2022 Michigan Cyber Summit
Thursday, Oct. 27, 2022
Suburban Collection Showplace - Novi, Mich.
#MiCyberSummit
Agenda

Time	Agenda
8:00 a.m. – 11:00 a.m.	**Governor's High School Cyber Challenge**
8:00 a.m.	**Registration, continental breakfast, and visit with sponsors in the display area.**
9:00 a.m.	**National anthem and presentation of the colors by the Michigan State Police Color Guard.**
9:10 a.m.	**Welcome & event kickoff** *Laura Clark*, Chief Information Officer and Chief Security Officer, Michigan Department of Technology, Management & Budget
9:15 a.m.	**Opening remarks from Gov. Gretchen Whitmer**
9:30 a.m.	**Keynote session – Fireside chat** Join our experts for a fireside chat to touch on the hottest topics in the cybersecurity ecosystem. The discussion will include the latest issues, threats, and innovations in cybersecurity protection. **Speakers:** *Jen Easterly*, Director of the Cybersecurity & Infrastructure Security Agency (CISA) *Laura Clark*, Chief Information Officer and Chief Security Officer, Michigan Department of Technology, Management & Budget
10:00 a.m.	**Panel discussion: Diamond & Platinum sponsors** Join industry leaders in a discussion focused on virtual reality and how it is changing the way business is conducted. Topic will include what the security implications are for virtual or augmented reality and how companies are using it in their day-to-day business. **Moderator**: *Cindy Peruchietti*, Senior Deputy Director, Agency Services, Michigan Department of Technology, Management & Budget **Panelists**: *Eddie Doyle*, Sales Leader, Check Point *Daryl Knopf*, Senior Solutions Architect, GitLab Representative from Deloitte Representative from Trace3
10:45 a.m.	**Networking break & visit with sponsors**
11:05 a.m.	**Panel discussion: Automotive IoT – A conversation on connectivity and the cybersecurity ecosystem in Michigan** Not since the days of Henry Ford has the automotive industry experienced such vast and dynamic change. The evolution of connected and automated cars, intelligent infrastructure, and the advancement of Artificial Intelligence and

	Machine Learning has placed cybersecurity in the heart of the future mobility movement. This panel of cyber-mobility professionals are pioneering a new digital era and tackling tough topics including automotive cybersecurity, smart cyber policymaking, automotive cyber crime, and preparing the next generation of cyber workforce while recognizing the value of hackers. **Moderator**: *Jennifer Tisdale*, CEO, GRIMM **Panelists**: *Kelly Bartlett*, Connected and Automated Vehicle Specialist, Michigan Department of Transportation *Kristie Pfosi*, Executive Director of Product Cybersecurity, Aptiv *Ron Kraus*, Cyber Specialist, Michigan State Police *Samir Tout, Ph.D.*, Professor, Information Security and Applied Computing
11:50 a.m.	**Transition to breakout sessions**
12:00 p.m.	**Breakout sessions -** Attendees may choose one session to attend during each of the breakout sessions.
	The state of cybersecurity, a current view into ransomware The session will cover ransomware groups we are currently tracking, trends and common techniques that attackers use for ransomware attacks based on the MITRE ATT&CK tactics. **Speaker**: *Terence Jackson*, Chief Security Advisor, Microsoft
	Keeping your remote workers productive and secure - A SASE Zero Trust approach The hybrid workforce and direct-to-app architectures have rendered legacy security architectures obsolete while dramatically increasing our attack surface. Cloud based security offerings have emerged, but they can offer only inconsistent and incomplete protections, as well as, deliver poor performance and user experiences. This session will explain a modern approach to ZTNA and how it is imperative to leverage it's key principles to securely keep remote workers productive and secure. **Speaker**: *Carlos Valarezo*, North America SASE Sales Leader, Public Sector, Palo Alto Networks
	Connecting intelligence to risk for an executive audience The consensus on intelligence is that actionability is critical to a return on security investment. "Actionable" means driving security outcomes that are straightforward to measure and communicate. "Actionability for executives" means translating intelligence into the language of business - risk, which is easier said than done. We've created and tested a framework that simplifies this challenge. During this session, you'll learn how to uncover second-order threat implications, clearly define risk, and convey threat intelligence insights in a way that resonates with executives. **Speake**r: *Levi Gundert*, SVP of Global Intelligence, Recorded Future
	Secure and resilient public services When we look at the threat landscape for public services, it's the perfect storm. There's an exponential growth in cyberattacks while there's an extreme shortage in cybersecurity talent. This presentation provides an overview of the cybersecurity threat landscape for public services, as well as, three initiatives CISOs can take to jump start their security and resiliency journey. **Speaker**: *Michele Myauo, Ph.D.*, North America Public Service Security Lead, Accenture
	State of software security **Speaker**: A representative from Veracode
12:30 p.m.	**Transition to luncheon**
12:40 p.m.	**Luncheon and award announcements with Lt. Gov. Garlin Gilchrist II**

	Announcement of the CyberPatriot and Governor's High School Cyber Challenge awards.
1:40 p.m.	**Featured speaker** *To be announced*
1:55 p.m.	**Panel discussion: CIO panel** Hear from state, federal and city agency leaders discussing cybersecurity issues, response to challenges faced, and future outlook. **Moderator**: *Doug Robinson*, Executive Director, National Association of State Chief Information Officers (NASCIO) **Panelists**: *Tracy Barnes*, Chief Information Officer, State of Indiana *Laura Clark*, Chief Information Officer and Chief Security Officer, Michigan Department of Technology, Management & Budget *Katrina Flory*, State Chief Information Officer/Assistant Director, State of Ohio *Joshua Spence*, Chief Information Officer, West Virginia Office of Technology *Art Thompson*, Chief Information Officer, City of Detroit
2:40 p.m.	**Networking break & visit with sponsors**
3:00 p.m.	**Breakout sessions** - Attendees may choose one session to attend during each of the breakout sessions.
	Digital transportation - Cloud as cybersecurity risk reduction Public cloud adoption can serve as the center point for digital transformation efforts. As organizations grapple with increasing challenges from adversaries and a call for increased transformation efforts, to include an improved cybersecurity posture, the drivers to consider a heavy investment in the adoption of cloud become increasingly compelling. **Speakers**: *MK Palmore*, Director, Office of the CISO, Google Cloud and *Vinesh Prasanna Manoharan*, Customer Engineer Lead, Google
	What is zero trust, and does it necessarily have to be difficult to gain benefits from implementing it? Attack surfaces and techniques are evolving, and traditional security models have failed to keep up. The Zero Trust model is unique in that it requires verification of everyone, whether they reside inside or outside of your network, removing that network perimeter mentality from your security landscape. In this session we will discuss the reasoning behind the Zero Trust model, the value it can provide and how it can be incorporated into security designs to gain a better security posture. **Speaker**: *Nic Cantu*, Solutions Engineer, Trend Micro
	Lessons from the field - Vulnerability disclosure and bug bounty program management Attendees will learn how a Vulnerability Disclosure Program (VDP) can be a vital tool in securing their business and products against today's cyber security challenges. This presentation will outline the differences between a VDP and a bug bounty, why you would want one, or both; and share real world experiences running a program for an automotive OEM. **Speakers**: *Sean McKeever*, Program Manager, GRIMM and *Jennifer Tisdale*, CEO, GRIMM
	The dark web: A playground for threat actors & scammers The term dark web can be found in the news nearly every day. Join the Michigan State Police and the Michigan Cyber Command Center, as they explain what the dark web is, who is accessing it, and provide a deep dive into the dark web landscape of recent, common threats, and scams. **Speaker**: *Samuel North*, Detective Sergeant, Michigan State Police
	Fireside chat: Privacy and preserving data collaboration methods that accelerate healthcare innovation In the continued quest to improve patient outcomes and lower costs, healthcare organizations are looking to technology, particularly advances in the field of artificial intelligence to spur exciting innovations. Such innovations have the

	potential to help with disease prediction and diagnosis, effective treatment selection and prognosis, life sciences and pharmaceutical research, epidemiology, public health, and precision health initiatives. While these approaches hold great promise to fuel future breakthroughs in healthcare and care delivery, they require access to sufficient qualities of diverse data for the development and validation of models capable of consistent performance. Thanks to electronic health records, medical devices, and personal smart devices, as well as, data collected in groundbreaking research studies at different academic medical centers around the globe, more data is available than ever before. The problem, however, lies in how to safely and ethically access, integrate, and then analyze the information while preserving individual privacy. **Facilitator**: *Preston Jennings*, VP, Information Security & Chief Information Security Officer, Trinity Health **Speaker**: *Chris Gough*, Worldwide General Manager Intel Health & Life Sciences, Intel Americas, Inc.
3:30 p.m.	**Transition to breakout sessions**
3:40 p.m.	**Breakout sessions** - Attendees may choose one session to attend during each of the breakout sessions.
	Risk management: Hindsight is 2020 Risk. We measure it. We model it. We prioritize security and communicate concerns using risk. But do we get action from the business? Often, no. Security teams aren't alone in this failure. The human condition is one of ignoring risk, as the recent pandemic clearly demonstrated. This session reviews behavior science research and explains how to transform risk management to gain buy-in and action. **Speaker**: *J. Wolfgang Goerlich*, Advisory CISO, Cisco
	Cyber insurance and the next phase With the rise in ransomware and social engineering events on all levels of organizations the cyber insurance industry is undergoing a significant shift. This rise in claims has resulted in rates increasing anywhere from 10-300%, and coverage applications now require a more robust security infrastructure before being considered for renewal. We will discuss these changes and how an organization can put themselves in the best position to meet security requirements and secure cyber insurance coverage. **Speaker**: *James R. Parry, Jr.*, Senior Vice President, Mason McBride
	Artificial intelligence cybersecurity threats Artificial intelligence (AI) is one of the most exciting and promising technologies to gain widespread adoption in recent memory. AI has the potential to impact a broad range of industries and verticals, and is currently providing a transformative impact in Michigan and across the globe. With the widespread adoption of AI comes a variety of challenges including cybersecurity implications. This presentation will focus on two cybersecurity issues: the security of AI applications, and the use of AI as a cybersecurity threat. **Speakers**: *Greg Gogolin, Ph.*D., Director of Cybersecurity & Data Science, Ferris State University and *Kasey Thompson*, Ferris State University
	Build ransomware resilience Sophisticated ransomware attacks are increasing and evolving quickly. Emerging ransomware strains can encrypt, corrupt, and delete backups in only a few hours, which makes recovery a grueling challenge. Learn how to shift your organization from a reactive model to a proactive approach that emphasizes resilience and mitigates the risk of an attack. **Speaker**: *Michel Hebert*, Research Director, Info-Tech Research Group
	Adopting a zero trust environment Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated. Join Kevin McLaughlin as he shares a collection of zero trust concepts designed to

	prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible. **Speaker**: *Kevin McLaughlin, Ph.D.*, Vice President, Cyber Security, Cyber Risk and IT Compliance, Stryker
4:10 p.m.	**Adjournment**