



2021 Michigan Cyber Summit
Thursday, Oct. 21 - Virtual Conference
Agenda

Time	Agenda
7:45 a.m.	Networking & visit with the sponsors in virtual booths
8:30 a.m.	Welcome & opening remarks <i>Laura Clark</i> , Chief Security Officer & Deputy Director, Michigan Department of Technology, Management & Budget <i>Julia Dale</i> , Director, Michigan Department of Technology, Management & Budget
8:35 a.m.	A message from Gov. Gretchen Whitmer
8:45 a.m.	Keynote Speaker Chris DeRusha will speak about the Biden Administration's cybersecurity goals. Areas of focus will include the Executive Order on improving the nation's cybersecurity, technology, modernization, and zero trust architecture. <i>Chris DeRusha</i> , Federal CISO, The White House
9:00 a.m.	State CIO panel discussion Hear the latest from CIOs in this roundtable discussion covering important topics impacting government IT and Security. Participants from Ohio, Indiana, and Michigan's Ingham County will lend their expertise and insights in tackling challenges and providing secure digital services to residents and businesses. Moderator: <i>Eric Swanson</i> , Director, Center for Shared Solutions, Michigan Department of Technology, Management & Budget Panelists: <i>Katrina Flory</i> , State Chief Information Officer/Assistant Director, Ohio Department of Administrative Services, Office of Information Technology <i>Tracy E. Barnes</i> , Chief Information Officer, State of Indiana <i>Deb Fett</i> , CIO, Ingham County, Michigan
10:00 a.m.	Remarks from government leaders <i>Paul C. Ajegba, P.E.</i> Director, Michigan Department of Transportation
10:05 a.m.	Break & visit with sponsors in virtual booths
10:20 a.m.	Remarks from government leaders <i>U.S. Sen. Gary Peters</i>
10:25 a.m.	Diamond sponsor panel discussion: Diversity & inclusion Countless studies have shown clear imbalances in the demographics of the country's cybersecurity professionals, depriving government and private organizations alike of potential resources to better secure themselves. This panel will feature a discussion of the challenges in expanding the diversity of the

	<p>cybersecurity workforce, possible solutions, and the experiences of those who have done it.</p> <p>Moderator: <i>Shamia Jenkins</i>, Senior Manager Deloitte Consulting Human Capital Practice, Deloitte Consulting LLP</p> <p>Panelists: <i>Lea Hurley</i>, Managing Director, Government & Public Services Cyber Risk Services, Deloitte & Touche LLP <i>Ti'Kyra Napoleon</i>, Equity and Inclusion Officer, Michigan Department of Technology, Management & Budget <i>Poppy Hernandez</i>, Chief Equity & Inclusion Officer, Executive Office of the Governor, State of Michigan</p>
11:25 a.m.	<p>Breakout sessions - Attendees may choose one session to attend during each of the breakout sessions.</p>
	<p>Modernizing the cybersecurity landscape to meet the needs of a changing workforce & higher education</p> <p>We have seen modernization initiatives trending higher in recent years at the state and local government and higher education levels. There are many examples of drivers associated with the higher trends such as an increase in cybersecurity threats like SolarWinds. Recently, President Biden issued an Executive Order related to modernizing cybersecurity tools at warp speed and governments are taking notice. With the pandemic we have seen the workforce change dramatically culminating an escalated demand for remote work which by nature introduces additional cybersecurity risks. GitLab not only modernizes current workflow process but also automates security scans to catch vulnerabilities with built-in mitigation processes at time of the application inception.</p> <p>Speaker: <i>Daryl Knopf</i>, Senior Solutions Architect, GitLab</p>
	<p>Dispelling the mobile myth</p> <p>There is a myth that mobile devices are inherently secure. But the numbers don't lie; over 35,000,000 pieces of mobile malware have impacted both iOS and Android, along with billions of phishing attempts and countless, and a rising number of zero-day vulnerabilities. With 60% of corporate-connect endpoints being unsecured mobile devices, enterprises must consider all four attack vectors - device, network, application, and phishing - and their impact on the enterprise attack surface. While mobile device management helps control aspects of device configuration, these legacy management toolsets only provide rudimentary jailbreak detection, leaving enterprises with a false sense of security. Join us for a session on the common mobile threat vectors, real-world exploits, and a demonstration of just how simple it can be to gain a toehold into an enterprise's infrastructure using mobile device exploitation. Attendees will not only learn about the mobile attack vectors exploited by cybercriminals at all levels of experience but how to minimize their enterprise's mobile attack surface and keep personal and corporate data safe.</p> <p>Speaker: <i>Kern Smith</i>, Vice President, Americas Pre-Sales Organization, Zimperium</p>
	<p>Never trust. Always verify.</p> <p>Humans are inherently both trusting and distrusting, without even knowing it. We pick up on innumerable subtle micro expressions and nuances of our environment, instantly spotting what's out of place. Without a second thought, our computer brains process and alert us to "things out of place" and focus our attention, silencing distractions so we can verify trust. In this session, Eddie Doyle will demonstrate that when we design systems after our neurobiology, we can focus our networks to eliminate threats in much the same manner as our natural born instincts.</p> <p>Speaker: <i>Eddie Doyle</i>, Cyber Security Evangelist, Check Point Software Technologies</p>
	<p>Cybersecurity education: Trends in training & development of the cyber</p>

	<p>workforce What kinds of cybersecurity training are available, and what does this mean for students, teachers, and professionals? Explore the common and uncommon pathways into a cybersecurity career, and how schools can foster the cybersecurity workforce. Speaker: <i>Helen Patton</i>, Advisory CISO, Cisco</p>
11:55 a.m.	Lunchbreak & visit with sponsors in virtual booths
12:55 p.m.	Award Announcements with Lt. Gov. Garlin Gilchrist II Announcement of the CyberPatriot and Governor’s High School Cyber Challenge awards.
1:10 p.m.	Remarks from government leaders <i>U.S. Rep. Peter Meijer</i>
1:15 p.m.	<p>Panel discussion: State of the state in cybersecurity Hear from state and federal agency leaders and experts describing Michigan’s overall cybersecurity position, response to challenges faced, and future outlook. Moderator: <i>Andy Brush</i>, Cyber Partners Program Lead, Michigan Department of Technology, Management & Budget Panelists: <i>D/F/Lt. James Ellis</i>, Cyber Command, Michigan State Police <i>Lt. Col. John Brady</i>, Commander, 272d Cyber Operations Squadron, Michigan Air National Guard <i>Jayson Cavendish</i>, Deputy Chief Security Officer, Michigan Department of Technology, Management & Budget <i>Kelley Goldblatt</i>, Cybersecurity Advisor, Cybersecurity and Infrastructure Security Agency <i>Anthony Rodgers</i>, Director of Technology Transformation Services, Michigan Department of Technology, Management & Budget</p>
2:00 p.m.	Breakout sessions - Attendees may choose one session to attend during each of the breakout sessions.
	<p>Silver sponsor session Cyberattacks 2021: Recent events have taught us there is no slow-down in pace at which we are incurring cyberattacks. The global ransomware crisis has entered a new phase, as threat actors adopt stronger pressure tactics and new targets— with attacks often highlighting weaknesses in an organization’s security posture. Learn how you can prepare, prevent, and respond as our environment changes. Speaker: <i>Doug LaGore</i>, Managing Director, Midwest Security Lead, Accenture</p> <p>Microsoft's perspectives on the cyber threat landscape & how we help defend you: Cyber adversaries continue to probe and attack citizens, governments, and critical infrastructure providers, and we expect this to worsen. Understanding the threat landscape, detecting threat activity, and remaining resilient from attacks increasingly requires you to collect, analyze, and bring context to various sets of data. In this session, Mark McIntyre will discuss Microsoft’s global cybersecurity detection capabilities, share findings from our recent Digital Defense Report, and provide practical recommendations for the state and its partners. Speaker: <i>Mark McIntyre</i>, Chief Security Advisor, Microsoft's Security Solutions Area, Microsoft</p>
	<p>Security modernization in government: A focus on zero trust Zero trust is a conceptual framework that helps organizations secure the ubiquitous nature of modern enterprise environments. This session will focus on latest imperatives in government with zero trust, misconceptions, benefits, and guiding principles to action. Speaker: <i>Daniel Jones</i>, Manager, Deloitte Cyber & Strategic Risk Government & Public Services Zero Trust SME, Deloitte & Touche LLP</p>
	The Michigan Cyber Civilian Corps (MiC3)

	<p>The MiC3 is Michigan's own group of trained, civilian technical experts who volunteer to provide rapid response assistance to the state of Michigan in the event of a cyber incident. In this session we will review the history and evolution of the group, recent learnings, and discuss transitions related to the "new normal".</p> <p>Speaker: <i>Ray Davidson, PhD, Office of the CSO, MiC3</i></p>
	<p>Left of boom: Michigan cyber partners approach to collaborative security</p> <p>Learn how Michigan is taking a whole of government approach to improving cyber resilience of public organizations across the state.</p> <p>Speaker: <i>Andy Brush, Cyber Partners Program Lead, Michigan Department of Technology, Management & Budget</i></p>
2:30 p.m.	Networking break & visit with sponsors in virtual booths
2:45 p.m.	<p>Remarks from government leaders</p> <p><i>U.S. Rep. Elissa Slotkin</i></p>
2:50 p.m.	<p>Panel discussion: Critical infrastructure & cyber</p> <p>Cyberattacks have significantly expanded from traditional corporate and public sector networks to our core critical infrastructure that all residents rely on day to day. From pipelines to the food industry to water departments, cyber threat actors are compromising organizations and demanding millions of dollars in ransomware. This panel will discuss how the recent influx of cyberattacks against critical infrastructure across the U.S. have impacted their organizations overall, what they are doing to prevent similar attacks, and what challenges they face in the current threat landscape.</p> <p>Moderator: <i>Brad Pagratis, Information Management Division Director, Michigan Department of Environment, Great Lakes and Energy</i></p> <p>Panelists:</p> <p><i>Jim Beechey, Executive Director Security, Consumers Energy</i></p> <p><i>Rod Davenport, Chief Information Officer, Lansing Board of Water & Light</i></p> <p><i>Dan Rainey, Chief Information Officer, City of Detroit Water and Sewerage Department</i></p>
3:35 p.m.	<p>Final remarks & event closing</p> <p><i>Laura Clark, Chief Security Officer & Deputy Director, Michigan Department of Technology, Management & Budget</i></p>
3:50 – 5:00 p.m.	Visit with sponsors in virtual booths