2023 Michigan Cyber Summit
Wednesday, Oct. 18, 2023
Suburban Collection Showplace - Novi, Mich.
#MiCyberSummit
Agenda as of 10/11/23

Time	Agenda
8:00 a.m. – 12:00 p.m.	**2023 Governor's 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 the first round of the competition and have scored high enough to participate in the final round of the 2023 Governor's High School Cyber Challenge. The challenge will be competed in the morning with the awards being presented to the top three teams at the luncheon.
8:00 a.m.	**Registration, continental breakfast, and visit with sponsors in the display area**
9:00 a.m.	**Welcome & event kick off** Includes the National Anthem and the presentation of the colors by the Michigan State Police Color Guard. Caleb Buhs, Chief Deputy Director, Michigan Department of Technology, Management & Budget
9:05 a.m.	**Opening remarks** **Speaker:** Jayson Cavendish, Chief Security Officer, Michigan Department of Technology, Management & Budget
9:15 a.m.	**Panel discussion: Michigan cybersecurity strategic plan - Roadmap to prevention, response, and success** Cybersecurity efforts in Michigan's state government have been underway for many years and Michigan has an established effort in supporting overall cybersecurity. Join state agency experts to discuss the collaborative effort to expand upon the existing cybersecurity programs by bringing together distinguished leaders from both the public and private sectors to work together towards fortifying Michigan's digital infrastructure. The panelists will share their successes and insights as well as solutions that will bolster the state's collective defense against cyber threats and safeguard its critical data assets. **Moderator**: Major General Paul D. Rogers, Adjutant General and Director of the Michigan Department of Military and Veterans Affairs **Panelists**: Jayson Cavendish, Chief Security Officer, Michigan Department of Technology, Management & Budget Sarah Tennant, Senior Sector Development Director and Cyber Advisor, Michigan Economic Development Corporation Lt. Col. Chris Kelenske, Commander of the Field Support Bureau and Deputy Director, Michigan State Police

9:40 a.m.	**Panel discussion: Michigan Agencies – Working together to provide resources and foster relationships** Join our panel of agency experts to discuss the tools and resources available to assist with cyber incidents. Learn tips on how to be prepared and respond, as well as where to go for assistance. Panelists will share incident examples and discuss how working together creates a robust cybersecurity posture for Michigan. **Moderator**: Eric Swanson, Deputy Director, Michigan Department of Technology, Management & Budget **Panelists**: Detective 1st Lt. James Ellis, Cyber Commander, Michigan State Police |Michigan Cyber Command Center Lt. Col. John Brady, Commander, 272d Cyber Operations Squadron, Michigan National Guard Luke Thelen, IT Specialist, Michigan Department of Technology, Management & Budget
10:05 a.m.	**Diamond & Platinum sponsor panel discussion: The truth about passwordless authentication** Join our panel of experts for a discussion on the realities of passwordless authentication and the value adoption can provide to your organization. The session will debunk the myths regarding implementation and explore the benefits it can provide such as reducing the cost of an intermediate breech as well as providing a security environment that is harder to crack and less prone to the most common cybersecurity attacks. Discussion will include deciphering whether implementation obstacles are a result of the technology or are from organizational challenges. Our experts will share their implementation challenges and experiences to provide takeaways to help you enhance your system security. **Moderator:** Jack Harris, Chief Technology Officer, Michigan Department of Technology, Management & Budget **Panelists:** Eric Dull, Managing Director and AI Fellow, Deloitte Gabe Albert, Managing Director, Digital Identity Practice, Accenture Shane Harsch, Senior Solution Engineer, SentinelOne Jason Berland, Practice Director Identity and Access Management, Trace3 Cindy Qu, Senior Product Manager, Cisco/Duo Security
10:50 a.m.	**Networking break & visit with sponsors in the display area**
11:10 a.m.	**CIO panel discussion: State & local partnerships working together to create a transformational cybersecurity culture** Join our panel of state and local government chief information officers for dialogue on the current issues facing cybersecurity in the public sector. Discussion will include the cybersecurity implications within generative AI; evolving challenges with workforce development and talent retention; the increasing overlap with cybersecurity and fraud; and how forming partnerships can improve a whole-of-state cybersecurity culture. The panel will also focus on best practices on keeping cybersecurity at the forefront of digital government services. **Moderator**: Meredith Ward, Deputy Executive Director, National Association of State Chief Information Officers **State panelists**: Laura Clark, Chief Information Officer, State of Michigan, Chief Deputy Director, Michigan Department of Technology, Management & Budget Katrina Flory, State Chief Information Officer, Assistant Director, Ohio Department of Administrative Services

	Trina Zanow, Chief Information Officer, State of Wisconsin and Administrator, Division of Enterprise Technology **Local panelists**: Art Thompson, Chief Information Officer, City of Detroit Hector Roman, Chief Information Officer and Director of Information Technology, Wayne County Rod Davenport, Chief Information Officer, Oakland County
12:00 p.m.	**Transition to breakout sessions**
12:15 p.m.	**Breakout sessions -** Attendees may choose one session to attend during each of the breakout sessions.
	Security 2.0 - Building blocks of a modern security architecture Our current security architectures are continually challenged to prevent or even detect malicious actors. How can we take our security programs and architecture to the 'Security 2.0?' This talk walks through three major building blocks of a modern security architecture and its use of AI and automation to name some components. This interactive session will walk through explaining what capabilities are being seen in newer modern architectures and whiteboard an approach to build it out. **Speaker:** Joseph Daw, IBM Principal Security Architect, Americas
	How AI is transforming network security and user experience Today, we stand on the precipice of a remarkable technological transformation with the latest advancements in AI and machine learning and large-scale cloud adoption. Join the Palo Alto Networks team to learn about the key trends and top innovations that are powering the accelerated adoption of SASE. As states adopt SASE at an unprecedented pace, the key question that's emerging is around the right approach for effective implementation. In our time together, we will discuss why a unified approach can help you drive better security outcomes, modernize your branch offices, and automate complex and manual IT operations. **Speaker**: Fadi Fadhil, US SLED Field Strategist, Palo Alto Networks
	Strategies for building a resilient cybersecurity workforce Experienced and qualified security resources are hard to find, and yet the need for cybersecurity is escalating. Common challenges faced by organizations in scaling up their cybersecurity workforce include: • Closing a widening gap between vacant positions and the talent pipeline. • Retaining qualified security staff in a highly competitive market. • Providing employees with ongoing training and skill-building opportunities to support evolving business needs. Join us in exploring how organizations can upskill their IT teams to build cybersecurity maturity and resiliency. **Speaker**: Fritz Jean-Louis, Principal Research Advisor, Info-Tech Research Group
	Artificial intelligence: Friend or foe in the context of ransomware The industrial revolution was powered by coal and steam. They were the power that enabled innovation and propelled the world down the road that has brought us to where we are today. The next revolution is on the horizon, and it's an information revolution. Smartphones, smart homes, and smart assistants are proliferating our lives. Artificial intelligence is becoming in integral contributor to how this technology adds value to our lives. The capabilities of the cyber security ecosystem must keep pace with this evolution. During this session we will cover how artificial intelligence is being used to fuel the next generation of cyber security ecosystems. We will see how it can be used to improve accuracy, speed and efficiency of enforcement technologies while enhancing the information used to make business and security decisions. On the other hand, how could AI and machine learning be used against us? If we have the technology, so do our adversaries.

	Speaker: Anthony Sabaj, Head of Channel Security Engineering for the Americas, Check Point Software Technologies
	Beyond VPN: Securing your network with Zero Trust Network Access Organizations with workers accessing their networks on a multitude of devices and from a wide range of locations need a way to ensure that all incoming traffic is genuine. VPNs are no longer up to the challenge. They are frequently overloaded with too many users and often grant too much access to users who don't need it. Enter Zero Trust Network Access. Discussion will include: • VPNs then vs now. Why VPNs are no longer enough. • Zero Trust Network Access and how it works. • Examples of real-world attacks that could have been prevented with Zero Trust Network Access. • How to implement Zero Trust Network Access successfully. **Speaker**: Steve Fiorelli, Senior Solutions Architect, Barracuda Networks
	Cyber turbulence ahead - A front-line perspective on how to prepare for the coming wave of next-gen threats Cyberattacks generally reflect geopolitical conditions and economic realities. This is especially true in the public sector. 2023 was a year of both conflict and macroeconomic pressures that fostered innovation and evolution of cyberattacks. During this session, we will discuss what Mandiant has witnessed on the frontlines, responding to hundreds of cyber intrusions in 2023, and how those insights can help state government defenders better prepare for 2024. We will share the TTPS of the attackers as well as the trends in cyber-defense so public defenders can make more informed decisions. **Speaker**: Jon Ford, Senior Practice Leader, SLED Solutions, Google Public Sector
12:45 p.m.	**Transition to luncheon**
1:00 p.m.	**Luncheon and award announcements featuring Lt. Governor Garlin Gilchrist, II** Announcement of the top three teams of the 2023 Governor's High School Cyber Challenge.
2:00 p.m.	**Keynote session: Talent Development in Michigan** **Speakers:** Lt. Governor Garlin Gilchrist, II and Michelle Lange, Director, Michigan Department of Technology, Management & Budget
2:20 p.m.	**Featured speaker** Chris DeRusha, Federal Chief Information Security Officer, Office of Management and Budget and Deputy National Cyber Director, Office of the National Cyber Director
2:35 p.m.	**Panel discussion: Whole-of-state cybersecurity – A recipe for success** Join our panel of experts as they discuss the benefits of the whole of state cybersecurity approach which emphasizes support and partnerships among different levels of government, educational institutions, healthcare and other organizations in both the public and private sector. Discussion will include trends in talent development, funding, and tips for creating beneficial relationships and partnerships as well as provide information on the many resources available to help bolster your cybersecurity defenses. **Moderator**: Kelley Goldblatt, Supervisory Cybersecurity Advisor for Michigan and Ohio, Cybersecurity & Infrastructure Security Agency **Panelists**: Jayson Cavendish, Chief Security Officer, Michigan Department of Technology, Management & Budget Deb Fett, Chief Information Officer, Ingham County Bobby Hodges, Network Architect, Wayne County Regional Educational Service Agency

	Ashley Gelisse, CISSP, GIAC, Director, Office of the Chief Information Security Officer, Michigan Medicine
3:20 p.m.	**Networking break, visit with sponsors in the display area and transition to breakout sessions**
3:40 p.m.	**Breakout sessions** - Attendees may choose one session to attend during each of the breakout sessions.
	Money, money, money... Do you qualify? Join this interactive session to test your knowledge of how well you know the State and Local Cybersecurity Grant Program. An engaging panel of experts will provide information and real-life tips on navigating through the application process and address the most frequently asked questions. You will gain beneficial insight into the program and how it can work for your organization. **Moderator**: Michelle McClish, Senior Security Consultant, Michigan Department of Technology, Management & Budget | Michigan Cyber Partners **Panelists**: Kelley Goldblatt, Supervisory Cybersecurity Advisor for Michigan and Ohio, Cybersecurity & Infrastructure Security Agency Joe Polasek, State E-Rate Coordinator, Michigan Department of Education David Holcomb, Director of Information Technology, Hillsdale County Joni Harvey, Michigan State 911 Administrator, Michigan State Police
	Whole-of-state cybersecurity: The importance of collective defense Join us for a discussion on enhancing government security strategy through collaboration. Learn how the challenges of government can be mitigated by effective partnerships and the utilization of industry resources. In this session, you will gain insights on how to accelerate deployment and implementation, and how to improve incident response to reduce risks statewide. **Speaker**: Maria Thompson, Executive Government Advisor, Cybersecurity, Amazon Web Services
	Cybersecurity and what's next in tech The future of technology is moving at an incredibly rapid pace. Governments must make sense of this difficult technology landscape with the help of their partners. Being prepared for the future is never easy, but this discussion will provide an innovative look into what state and local governments can expect as technology continues to evolve at a rapid pace. **Speakers**: Phil Bertolini, Senior Vice President, e.Republic | Government Technology
	Asset visibility and intelligence - Eliminating the blind spots that exist across the public sector Discussion on how comprehensive asset visibility and rich contextual asset intelligence enables state and local IT teams to eliminate risk, reduce cost, and streamline operational workflows. **Speakers**: Curtis Simpson, Chief Information Security Officer, Armis John Evans, Chief Technology Advisor, State & Local Government & Education, World Wide Technology
	The five essentials of ransomware prevention To achieve optimal network security, you must implement a proactive and comprehensive approach to make your network a "hard target" capable of defending against ransomware and other damaging cyberattacks. This presentation will address five essential components of effective cyber defense. Attendees will learn that the common vulnerability scoring system is not a measure of risk, an effective basis for vulnerability prioritization must be dynamic and incorporate threat intelligence, and that risk scoring and tracking enables effective decision making. Attendees will also learn that an external view of their network is required to eliminate dangerous blind spots in identifying internet-facing assets as well as learn that active directory is the default path for

	ransomware attacks, and that effective management and continuous monitoring of that environment are essential to block attackers from achieving their objectives. **Speaker**: Chris Jensen, Public Sector Business Development Executive, Tenable
	Threats & trends: Cybercrime The presentation will discuss the current threats and trends that the Michigan Cyber Command Center is seeing and investigating. **Speaker**: D/Sgt. Torey Johns, Michigan State Police | Michigan Cyber Command Center
4:10 p.m.	**Transition to breakout sessions**
4:25 p.m.	**Breakout sessions** - Attendees may choose one session to attend during each of the breakout sessions.
	From security to privacy with encrypted computation In 2017, two professors at University of Michigan,Todd Austin and Valeria Bertacco, received a DARPA grant to build the Morpheus machine, a computing system that would defend against seven classes of cybersecurity attacks. After three years, they were the only team left standing in the program, beating secure system designs from Stanford, MIT, and Lockheed Martin and having been the only system in the program that was never hacked. Working with Intel Corporation and In-Q-Tel, the venture capital arm of the CIA, they have commercialized this technology in TrustForge for Azure and Amazon Web Services. In this talk, Todd will detail how a small Michigan startup was able to bend the rules of security in favor of the defenders and deliver next-generation technology for security and privacy-oriented applications in the cloud. **Speaker**: Amy Wirth, Chief Financial Officer, Agita Labs, Inc.
	Transportation cybersecurity in Michigan and TSA's role as both regulator and partner This session will cover the unique role that the Transportation Security Administration (TSA) has in cybersecurity for the transportation sector. TSA not only performs screening functions at U.S. airports but also regulates airports, airlines, pipeline, and rail companies. In doing so, TSA has taken on the challenge of helping those organizations implement the regulations while partnering with them to strengthen their cyber defenses. TSA partners with federal and state entities to train, educate, and discuss relevant cyber-threats to transportation. **Speakers**: Reginald Stephens II, Federal Security Director, Transportation Security Administration of Michigan William Byrne, Deputy Federal Security Director, Transportation Security Administration of Michigan Larry Marshall, Assistant Federal Security Director Inspections, Transportation Security Administration of Michigan Carissa VanderMey, Senior Liaison Officer to Cybersecurity Infrastructure Security Agency and Cybersecurity Coordinator for Security Operations, Transportation Security Administration of Michigan
	Artificial or intelligence? Or both? According to Elon Musk (Tesla), and Steve Wozniak (Apple founder), AI is a danger because of its potential for criminal exploit. The regulations and laws are close to non-existent. See the advantages and pitfalls of computer-generated answers and how it applies to cybersecurity related issues. **Speaker**: Ann-Marie Horcher, Ph.D., Cybersecurity Program Lead, Northwood University
	Incident response - Live tabletop This presentation will be a live demonstration of an incident response tabletop exercise designed to outline the benefits of conducting exercises within business and governments and provide attendees with first-hand experience of what an

	event like this would entail. The exercise will interact with the audience, relying on them to help drive the incident through each stage of the process. **Speaker**: Sean McKeever, Senior Security Researcher, GRIMM
	Lessons learned: Navigating a cybersecurity incident from the perspectives of a CISO Cyber incidents can happen at any time, but commonly happen at the end of the week or around holidays when staffing is limited. Having robust up-to-date incident response plans and a trained staff is critical to successfully navigating these events. Hear from a panel of healthcare Chief Information Security Officers how they've navigated cybersecurity issues with their incident response plans. Learn how their plans worked in real life, including best practices they have found and pitfalls they have run into. **Moderator**: George Goble, Chief Information Security Officer **Panelists**: Trent Carpenter, Chief Information Security Officer, Sparrow Health System Doug Copley, Chief Information Security Officer, AtlantiCare Health System Preston Jennings, Executive Vice President, Information Security and Chief Information Officer, Trinity Health Greg Sieg, Deputy Chief Information Security Officer and Director of Affiliate Information Assurance, University of Michigan-Michigan Medicine
	Zero Trust is going to cost how much: Budgeting ideas for a Zero Trust future Ransomware, malware, phishing, DDoS, social engineering, zero-day exploit, botnets…the list of types of attacks out there is long enough to keep even the most seasoned cybersecurity expert awake at night. As the cyber-attack surface grows, everyone working in the industry must be on the top of their game every minute of the day. The attacks continue to grow and expand while many federal, state and local budgets stay the same. At the same time, many of us have been tasked to begin building a pathway to a Zero Trust environment that seems out of reach for many small offices and budgets. So how can you plan for a Zero Trust future while working with budgets that are slow to grow? This session will explore some of the unique concepts and ideas that helped to create one of the most cutting-edge cybersecurity centers in the country. Hear from someone who has experienced the industry from both sides and understands what it takes to create a Zero Trust path that can be followed. **Speaker**: Brian S. Dennis, Principal Technologist for the Public Sector, Akamai Technologies
4:55 p.m.	**Adjournment**