidence (AIDE) conference at Marshall University, and more.

Bruce Wilson

Bruce Wilson is a chemist who's found a home doing IT so that other scientists can focus on doing science. His recent work has focused on Identity, Credential, and Access Management (ICAM), including both user functionality and security. JT Liso (co-author) is a third-year Computer Science student at the University of Tennessee, with an interest in combining machine learning and cybersecurity.



Casey Smith

Casey Smith is a Researcher with the Veris Group Adaptive Threat Division. His interests include testing and understanding defensive systems.

Chris Sanders

Chris Sanders is an information security author, trainer, and researcher who leads a research team at FireEye. He is the author of the best-selling security books Applied Network Security Monitoring and Practical Packet Analysis, and developer of the Investigation Theory online course. Chris also founded the Rural Technology Fund, a nonprofit devoted to providing technical education resources to rural and high poverty schools. His blog is http://www.chrissanders.org.

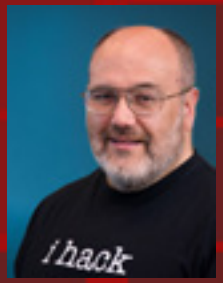
ISSA
Information Systems Security Association
Middle Tennessee Chapter

BSIDES NASHVILLE

Jason Smith

Jason Smith has a background in physics, and has built everything from particle accelerators to explosive neutralizing robots used by the military. He has worked in multiple US Department of Defense SOCs and has worked with the largest security vendors to operationalize security in the world's largest organizations. Jason co-wrote Applied Network Security Monitoring and maintains the open source project FlowBAT, a graphical flow data analysis tool. Jason works remotely for Cisco from his home in Nashville, TN.

Jeff Man

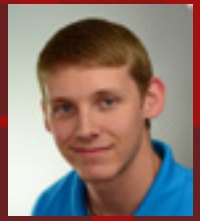


Jeff is a respected Information Security expert, advisor, speaker, teacher, advocate, and curmudgeon. He has over 33 years of experience working in all aspects of computer, network, and information security, including risk management, vulnerability analysis, compliance assessment, forensic analysis and penetration testing. He has held security research, management and product development roles with NSA, the DoD and private-sector enterprises and was part of the first penetration testing "red team" at NSA. For the past twenty years, he has been a pen tester, security architect, consultant, QSA, and PCI SME, providing consulting and advisory services to many of the nation's best known companies.

"After spending nearly 13 years working for the Department of Defense, I ventured out into the private sector to consult and advise on matters of information security. On many occasions, after explaining some basic security concept to a customer and outlining what they need to do to be secure, I often heard the retort, "yeah, but we don't need DoD level security." Well, after twenty years in the private sector, and especially over the past 2-3 years with the proliferation of data breaches against major companies, I find myself wanting to reply, "yeah, you really DO need DoD level security!"

Joe Gray

Joe Gray joined the U.S. Navy directly out of High School and served for 7 years as a Submarine Navigation Electronics Technician. Joe is an Enterprise Security Consultant at Sword and Shield Enterprise Security in Knoxville, TN. Joe also maintains his own Blog and Podcast called Advanced Persistent Security. He is in the SANS Instructor Development pipeline, teaching SANS Security 504: Hacker Tools, Techniques, Exploits, and Incident Handling. In his spare time, Joe enjoys reading news relevant to information security, attending information security conferences, contributing blogs to various outlets, bass fishing, and flying his drone.

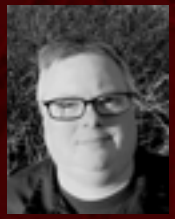


Matt Nelson

Matt Nelson is a Red Teamer and Researcher with the Veris Group Adaptive Threat Division. Matt has a passion for offensive PowerShell, is an active developer on the PowerShell Empire project, and helps build offensive toolsets to facilitate red team engagements

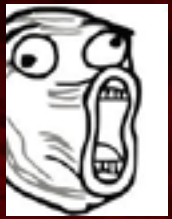
Rodney Hampton

Rodney Hampton is a cybersecurity consultant. Rodney has 16 years of professional IT experience. Previous positions include being the IT Security Manager for a Fortune 500 energy company and working as a member of the security team for one of the largest insurance companies in North America. Rodney's formal education includes an AS in Business Magna Cum Laude, a BA in Military and Diplomatic History from The Ohio State University, and a JD in law Magna Cum Laude from Western Michigan University. He is a Certified Information Systems Security Professional and holds several other vendor-specific certifications. He currently lives in Tennessee where he and his wife raise their three children.



Ron Foster

With over 15 years of IT experience with various platforms, and technologies, I have tested both large and small enterprise applications. Cutting my teeth as a unix instructor for Sun Microsystems. I then went on to make a career out of breaking things. When not running security assessments for HPE's Fortify On Demand service, you can find me meddling with drones, refurbishing an old WWI/WWII rifle, or breaking stuff.



Russell Butturini

Russell Butturini has been in IT and information security for the last 14 years and currently is a member of the penetration testing team at a "Big 5" health insurer. Every once in awhile, struck by inspiration between watching horse racing and chasing his 8 year old daughter around, he cobbles together some cool Python code that people seem to like and presents it at various conferences such as DEFCON, Derbycon, and various BSides. His tool, NoSQLMap, has been starred 405 times on Github (which is 404 times too many), and was also published in "The Hacker Playbook 2".

Ryan Goltry

Ryan is a Santa Maria Lime Steak Rub seasoned IT Generalist with a love of performance tuning and security reviews. A senior security architect, he is a recovering CISO with a wealth of web application security experience. Currently interested in helping SOC operators, while researching botnet detection, vulnerability management, and bourbon.

Ryan Hays

Ryan Hays is the Security Programs Director at TBG Security. With 15 years of experience within the IT field, he has worked in a variety of capacities, currently specializing in offensive security and threat emulation techniques. During his career he has worked with a multitude of Fortune 500 and 1000 companies, along with various U.S. Government Intelligence agencies. Ryan takes pride in giving back to the InfoSec community by presenting at multiple conferences, as well as providing training and mentorship to people across the globe.

Tara Wink

Tara Wink has a background in Physics and penetration testing. As a former security consultant, she has experience working with various government and private industries. Her current role is working as a Senior SOC Analyst for Change Healthcare in Nashville. When Tara isn't working, she enjoys traveling, rock climbing, socializing, and tormenting her Bengal cat, Cheeto.

SYNCURITY

SDGblue®
secure technology

Tim Roberts

Tim is a Sr. Security Consultant within NTT Security's Threat Services group. He has spoken at national, international, and collegiate security conferences, including ISSA International, DEF CON, DerbyCon, various B-Sides, CircleCityCon, Techno Security Con, SaintCon, Appalachian Institute of Digital Evidence at Marshall University, and more. He has been interviewed on the subject of "White hat hacking" for Microsoft's "Roadtrip Nation" television series, was featured on IDG Enterprise's CSO Online publication by Ryan Francis on social engineering, and is a regular contributor to NTT Security's #WarStoryWednesday blog series.

Tim has held management, IT and physical security roles across multiple industries, including healthcare and government. His professional experiences cover traditional/non-traditional hacking techniques that include network, wireless, social engineering, application, physical, and scenario-based compromises. These techniques have led to highly successful Red Team assessments against corporate environments. By continuing to share these experiences, he hopes to further contribute to the InfoSec community.

Willie Hight

Working in IT/InfoSec approaching 20 years, I can attest to how every year has been different and the only consistent factor is change. I've enjoyed the ride and look forward to sharing and learning daily. Personally, I think good food, interesting people, and projects help make life fun. Food, fellowship, and fun are very important ingredients to a good day.

SANS

GOT 2-SECOND VISIBILITY?

ACHIEVE 2-SECOND VISIBILITY across your on-premise, endpoint and elastic cloud global IT assets.

CONTINUOUSLY ASSESS your security and compliance posture, and identify whether you've been compromised.

DRASTICALLY REDUCE YOUR TCO by consolidating multiple enterprise security and compliance solutions with the Qualys Cloud Platform – ***and more to come.***

Sign up for a free trial at qualys.com/2seconds

QUALYS®
CONTINUOUS SECURITY

© 2017 Qualys, Inc. All rights reserved.

Partner with Nashville's pacesetter in technology education.

MS-Information Technology

MS- Software Engineering

MS- Data Science

Whether you need to acquire new talent, create stronger employees or create your own impact in the IT community, Lipscomb University leads the way with innovative and one-of-a-kind graduate degrees for our region as well as industry partnership programs, community events and a strong commitment to developing tomorrow's leaders.

Find out what it means to have **one of the nation's top 35 information technology schools** on your team. Contact Brett Ramsey at **brett.ramsey@lipscomb.edu** for more information.

LIPSCOMB UNIVERSITY | COLLEGE OF COMPUTING & TECHNOLOGY

technology.lipscomb.edu

Level up your cyber security strategy.

Level up your business.

Working together, we enable better business outcomes through optimized cyber security.

OPTIV

CARBON BLACK

Optiv is your source for security success. We combine extensive expertise, experience and research with powerful partnerships with industry leaders like Palo Alto Networks to help our clients achieve their security objectives. We provide a wide range of services for Palo Alto Networks products including resale, identification and selection, implementation and integration, optimization and support. Let us help plan, build and run a successful security program for your organization, focused on your specific needs.

www.optiv.com

Red.....112
Green....110
Blue.....102
Purple...108

RED Track

The Red track is for technical talks telling us about new attack vectors or tricks learned while pentesting or during research. We all love a good attack talk and to hear about the latest things, but we have a challenge to all Red Team talks, include at least one slide telling the defense side about signatures for the attack, defense mechanisms to protect against it or how you could have been caught.

BLUE Track

The Blue track is for talks about defense. We all know attacks are sexy but many of us are on the defensive side. This track is to tell us about Defensive tactics, how a program was built with duct tape and bubble gum or other stories from the defensive trenches.

GREEN Track

The Green track is geared toward newcomers to the Infosec industry and professional growth.

TIME	Purple : We're all in this together		
08:00 - 09:00	**REGISTRATION OPENS!!!**		
09:00 - 09:15	**Welcome to BSidesNashville**		
09:15 - 10:15	Keynote: Amanda Berlin		
10:15 - 10:30	**Coffee Break**		
Time	**Green**	**Red**	**Blue**
10:30 - 11:30	**Infosec Tools of the Trade: Getting Your Hands Dirty** *Jason Smith, Tara Wink*	**Security Guards -- LOL!** *Brent White, Tim Roberts*	**Got Vendors?** *Armin Smailhodzic, Willie Hight*
11:40 - 12:40	**How to learn reverse engineering, kick ass at bug bounties, and being a bad ass SOC analyst** *Ben Actis*	**Windows Operating System Archaeology** *Casey Smith, Matt Nelson*	**Emerging Legal Trends in Cybersecurity** *Rodney Hampton*
13:00 - 14:00	**LUNCH**		
14:00 - 15:00	**A Pyrate looks at 40** *Adam John*	**Intro to drone tech** *Ron Foster*	**Trust, But Verify, Your SAML Service Providers** *Bruce Wilson*
15:10 - 16:10	**Springtime for code reviews** *Ryan Goltry*	**Weaponizing Splunk:** ***Using Blue Team Tools for Evil*** Ryan Hays	**Does DoD Level Security Work in the Real World?** *Jeff Man*
16:20 - 17:20	**Marrying Incident Response and Threat Intel Within Your Enterprise** *Joe Gray, Ben Shipley*	**Chunky Cookies:** Smashing Application Aware Defenses *Russell Butturini*	**Abstract Tools for Effective Threat Hunting** *Chris Sanders*
17:30 - 17:40	**Closing Ceremonies**		
18:00 and Beyond	**After Party at: Pour House Burgers, Bourbon and Brews**		

KEYNOTE :

Mental Health in Infosec - Hackers, hugs, and drugs

Amanda Berlin

The infosec community is difficult to compare to any other. We are composed of intelligent, driven, passionate, opinionated individuals. When you combine the pressure and stress we put on ourselves in the form of research, learning, teaching, and creating it starts to build up. Not only do we put pressure on ourselves, but we also take it on from our bosses, co-workers, and family in many different forms. The majority of roles we fill cater to our drive and willingness to be behind a keyboard for hours on end. The end result is that many of us are broken. Broken in different ways, at different times, and for different reasons. We need to bring to light a topic that shouldn't be as faux pas as it is. I'll share my personal struggles, stories of friends and family, and hopefully help us come closer together as a community to help you or people around you.

Green Track

Infosec Tools of the Trade: Getting Your Hands Dirty

10:30am - 11:30am

Jason Smith & Tara Wink

In this presentation we will be going over introductions to the various focuses in information security and demoing the most common tools that are used in operational security, both offense and defense. You will leave with an idea on how to freely obtain and use these tools so that you can have what you need for that first interview: experience and a passion for security. This is a green talk for people who do not have a clue on what offensive and defensive people do operationally, from a tool perspective.

How to learn reverse engineering, kick ass at bug bounties, and being a bad ass SOC analyst

11:40am - 12:40pm

Ben Actis

This talk is designed to provide novice security professionals and aspiring bug bounty participants several tips and resources to grow their skill sets in reverse engineering and (ethical) hacking applications. It will break down all the skill sets above into areas for visual, auditory, and kinesthetic learners. By the end of the talk, those in the audience will walk away with a list of resources and encouragement to further their security careers – and start earning bug bounties (hopefully).

A Pyrate looks at 40

2pm - 3pm

Adam John

At 40, everyone is obligated to take that mid-life look at one's self and take an account of where they have been, where they wanted to go, the bitch that is reality, and where they will probably end up. After sailing my way through the the IT and infosec worlds from techie to interacting with C-levels, it's been an interesting ride with potholes and great opportunities. I'll opine about what I've found to really matter, what doesn't, and what you need to do but you don't want to. I don't have all of the answers, but I have a map that will help you get where you really should go.

Springtime for code reviews

3:10pm - 4:10pm

Ryan Goltry

You come upon a long running project that has never had a security centric code review before. There are a couple millions lines of code, web applications, microservices, a database; a gold mine of s*** to dig through. The opportunity for findings is massive. How the next steps are executed all depend on situational awareness and could result in CSMs (career shortening maneuvers). Topics covered will include what tools to have in the kit for a whitebox code review, what to prioritize, and whom with and how to collaborate for short and long term engagements.

Marrying Incident Response and Threat Intel Within Your Enterprise

4:20pm - 5:20pm

Joe Gray & Ben Shipley

Having actionable Threat Intelligence is vital to preventing attacks.Having a strong Incident Response team is vital to protection of yourenterprise. All too often, these two groups don't work together within an organization. This session will demonstrate the common ground between
Threat Intelligence and Incident Response with examples like utilization of data sources, goals, and even personnel. Get tips on how to communicate the
value of this type of collaboration to management and the C-Suite. You will come away from this session with a better understanding of the importance of sharing information and resources to improve the security capabilities of the enterprise.

Red Track

Security Guards -- LOL!
10:30am - 11:30am
Brent White & Tim Roberts

During this presentation you will hear real-world stories from various Red Team assessments that we have performed. These assessments will be broken down to discuss the various social engineering and physical security bypass methods and tools used. We will also provide our recommendations for remediation and provide the audience the opportunity to ask questions.

3 things you will learn from this session:
- Hear real world scenarios used during red team, physical and social engineering assessments.
- What techniques we use vs. security guards and tenacious employees.
- What tools we use such as forging fake badges and documents, physical entry/bypass tools and social engineering/ manipulation techniques for successful assessments.

Windows Operating System Archaeology
11:40am - 12:40pm
Casey Smith & Matt Nelson

The modern Windows Operating System carries with it an incredible amount of legacy code. The Component Object Model (COM) has left a lasting impact on Windows. This technology is far from dead as it continues to be the foundation for many aspects of the Windows Operating System. You can find hundreds of COM Classes defined by CLSID (COM Class Identifiers). Do you know what they do? This talk seeks to expose tactics long forgotten by the modern defender. We seek to bring to light artifacts in the Windows OS that can be used for persistence. We will present novel tactics for persistence using only the registry and COM objects.

Intro to drone tech
2pm - 3pm
Ron Foster

For the noob, or the expert, this talk will cover types of drones, typical components, and hobby vs commercial from a legal point of view. Plus there is nothing like wardriving our neighborhood from your drone.

Weaponizing Splunk:
Using Blue Team Tools for Evil
3:10pm - 4:10pm
Ryan Hays

Splunk is a log aggregation and correlation tool that is normally used for defensive analysis and infrastructure management. What if Attackers could use this same tool against the blue team? During this presentation, I will discuss creative uses that penetration testers and Red Teamers can use to gain more access, and move laterally within an organization.

Chunky Cookies: Smashing Application Aware Defenses
4:20pm - 5:20pm
Russell Butturini

n recent years, defensive technologies have moved past the traditional filtering and anomaly detection at Layer 3 and 4, and deep packet and payload inspection have become more prevalent. As penetration testers, it's important to understand how to adapt exfiltration techniques to exploit the limitations next generation firewalls, application aware proxies, URL filters, and data loss prevention packages have. This talk will cover several techniques for building payloads to bypass all of these technologies, from basic file encoding to making and proxying outbound connections as legitimate applications. A completely revamped and extended version of Fireaway, a tool originally designed to bypass next generation firewalls, will be released as part of the talk as well.

netWorks
networksthatwork.net

SOPHOS
Security made simple.

Blue Track

Got Vendors?

10:30am - 11:30am

Armin Smailhodzic and Willie Hight

How many vendors does your company have? Do you have a list of all the vendors used within the company? Did you know that you were a vendor at one point? What is he process for approving vendors? How do you verify if these vendors are compliant to what your organization requests? Will they sign a BAA? Are these vendors on your network, in your building, looking at your information (PHI or PII)? Are they using their own machines while on your network, how are they protecting those if they are viewing/storing/modifying your data? Does your endor have vendors working for you? What is the process for approving these vendors and who is Involved?

Emerging Legal Trends in Cybersecurity

11:40am - 12:40pm

Rodney Hampton

How can you make a bad event like a major security breach even worse? By failing to be aware of your legal obligations, liabilities, and options. This presentation will orient you to the rapid changes in the legal environment as it pertains to cybersecurity. Your in-house legal department, if you are lucky enough to have one, may be too overworked to have kept up or given much thought to how these pieces fit together with your incident response program. This presentation will discuss outcomes of cases involving data breach, cybersecurity insurance litigation, the increasing regulatory involvement from the FTC and other agencies of state and federal government. The discussion will also touch briefly on emerging legislation for data breach notification and consumer/patient privacy in the US and in Canada, UK and Europe. An exciting time will be had by all.

Trust, But Verify, Your SAML Service Providers

2pm - 3pm

Bruce Wilson

SAML (Security Assertion Markup Language) is a key tool for single sign on and enterprise use of cloud services. It relies on public key cryptography, and there are lots of examples of poorly implemented crypto out in the world. We wanted to be able to test whether the service providers we were hooking up to our SAML Identity Provider actually checked the things they wanted to check. And we wanted to be able to do this within the Cucumber-based framework we've been using for other aspects of functional

So, we have built some (open source) tools to do that. In this talk, we'll present the tools and the results of the tests we have run to date.

Does DoD Level Security Work in the Real World?

3:10pm - 4:10pm

Jeff Man

What does this mean? Probably not what you are thinking. This talk willstart with an overview of the foundational nature of data security,highlight the major tenets or goals of data security, introduce the riskequation, discuss how and why so many companies so often fail at implementing the basics of data security, and explore some ways that aDoD-centric approach to data security might be implemented in the privatesector. Brainstorming, discussion, dissension all welcome. Hint: Thisain't about Cyber!

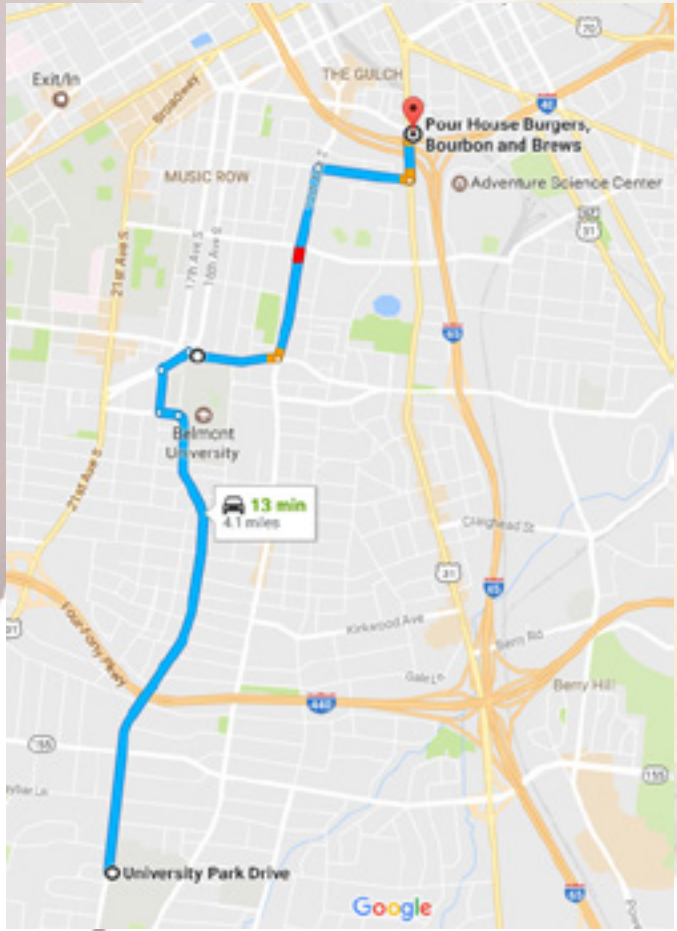
Abstract Tools for Effective Threat Hunting 4:20pm - 5:20pm

Chris Sanders

Because breach is inevitable, the ability to investigate security compromises has never been more important. But, what makes someone good at finding and catching bad guys? Even most experts cannot fully articulate the tacit knowledge that makes them so good at what they do.

In this presentation, I will tackle that question by approaching information security from a cognitive psychology perspective to identify abstract tools that are commonly mastered by expert threat hunters. This will include discussions about framing the investigation process using the scientific method, curiosity as an x-factor contributing to success, the merits of thinking with a pivoting mindset, and more.

This talk should provide valuable insight to beginner nd expert analysts alike. You should walk away with a more thorough understanding of how investigation expertise is a lot less about tangible software tools and much more about abstract tools inherent to the mind, and how to further your skills and career using that knowledge."



Party

Pour House Burgers, Bourbon and Brews

730 8th Ave S,
Nashville, TN 37203

Sponsored by:

QUALYS®
CONTINUOUS SECURITY

Please Rideshare and/or use valet

SPONSORS

We would again like to thank our sponsors, volunteers and attendees.

Without everyone's generosity and time we would not be able to put on this awesome security conference.

We could not have done this event without you!

LBMC
PLATINUM SPONSOR

LIPSCOMB
PLATINUM SPONSOR

QUALYS
GOLD SPONSOR

PARTY SPONSOR

Parameter
PARTY SPONSOR

network
SILVER SPONSOR

SOPHOS
SILVER SPONSOR

TrustedSec
SILVER SPONSOR

KASPERSKY
SILVER SPONSOR

AccuvantFishnet Security
SILVER SPONSOR

Sword & Shield
BRONZE SPONSOR

GRAPHIC DESIGN

OLD rework this template

ORGANIZERS AND STAFF

Type-layout needs worked
Lauren Rogers, President
Geoff Collins, Treasurer
Finn Breland, Secretary
Gabriel Bassett, Badge Wrangler
Tommy Wolosin, Swagger Supplier
Adrian Crenshaw, Norse god & AV
Scott Haber., Caffeination Specialist
NSA_Key, Phish the Hoopy Phrood
RC, The Force
Jennifer Samardak, Nerf Herder
Victor Wieczorek - Digital Media Wizard
Lill Haber - Head of Strategic Social Planning
Ryan Goltry - I can do what?

© B-Sides Nashville 2017