# 2018 North American International Cyber Summit

## Monday, October 29, 2019

## Cobo Center – Detroit, MI

## Draft Event Agenda

7:30 AM - 8:30 AM
**Registration and Continental Breakfast & Visit with Sponsors**

8:00 AM - 12:00 PM
**High School Cyber Challenge**
Teams of high school students from around the state will compete against each other in a unique cyber competition. These students have completed Round 1 of the competition and have scored high enough to be invited to go head-to-head in a fast-paced cyber challenge. Students will complete the challenge from 8:00 am until 12:00 pm with the top 3 teams receiving awards.

Each student in Round 2 of the Governor's High School Cyber Challenge will receive a voucher to take a Security + Bootcamp Course & Certification Exam Voucher (a $3,000 value!). Upon passing the exam, this certification qualifies students for direct entry into first level cyber personnel job positions.

8:30 AM - 8:35 AM
**Presentation of the Colors by the Michigan State Police Color Guard and Performance of the National Anthem by One AChord**

8:35 AM - 8:40 AM
**Welcome & Event Kick Off by Event Emcee**
***Kristin Judge***, CEO/President, Cybercrime Support Network

8:40 AM - 8:45 AM
**Opening Remarks from the State of Michigan CIO**
***David DeVries***, DTMB Director and State CIO, State of Michigan

8:45 AM - 9:10 AM
**Keynote Address - *Michigan Governor Rick Snyder***

9:10 AM - 9:35 AM
**Featured Speaker**
To be announced

9:35 AM - 10:05 AM
**Featured Speaker**

*A Representative from the Department of Homeland Security* (invited)

10:05 AM - 10:35 AM
**Networking Break and Visit with Sponsors**

10:35 AM - 11:20 AM
**Diamond/Platinum Ted Talk Session - Information Sharing and Effective Partnership for Cyber Security**
In today's cyber landscape it is imperative to collaborate to solve national cyber security problems. Our group of experts will discuss how to improve information sharing and build effective partnerships between the public and private sectors to counter cyber security issues.
Moderator: ***Rajiv Das***, Chief Security Officer and Deputy Director, State of Michigan Department of Technology, Management and Budget (DTMB)
Speaker: ***Michael Wyatt***, Principal, Cyber Risk, Deloitte & Touche LLP
Speaker: ***Paul Girardi***, Assistant Vice President Cybersecurity, AT&T
Speaker*:* ***Stewart Tan***, Cisco

11:20 AM - 12:05 PM
**Breakout Sessions - Attendees may choose one session to attend during each of the breakout sessions.**

**Thwarting a Cyberphysical Attack in the IoT Era**
While businesses and consumers see opportunity and efficiency in the billions of devices now connected to the Internet of Things and Industrial Internet of Things, cyber criminals also see an opportunity in the vulnerabilities created with each connection. This session will outline three things you need to understand in order to prevent a cyberphysical attack in our digitally connected world. Walk away with best practices you can use to implement the right mix of policy, architecture, regulation and technology to keep your organization secure.
***William J. Malik, CISA***, VP Infrastructure Strategies, Trend Micro

**Cyber Workforce Development: Advancing the Cybersecurity Pipeline Through Educational Ecosystems**
The cybersecurity talent gap is a familiar problem by now. Ubiquitous studies and speakers highlight the increased cybersecurity workforce talent gap. These conversations are now rote; What are the outstanding hurdles to fill the talent pipeline? Using actionable items on a reasonable budget, our panelists have successfully begun recruiting, training and retaining cyber talent. This discussion will provide information about fostering public and private collaborations to both attract and train entry level talent for the workforce, and recruit and retain mid level individuals and veterans - All at an attainable level of investment.
Moderator: ***Tonia Cronin***, Michigan Cyber Range Business Development Manager, Merit
Panelists:
***Pierrette Dagg***, Director of Marketing and Communications, Merit
***Jim Darga***, Director of the Pinckney Cyber Training Institute
***Kevin Hayes***, Chief Information Security Officer, Merit
***Cyndi Millns***, Professional Faculty-Cybersecurity, Merit
***Rebecca Steele***, Sales Leadership, Strategy and Business Development, Cisco
***Richard Schott***, Professor, Cyber Security Programs, Wayne State University

**Leveraging Security Diagnostics fo IAM Automation Strategies**

This session will discuss the strategies for executing a successful Identity Governance and Access Management Program along with leveraging diagnostics and automation strategies.
***Brian Dudek***, Sales Engineer, Data Strategy
***Rebecca Harvey***, Information Security Solutions Architect

**Security at the Speed of Trust**
This session will discuss promoting information sharing and collaboration by building trust-based relationships.
***Scott Larsen***, Director of Cybersecurity, Acting CISO, Beaumont Health

**Locking the IoT Back Door: Strategies for a Safer Smarthome**
The Internet of Things revolution has put smart devices in our suitcases, on our wrists, and in our homes. Like most technology during the early stages, cybersecurity implementation and maintenance has not been a priority. Learn about the IoT risks and how to avoid and mitigate them in the Smarthome.
***Ann-Marie Horcher, Ph.D.***, Central Michigan University

**Demonstrations by Kibbey The Michigan State Police Cyber Dog**
Kibbey is a 2 1/2 year old Labrador trained to locate electronics. Her services are used during search warrants for child exploitation, murder, narcotics and fire investigations. Join us for a demonstration of Kibbey in action and see what she can do for you!

**Cyber Range - Annual International Invitation Cyber Competition**
The International Cyber Exercise is a multi-team event that challenges the offensive and defensive cybersecurity skills of its participants. This year, National Guard teams from a range of states and their partner countries will face off in Alphaville, the virtual training environment created by the Michigan Cyber Range. Using open source tools and their own skills, teams will compete to control as many of Alphaville's network assets as possible. This event requires a high degree of group skill, as they will have to protect the devices they control while attacking other teams. The team controlling the most devices at the end of the day is declared the winner.

12:05 PM - 12:15 PM
**Transition to the Ballroom for Lunch**

12:15 PM - 1:15 PM
**Luncheon & Presentation of the High School Cyber Challenge Awards by Governor Rick Snyder**

1:15 PM - 1:45 PM
To be announced

1:45 PM - 2:25 AM
**NGA Panel Discussion: Cybersecurity in Practice: Meet the NGA Cyber Policy Academy**
In 2018, the National Governors Association chose Indiana, North Carolina, West Virginia, and Wisconsin to participate in the year-long NGA Policy Academy on Implementing State Cybersecurity. This panel will feature team leaders from Indiana, West Virginia, and Wisconsin, who will discuss each state's cybersecurity priorities and challenges.
Moderator: ***David Forscey***, Senior Policy Analyst, Homeland Security & Public Safety Division, National Governors Association
Panelists:

***David Cagigal***, CIO, State of Wisconsin
***Chetrice Mosley***, Cybersecurity Program Director, State of Indiana
***Joshua D. Spence***, Chief Information Security Officer, West Virginia Office of Technology

2:25 PM - 2:50 PM
**Networking Break, Visit with Sponsors and Transition to Breakout Sessions**

2:50 PM - 3:35 PM
**Breakout Sessions - Attendees may choose one session to attend during each of the breakout sessions.**

**How to Gain Ground on Cyber Attacker - State of Cyber Resilience**
Organizations are gaining ground on the damaging impact of targeted cyber attacks, proving that recent security investments are paying off. Despite the number of targeted cyber attacks doubling in the last year, companies are improving cyber resilience and demonstrating they can perform better under pressure. But there is more work to be done. Now is the time to build on this momentum by drawing on investment capacity to fully realize the benefits of cyber resilience. Accenture reveals five steps to close the gap on cyber attackers and continue to embed security into the fabric of their organizations within the next two to three years.
***Lalit K. Ahluwalia, CISSP, CIPP, PMP***, Managing Director - North America Security Lead (Health & Public Sector), Accenture

**Michigan Leadership in Vehicular Cybersecurity Training Initiatives**
Michigan is on the leading-edge of talent creation and acquisition with three unique programs revolving around groundbreaking vehicle cybersecurity training. The CyberAuto Challenge, CyberTruck Challenge, and trailblazing a flagship high school engineering automotive cybersecurity STEM program are just three of Michigan's creative way to tackle talent creation. Each event is unique, innovative, and being held as a role model not only by other states, but other countries who wish to emulate Michigan's success in these areas.
***Karl Heimer***, Principal, Heimer & Associates, LLC

**Shedding Some Light on the Dark Web**
Imagine being in a foreign location in complete darkness; it can be incredibly hard to make your way around. Now try and find something specific, or better yet, collect and gather information related to an idea, while in that same darkness. Join the Michigan State Police on a visit into the Dark Web. We will explain what the Dark Web is, information that has been found pertaining to Michigan and its organizations, as well as what the Michigan State Police can do for you and your organization.
***Dedicated Dark Web Intelligence Analyst within the Michigan Cyber Command Center***, Michigan State Police

**Fixing What is Fundamentally Broken in Cybersecurity with Former CISO, U.S. Air Force, Maj. General Earl Matthews (Ret.)**
Organizations have been managing security based on assumptions, hopes and prayers for decades. We assume our technology will detect and block that attack or leak, we hope our incident response techniques will be efficient and effective when under assault, and we pray that our security teams are well trained and practiced when everything goes wrong. But in many cases, we don't have a way to evaluate our security effectiveness let alone have any empirical evidence to back up our assumptions. In short, assumption-based security sucks. Assumption-based security results in many negative outcomes.

- Security tool overload and shelf-ware is being predicated on a tradition of purchasing too many security buzzwords, evaluating solutions incorrectly, purchasing the wrong solutions, not tuning what we have, not retiring antiquated solutions and burning through time, money and other resources. - Defensive regression is resulting in perhaps a once effective set of security controls no longer operating as desired because of configuration mistakes, loss of expertise and even malice. - Poor business decision making is occurring because most of us don't know if our security spend is making us more secure, if we are investing in the right areas or if we can even communicate the state of our security effectiveness to stakeholders. Enough is enough. We need to move beyond assumptions. We need to "know." We need to assess the efficacy of our security technology, talent and techniques. This presentation will focus on moving from assumption based security to continuous security validation and as it relates to security effectiveness.
***Earl Matthews, Maj Gen (ret)***, Chief Strategy Officer, Verodin, Inc.

**Demonstrations by Kibbey The Michigan State Police Cyber Dog**
Kibbey is a 2 1/2 year old Labrador trained to locate electronics. Her services are used during search warrants for child exploitation, murder, narcotics and fire investigations. Join us for a demonstration of Kibbey in action and see what she can do for you!

**Cyber Range - Annual International Invitation Cyber Competition**
Description: The International Cyber Exercise is a multi-team event that challenges the offensive and defensive cybersecurity skills of its participants. This year, National Guard teams from a range of states and their partner countries will face off in Alphaville, the virtual training environment created by the Michigan Cyber Range. Using open source tools and their own skills, teams will compete to control as many of Alphaville's network assets as possible. This event requires a high degree of group skill, as they will have to protect the devices they control while attacking other teams. The team controlling the most devices at the end of the day is declared the winner.

3:35 PM - 3:45 PM
**Networking Break and Visit with Sponsors**

3:45 PM - 4:30 PM
**Breakout Sessions - Attendees may choose one session to attend during each of the breakout sessions.**

**Automotive - A Security Integration Headache**
Creating a vehicle is a systems integration project. Multiple suppliers providing a solution to eventually then be integrated into the sellable product. Taking into account enterprise IT and the issues that system's integration providers have, it is clear to see why automotive cybersecurity is not simple. This presentation discusses different scenarios experienced where security hasn't been considered during the integration and vulnerabilities have been identified. There is then a shift to understanding how with a change in thinking, security vulnerabilities can be designed out to reduce security and overall safety risk.
***Thomas MacKenzie***, Associate Partner, X-Force Red, IBM
***Ivan Reedman***, Global Hardware Security and Capability Development Lead, X Force Red, IBM

**Penetration Testing for Patient Care**
"But we passed our penetration test," the person handling the security breach groaned. "How come they missed this?" Since the late 1960s, penetration testing has been about two things: demonstrating

that the system can be broken into and finding some vulnerabilities. But, by now? We all know systems can be broken into. The shock and surprise are gone. And we all know there are vulnerabilities. Scores of vulnerabilities. Too many vulnerabilities. In fact, arguably today's penetration testing doesn't even identify a fraction of the vulnerabilities. Repeating ourselves isn't working. This session will present a new strategy for penetration testing focused on protecting patient health and safety.
***J Wolfgang Goerlich***, SVP, Strategic Security Programs, CBI

**Trends and Strategies in Cybersecurity**
As your business invests in cloud and mobile technology, it's important to understand major security trends and events so you can strengthen your company's security posture. The security threat landscape is constantly changing, which is why we track and analyze security threats—such as software vulnerabilities, malware, botnets, and attacker tactics. This talk will cover these trends, including the impact ransomware had on businesses, takedown of the destructive Gamarue botnet and explain changes in attack vectors, and provide recommendations organizations can implement to help reduce their attack surface and protect networks and critical services from destructive attacks.
***Shawn Anderson***, Chief Security Advisor, Microsoft

**A Candid Conversation with a Car Hacker**
Matt Carpenter leads a team of elite cybersecurity researchers at GRIMM, a cybersecurity research firm dedicated to supporting the automotive industry by "breaking" their stuff and ensuring automakers are securing their vehicle electronics. During this conversation, attendees will have the opportunity to ask questions about how and why hackers hack cars (trains, planes, medical devices, etc.) and to understand the process and value to industry.
***Matt Carpenter***, Principal Researcher, GRIMM Cyber Research

**Demonstrations by Kibbey The Michigan State Police Cyber Dog**
Kibbey is a 2 1/2 year old Labrador trained to locate electronics. Her services are used during search warrants for child exploitation, murder, narcotics and fire investigations. Join us for a demonstration of Kibbey in action and see what she can do for you!

**Cyber Range - Annual International Invitation Cyber Competition**
Description: The International Cyber Exercise is a multi-team event that challenges the offensive and defensive cybersecurity skills of its participants. This year, National Guard teams from a range of states and their partner countries will face off in Alphaville, the virtual training environment created by the Michigan Cyber Range. Using open source tools and their own skills, teams will compete to control as many of Alphaville's network assets as possible. This event requires a high degree of group skill, as they will have to protect the devices they control while attacking other teams. The team controlling the most devices at the end of the day is declared the winner.

4:30 PM
**Adjournment**