Technical Check In Thursday 6:00pm - 11:00pm - Discord - Open 24x7
BSides Support - Discord - Open 24x7

Register for the event at the North Alabama Chapter of ISSA site here:
[Tickets for Virtual BSides Huntsville]

Training Friday	**Class**	**Location**	**Proctor**
8:30 - 12:30	Professionally Evil Application Security taught by Ochaun Marshall	Zoom Training Room 1	TBD
1:00 - 5:00	Professionally Evil Network Testing taught by Alex Rodriguez	Zoom Training Room 1	TBD
9:00 - 5:30	Business OSINT Powered by The OSINTION taught by Joe Gray	OSINTION provided platform	TBD
8:00 - 5:00	Ethical Hacking Attack Phases by EC-Council, Instructor Gilbert Mashingaidze	EC Council provided platform Register Here	TBD
7:30 - 5:30	BSides Support and Volunteer Chat	Discord Monte Sano Room	TBD

BSides Support - Discord - Open 24x7

BSides Saturday	**Zoom Room 1**	**Zoom Room 2**	**Discord CTF**	**Discord Secure Code**
7:30		Coffee Time Meet Up Discord Monte Sano Room Speaker TBD		
8:30	Opening Ceremonies			
9:00	Keynote Joanna Burkey Cybersecurity as an ecosystem			
10:00	The Invisible War: A Look at the Ransomware Battle Fernando Tomilson	TBD	Threat Defence Challenge Trend Micro	Secure Code Tournament Secure Code Warrior
11:00	Hack in your sleep David Hunt	A Shock to the System: Static Analysis for Real AppSec Ochaun Marshall		*https://discover.securecodewarrior.com/BSidesHuntsville-tournament.html*
Break/Chat/Meetup		Andy Bryan for Snowflake/Hunters.ai Threat Detection across all environments with SnowflakeData Security Lake		
1:00	Keynote Chirs Cochran Performing Like a Cybersecurity Champion			
2:00	Eddie Glenn Secured Code Signing at the Speed of DevOps	Steven Kriby Requiem for the Password		
3:00	Luke Gleba Using SIP Traffic to Influence the Communications and Geopolitical Landscape of Germany	Lighting Topics Forum Moderator TBD		

4:00	Closing Ceremonies Comments and CTF awards			
5:00	Meetup			

Joanna Burkey

Cybersecurity as an ecosystem - The democratization of technology is only one of the forcing functions that is pushing cybersecurity to migrate from an empire to an ecosystem. Join me to dive in on how cybersecurity organizations take off our traffic cop hats and put on the business partner hats in order to adapt to the changes in both technical and threat landscapes. Bio: Joanna Burkey is the Chief Information Security Officer at HP. In this role, Joanna and her team have responsibility for HP’s global cybersecurity program, including IT infrastructure, technology platforms, and business units. Her organization has responsibility for identity, governance, compliance, security operations, strategy and architecture as well as product security. Joanna returned to HP in April, 2020 after several years with Siemens AG where she was most recently the Global Head for Cyber Defense responsible for cybersecurity defense across IT/OT infrastructure as well as products, solutions, and services. Joanna has a computer science/mathematics background from The University of Texas at Austin and Angelo State University. She has focused on cyber security throughout her career. Her previous roles have included software engineering, product strategy, and security evangelism. Joanna is based in Austin, Texas.

Fernando Tomilson

The Invisible War: A Look at the Ransomware Battle - The use of ransomware has taken organizations by surprise. While most organizations have dedicated staff to minimize and reduce the attack surface for such threats, the malware is still successful. Once infected, the attack has huge impacts on an organization's business and its ability to operate. In some cases, organizations pay the fee to return their systems to normal. In other cases, organizations take to remediating the attack by restoring backups or seeking to reverse the encryption used through internal means. In this talk, we will dive into the ransomware pandemic and its effect on organizations. Additionally, we will look at defensive measures an organization can take to limit their chances of becoming a statistic and the headline on the evening news. Bio: Fernando Tomlinson has 19 years in cybersecurity and system administration within the Department of Defense. He currently does Forensics and Malware Analysis for the United States Army Cyber Command. Previously he was a Technical Director of a Cyber Operations Center and has lead multi-level Digital Forensics and Incident Response (DFIR) and threat hunting teams. He is also a collegiate cybersecurity Adjunct Professor who enjoys contributing to the community through his blog at https://cyberfibers.com and projects at https://github.com/wiredpulse. He is the developer of PoSh Hunter (https://posh-hunter.com) and co-developer of Under the Wire (https://underthewire.tech), which both are interactive PowerShell educational platforms. Additionally, he is a consultant with Reliable Cyber Solutions (https://rcybersolutions.com), a company focused on cybersecurity training and certification.

David Hunt
Hack in your sleep - When you wake up, do you brush your teeth or pour a cup of coffee? Afterwards, do you reach for your phone and scroll through notifications or take the dog for a walk? If real world decisions could be laid out on a decision tree, you could identify trends. To use a military term, you could start to break your day into tactical decisions. Now imagine you're a hacker. You were just dropped into a computer network. Do you start running discovery tactics to determine what computer you compromised? Or do you maintain persistence? Or move laterally to increase your foothold? Each decision is naturally weighted with a calculation between risk and reward. Leveraging the concept of automated planning, you can build autonomous defense systems which probe your assets looking for holes. Focusing on realism helps you identify not only unknown vulnerabilities, but those which are most likely to be exploited. In this talk, I will break down how attackers chain together benign actions to form a malicious attack. Then, we will analyze how decisions are made in the real world and attempt to map them into a program to run on repeat - non deterministically - in your own network. You should walk away with a greater understanding of how hackers think, along with a customizable program allowing you to "hack in your sleep." Bio: David Hunt is the CTO of Prelude Research Inc. There, he leads a team supporting a cutting-edge autonomous red team platform. Prior to this work, David built CALDERA, an open-source adversary emulation framework, while working as a Principal Cyber Security Engineer for MITRE. David has spent 15 years working as a security consultant for the U.S. Government, along with full-time roles at major cyber security firms, such as FireEye.

Ochaun Marshall
A Shock to the System: Static Analysis for Real AppSec - Static analysis (SA) is one of the few techniques that provides a low-level examination of source code. When SA is combined with DevOps automation and traditional pentesting, it can offer valuable insights that help with implementation and remediation efforts. Ineffective use, however, overwhelms development teams with false positives and causes dysfunctional communications with security teams. This talk goes over several toolkits for static analysis based on language and tech stack. After that, we will talk about how to use automation to create workflows for developers and application security engineers. We will conclude with cultural transformations needed to make effective use of these tools and techniques. Bio: Ochaun (pronounced O-shawn) Marshall is a developer and security consultant. In his roles at Secure Ideas, he works on ongoing development projects utilizing Amazon Web Services and breaks other people's APIs and web applications. When he is not swallowing gallons of the DevOps Kool-Aid, he can be found blasting songs from Vitamin String Quartet while hacking, blogging, and coding.

Andy Bryan for Snowflake/Hunters.ai
Threat Detection across all environments with SnowflakeData Security Lake, Bio: Andy Bryan is the Head of Field Security Engineering at Hunters.ai. Andy is a technologist who has spent most of his 24-year career in early stage companies moving them toward publicly traded

companies. Prior to Hunters.ai, Andy spent several years in the network detection space with Vectra.ai, Extrahop, FireEye/Mandiant, along with other companies like Aruba Networks and Fortinet. Andy currently holds his CISSP and has taken numerous security certifications from ISC2, SANS, Offensive Security, and attended both Colorado Tech and NorthEastern for Computer Science. Early in his career Andy was indoctrinated into the security mindset having served in the US Army and attended several different schools over his military career, along with spending several years abroad.

Chirs Cochran

Performing Like a Cybersecurity Champion - Cybersecurity practitioners are mental athletes with no off-season. Every day we are playing chess against an opponent that doesn't sleep and doesn't play by the rules. This talk will explore the human performance facets of cybersecurity and give the audience a framework for practical excellence. Bio: Chris Cochran is the Director of Security Engineering for a financial technology company by day and producer and host of the popular Hacker Valley Studio podcast by night. Chris is prior active duty US Marine Corps intelligence, which led him to a career in cybersecurity. He has dedicated that career to building and leading advanced cybersecurity teams for organizations across many industries. His ultimate passion is finding and amplifying human stories in cybersecurity to inspire and enlighten our community.

Eddie Glenn

Secured Code Signing at the Speed of DevOps - Can your code signing infrastructure keep up with the application development teams that have embraced DevOps? Or maybe the more appropriate question is if you even have visibility into how your application teams are handling code signing? Hackers are targeting code signing credentials more than ever before. Prominent companies have been the victims of code signing breaches and as a result, malware was inserted into legitimate software updates by hackers. Customers, seeing that the update was properly signed, install the update and promptly get infected with malware. Even though DevOps teams may be responsible for code signing the applications they deliver, your team is responsible for the information security of your company. A breach can have major impact on your company: impacting revenue, market share, and even exposing sensitive data. As more companies have embraced digital transformation and DevOps, the frequency of software releases has increased substantially which can stress any code signing system that is based on manual steps. In this session, we will examine why the InfoSec team should be concerned about how applications are code signed, the best practices for securing a code signing process, and how to support the special needs of DevOps teams.

Steven Kriby

Requiem for the Password - Topics include: History of password usage, the modern consensus about passwords, the sad reality, or there ought to be a name for doing the same thing over and over again and expecting different results, emerging password theory including forget complexity, and alternatives to passwords. Bio:

Luke Geba

Using SIP Traffic to Influence the Communications and Geopolitical Landscape of Germany - The amount of enterprise networks and organizations that use Voice Over Internet Protocol (VoIP) is obviously more abundant than it was during the advent of the technology many years ago, which raises the concern of potential large scale attacks on the protocol itself. A concerning observation is that nations have begun to switch entire PBX systems to VoIP. After sifting through some of Rapid 7's most up-to-date SIP data recorded by Project Sonar, I discovered that a large amount of data comes from SIP reply packets. Included in the data were source addresses, destination addresses, user agents, and server headers. Of 1000 packets containing user agents selected at random, 380 were FRITZ!OS or AVM products originating from Germany. This is commensurate with Project Sonar data collected worldwide which shows 38% of the sampled data was from SIP devices in Germany.