MiSecure

MiSecure Legislative Report 2023-2024

Ingham ISD

Dear Legislators and Stakeholders,

We are excited to share this report on the MiSecure initiative, a program that has elevated cybersecurity protections for Michigan's K-12 schools. Through collaboration, innovation, and unwavering dedication, MiSecure is ensuring safer schools, uninterrupted education, and the trust of our communities.

Made possible by the School Aid Fund section 97g, MiSecure established Michigan's first K-12 Security Operations Center (SOC) and implemented advanced Managed Detection and Response (MDR) software to protect critical infrastructure. Since its inception, MiSecure has assisted in six major cyber incidents and many minor incidents, showcasing the power of early detection and the value of statewide collaboration in preventing disruptions.

We extend our deepest gratitude to Senator Sarah Anthony and Representative Angela Witwer for their support of this vision and their commitment to ensuring the safety and continuity of Michigan's educational systems. Their leadership has been instrumental in bringing MiSecure to life.

This report highlights the accomplishments achieved so far and the foundation laid for the future. We encourage you to connect with us to learn more about this vital work and the ongoing efforts to secure Michigan's schools.

Thank you for your continued support.

With appreciation,

Jason Mellema
Superintendent
Ingham Intermediate School District

Dr. John Severson
Executive Director
Michigan Association of Intermediate School Administrators

Michael Lilly
Executive Director of IT
Ingham Intermediate School District

Matt McMahon
Director of MiSecure
Michigan Association of Intermediate School Administrators

Tammy Evans
MiCH IT Director
Michigan Association of Intermediate School Administrators

Tom Johnson
Director Michigan Collaboration Hub
Michigan Association of Intermediate School Administrators

Forward

We are proud to celebrate the remarkable progress achieved through the MiSecure initiative. This collaborative effort reflects a statewide commitment to protecting Michigan's K-12 schools against ever-evolving cyber threats.

The establishment of Michigan's first K-12 Security Operations Center (SOC) has proven transformative, providing essential support to schools across the state. Since its launch, the SOC has assisted in six (6) major cybersecurity incidents, demonstrating the value of having a centralized team equipped with advanced tools and expertise. Early detection capabilities provided by the program's Managed Detection and Response (MDR) software have been instrumental in identifying and mitigating threats before they could cause significant harm.

The success of this initiative goes beyond protecting technology infrastructure; it ensures that schools remain open and operational, preserving valuable instructional time and safeguarding community trust. The MiSecure program underscores how collaboration among educational, technological, and governmental entities can address critical challenges while setting a precedent for future efforts.

We extend our gratitude to Ingham Intermediate School District, MAISA, METL, the MiSecure Advisory Board, and all the participating districts for their leadership and vision. Together, they have built a model for cybersecurity that protects not only our schools but the futures of Michigan's students.

Signed,

Roger Blake
President & CEO
Merit Network, Inc.

Jayson Cavendish
Chief Security Officer (CSO)
State of Michigan, Michigan Dept. of Technology, Management & Budget

D/F/Lt. James Ellis
Cyber Commander
Michigan State Police

Amy Guilford
Chief Program Administrator
SET SEG

Michelle McClish
State Assistant Administrator
Michigan Cyber Security External Engagements Lead

Table of Contents

Executive Summary

In 2023, Michigan launched MiSecure, a transformative initiative designed to protect K-12 schools from cyber threats. Backed by $9 million in legislative funding, MiSecure established the state's first K-12 Security Operations Center (SOC) and implemented Managed Detection and Response (MDR) solutions to safeguard critical infrastructure. This program, driven by the collaboration of Ingham Intermediate School District, Michigan Educational Technology Leaders (METL), Michigan Association of Intermediate School Administrators (MAISA), and Senator Sarah Anthony and Representative Angela Witwer, represents a vital step forward in securing education.

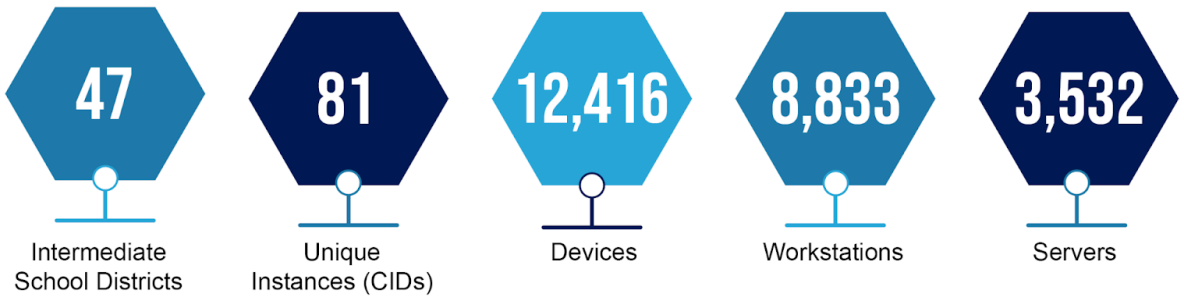
From Vision to Action

What began as a legislative goal for cybersecurity assessments evolved into a comprehensive protection plan through the leadership of Ingham ISD and its partners. By deploying MDR software and building the SOC, MiSecure not only identifies and mitigates threats but also provides expert guidance and a critical escalation point for districts across the state.

Proven Success in Protecting Schools

MiSecure's unique combination of technology and people has prevented disruptions, strengthened defenses, and protected community trust. Key achievements include:

- **Cybersecurity Incident Response**: In 2024, MiSecure successfully prevented multiple cyberattacks from disrupting education. In one case, a ransomware attempt was stopped on the eve of the first day of school, allowing operations to continue seamlessly. In another instance, suspicious login activity identified by MiSecure led to timely interventions that stopped a potential breach.
- **Cost Efficiency**: Statewide procurement saved over $5.3 million on MDR licenses, enabling districts to access critical technology affordably.
- **Widespread Participation**: MiSecure protected over 12,000 devices across Districts in 47 ISDs, with additional districts onboarding as part of Phase 2.



Leadership and Collaboration

The SOC has proven invaluable as both a crisis partner and a proactive leader. MiSecure's expert team provides districts with training, consulting, and standardized response strategies. By fostering statewide collaboration, the SOC has elevated cybersecurity readiness across Michigan's education system.

Phase 2 of MiSecure aims to expand participation and strengthen defenses, ensuring every district can benefit from this proactive model. The program's early successes demonstrate the critical need for sustained funding and investment to protect schools from evolving threats.

Gratitude

This success is a testament to the leadership of Ingham ISD, METL, MAISA, and Michigan lawmakers. Their vision and commitment have ensured that Michigan's schools are safer, its communities are more secure, and its education system is prepared for the challenges ahead.

MiSecure Success Stories:

Large Incident Response

On July 19th, 2024 the MiSecure Operations Team was put to the test. Due to a software bug that impacted devices throughout the world, many Michigan K12 servers crashed. As soon as they were alerted to the issue, the MiSecure Operations Team opened a virtual help desk to support schools as they began restoring operations. Furthermore, this team used tools provided by a major security vendor to identify servers that were impacted and shared this information with each ISD individually. The impact on other organizations was significant and in some cases lasted days and weeks. Due to MiSecure's quick response and leadership and more importantly, the attention of Michigan's K12 IT staff, 90% of servers were operational by 10 am that same day. An Executive Briefing was prepared and shared with superintendents throughout the state and is included in Appendix D.

Defending Against Cybersecurity Attacks

School Example 1:
August 19, 2024 was the first day of school for students in one Michigan district. An attacker, having previously stolen a district staff member's credentials to gain access to their district network, launched a cyber attack. One-by-one they gained access to seven district servers, but each of these had the MiSecure provided MDR software running. Each server stopped the encryption software from executing and isolated the server from further access. District personnel were alerted. With the help of the MiSecure team, by 11:00 am, just 5 hours after the attack, the intruder's access had been removed, the district firewall was locked down, and servers were reviewed and returned to service. Additional recommended cybersecurity measures were implemented and school continued uninterrupted. A cybersecurity insurance claim was not needed and no instruction time was lost. The only impact was that staff were required to reset their passwords as a measure of caution.

School Example 2:
A district in Michigan's Upper Peninsula reached out to the MiSecure Operations Team when they observed a spike in "Failed logins" in their MDR security console. After an investigation, it was determined that a hacker was attempting to establish a remote connection into the district's network. The district, aware that their remote connection service was exposed to the Internet, was able to act quickly to enable protections without incident.

School Example 3:
In the early morning hours of October, the MDR Security called district technicians and the MiSecure Operations Team to alert them of a possible attack. The MDR service provider had observed failed attempts to access servers using patterns it had previously seen. The district investigated and discovered an attacker had gained access to their network and was in the early

stages of launching a cyber attack. Their access was removed and the network was secured from future attacks.

What Impacted Districts Are Saying

- “I want to say a big thank you to you and your team for the assistance and extra eyes on the incident at [our district]”
- “[MDR Vendor] really came through and stopped this incident from exploding into a more severe incident as the attackers found multiple weaknesses and attacked them despite the district taking various precautions”
- “They were not too far away from deploying payloads as if they had more time, I have no doubts they would have been able to do it as they have a domain admin account at their disposal”
- “The logging you did on this incident was great to see, as it's hard to document and analyze logs”
- “This, so far was a huge win for the MiSecure MDR service”
- “We didn't have to shut down school and the service stopped the bad actor just in time from deploying bad payloads”

Governance

Having received the 97g funds, the responsibility for fiscal oversight for MiSecure is through Ingham Intermediate School District. Ingham ISD selected MAISA as the statewide educational organization to establish and manage the MiSecure Operations Team and to ensure that the key measures outlined in the legislation are met. One such measure was to establish an advisory board to oversee the implementation of the project.

The MiSecure Advisory Board is made up of representatives from each of the 10 MAISA regions, ensuring equitable access to the resources provided by the operations team. In addition to the educational representatives, several other agencies are included:

- Cybersecurity and Infrastructure Security Agency (CISA)
- Michigan Statewide Educational Network (MISEN)
- Michigan State Police, Cyber Command Center (MC3)
- Department of Technology Management and Budget (DTMB)
- Michigan Department of Education (MDE)

Appendix B provides the current list of advisors.

Background

From the 2023-24 School Aid Fund, section 97g allocated $9,000,000 in one-time funding to provide for a statewide K12 Security Operations Center (SOC) and Managed Detection and Response (MDR) services to ISDs, local districts, and PSAs in the State of Michigan. Funding was secured through Ingham ISD which worked with the Michigan Association of Intermediate School Administrators (MAISA) to establish this SOC. The Michigan Education Technology Leaders (METL) had previously formed the MiSecure Cybersecurity Task Force and the work of this team laid the groundwork for the new MiSecure Operations Team.

The success of this newly formed MiSecure Operations Team is due in no small measure to the previous work of the METL Cybersecurity Task Force. Over the past 5 years, that team, made up of Michigan K12 IT leaders as well as representatives from DTMB, MDE, Michigan State Police, CISA, Merit Networks and SET-SEG, has provided:

- A comprehensive cybersecurity guide: “Essential Cybersecurity Practices for K12“
- On-demand video training for educators: “Cybersecurity for Educators - How to Become a Human Firewall”
- An online cybersecurity assessment tool, the MiSecure Quick Self-Audit
- Incident response planning tools

This work laid the foundation for the formation of a dedicated staff to assist schools in utilizing these resources as well as implementing the funded MDR solution.

The MiSecure Operations Team is focused on providing advocacy and leadership around cybersecurity tools and practices for all Michigan schools. As directed in the 97g language,

MiSecure selected and made available a high quality MDR system for all critical servers in every ISD, local district, and PSA.

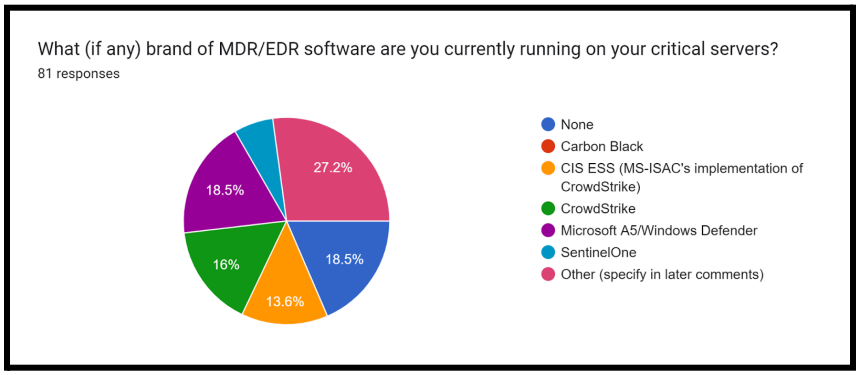
This MDR software can stop suspicious software installation, remove a machine from network access, report on known vulnerabilities, and alert local IT staff of any issues 24x7x365 utilizing a team of dedicated cybersecurity experts. This allows districts to focus on cybersecurity improvements, technology operations, and student and educator support. With the assistance of MiSecure cybersecurity experts, the insights provided by the MDR software can be reviewed and specific areas of improvement identified and remediations planned.

Progress

- September, 2023: After reaching an initial agreement with Ingham ISD to manage the MiSecure project, MAISA hired the MiSecure Director
- September, 2023: The project is announced at the Michigan Association of Superintendents & Administrators (MASA) during their fall conference
- October, 2023: State of Michigan establishes first ever K12 Security Operations Center (SOC)
- October, 2023: MDR research begins
- January, 2024: Participation survey is released
- January, 2024: First Cybersecurity Analyst is hired
- April, 2024: MiSecure coordinates efforts with DTMB to identify supported MDR products
- April, 2024: Selected MDR solution serving as MiSecure's 24x7 cybersecurity protection software
- April, 2024: MAISA negotiates significant costs savings for a MDR solution, resulting in $5,367,600 savings over the 3 year contract term
- May, 2024: Second Cybersecurity Analyst is hired
- June, 2024: MiSecure offers pre-bid, extended pricing on additional, optional licenses at an approximate 70% discount from MSRP, resulting in $1,473,573.84 savings over the 3 year contract term
- June, 2024: Third Cybersecurity Analyst is hired
- August, 2024: MiSecure Security Operations Team works with a participating district to address a cybersecurity incident identified by and mitigated by the provided MDR software
- September, 2024: MiSecure initiates regular, in-person SOC reviews with ISDSs

Participation

An initial participation survey was conducted of ISDs with a 82% return rate. In response to a question about whether their servers were protected 24x7 by 3rd party monitoring services, only 43% of districts indicated that they were protected 24x7 and nearly 20% had no monitoring at all.



The MiSecure operations team then conducted a thorough evaluation of leading MDR software which includes a 24x7 response team. The MDR vendor team reviews cybersecurity event alerts, analyzes them, and responds based on their severity. Responses may include

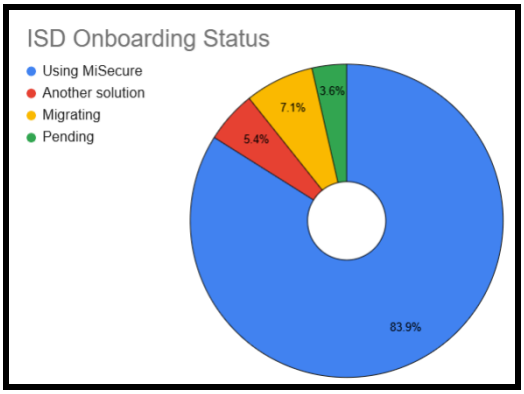
- Simple alert to district IT staff
- Stopping a rogue process
- Locking a user account
- Isolating a server
- Calling district IT staff

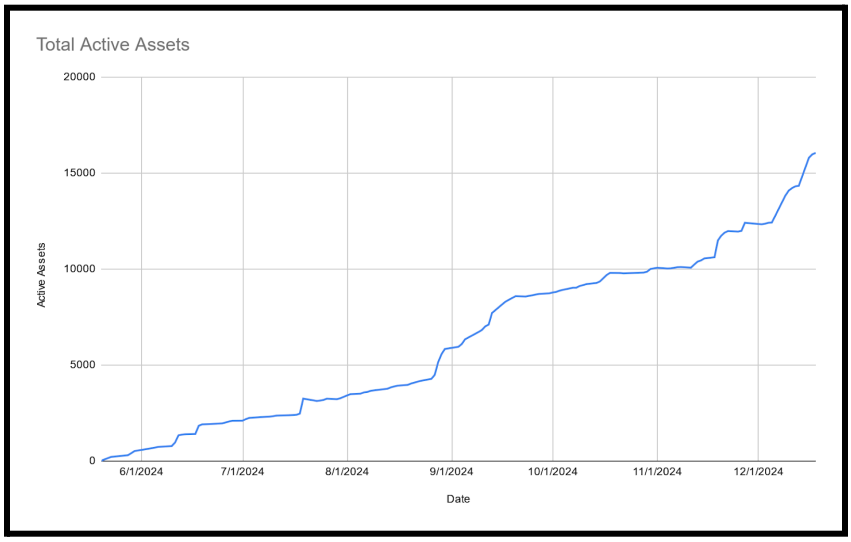
MAISA negotiated bulk pricing discounts on behalf of districts and placed the purchase through Amazon (AWS) Marketplace, leveraging the OMNIA purchasing contract. Districts were able to begin installing the software in May 2024.

As of 12/31/2024, participation includes:

- 8,833 workstations
- 3,532 servers
- 47 ISDs onboarded (84%)

Adoption continues through the end of the contract, June 30, 2027 with remaining districts joining as their current MDR & EDR software licenses expire.

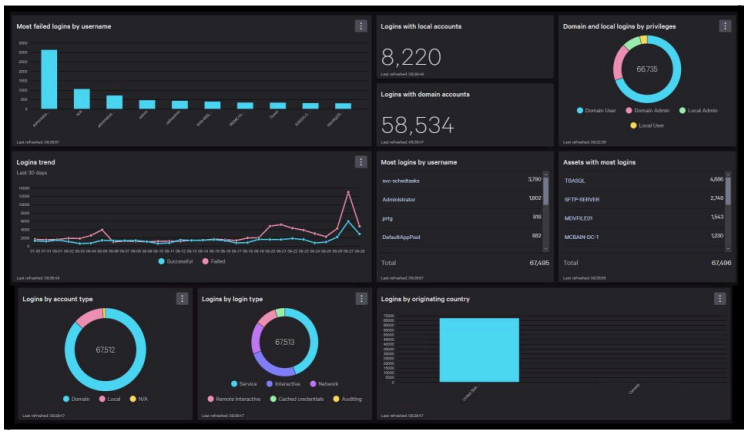




Technology

The selected MDR provides a district with a web-based dashboard revealing correlated insights into:

- Server assets
- Operating Systems and their support
- Account activity
- Specific vulnerabilities and severity
- Applications installed
- Detections
- Recommended remediations



In addition to providing this comprehensive view into their operations, district resources are also being monitored 24x7x365 by a team of cybersecurity experts. This team reviews each detection to determine if its significance and if it rises to the level of a cybersecurity incident. If the issue is deemed serious enough, the security team will reach out to members of the district to alert them of the concern. At the same time, the software and/or security team may make automated or manual mitigations including stopping processes, blocking rogue users and even isolating the server from the network. These steps can and have protected Michigan K12 servers from intruders.

The MiSecure security operations team has similar visibility, but at a whole-of-state level. This allows the team to recognize common vulnerabilities and to advocate for common remediation strategies. For example, the team may notice that a new operating system vulnerability is “critical” and “currently being exploited.” Alerts can be made to all IT contacts within the impacted location and action can be taken by district IT staff. Likewise, MiSecure may learn of a new vulnerability in a particular application. They can then identify all districts using that application and alert them to the danger, including remediation recommendations provided by our security partner.

Finally, when districts utilize a common tool for cybersecurity defense, it allows them to rely on the MiSecure operations team - or even on personnel from other districts - to assist them in incident response. Such examples have occurred. Because of the whole-of-state visibility and the formation of MiSecure, districts have been able to leverage the operations team to help isolate and mitigate existing cyber threats.

Coordination with other programs

Once established as Michigan’s first-ever K12 Cybersecurity SOC, the MiSecure team immediately began fostering relationships with other related, existing organizations. Some examples include:

- Working In conjunction with the Michigan Department of Education's State E-Rate Coordinator as well as the Michigan Statewide Educational Network (MiSEN) Director, Michigan was able to influence the E-Rate cybersecurity pilot project. Working with their respective advisories, MiSecure and MiSEN provided coordinated comments that shaped how the federal-level funding program can support K12 cybersecurity.
- Members of MiSecure and the Michigan State Police MC3 cybersecurity program met throughout the year to coordinate information on cyber attacker's tactics and best preventative measures. MiSecure has also co-presented with representatives from MC3 to Michigan school administrators.
- The vast majority of Michigan schools are covered by cybersecurity insurance provided by either SET SEG or Gallagher. MiSecure has communicated with both organizations to help maintain that insurance and to keep costs as low as possible. Furthermore, MiSecure has co-presented with SET SEG to business officials and superintendents.
- Michigan was awarded $4.7M through the federal State Local Cybersecurity Grant Program (SLCGP). MiSecure was asked to represent K12 schools on DTMB's SLCGP advisory board. Through regular communication and coordination, the two efforts were able to extend funding beyond the MiSecure MDR project, allowing schools to purchase additional Crowdstrike EDR licenses to cover additional devices. MiSecure continues to work with DTMB to help coordinate funding for similar efforts being made at municipalities and other SLTTs.
- MiSecure is directed to use the remaining funds to "partner with K to 12 statewide connectivity partners to install and monitor intrusion detection systems." This effort has begun by forming the MiSEN Security team which will recommend specific, statewide cybersecurity solutions and strategies to protect Michigan K12
- Organizationally, MiSecure is working in conjunction with other similar organizations focused on technology services that are most effectively done at the state level. Michigan DataHub, MiCHDev, MiCloud, MiSEN, and MiServiceDesk are all coordinated by MAISA under the MichIT umbrella and this coordination extends MiSecure cybersecurity services to support student statewide data efforts, cloud computing, and cybersecurity assessments. Likewise, MiSecure benefits by utilizing existing resources such as help desk, infrastructure, and data-sharing platforms.
- In April, MiSecure was invited to a meeting with National Cyber Director Harry Coker to discuss "Tackling the Cyber Challenges to K-12 Schools." The conversation included representatives from DTMB, SET SEG, MASB, CISA, MS-ISAC and MC3. A candid discussion was held and the Cyber Director was actively listening to concerns from the group. Concerns included:
    - Challenges with Michigan's K12 local-control structure
    - Inadequate funding and a lack of identified cybersecurity standards
    - Smaller schools face nearly the same exact cybersecurity challenges as larger districts with significantly fewer resources
    - Inability to hire and retain qualified cybersecurity staff

Outreach & Advocacy

In addition to supporting other statewide efforts to provide advocacy and leadership for cybersecurity, MiSecure has represented K12 to various K12 teams and professional organizations, reaching hundreds of educators and increasing participation in the project. Several events are listed below.

- September, 2023: MASA
- September, 2023: UP Cybersecurity Symposium
- October, 2023: Oakland Schools Technology Team
- November, 2023: Gratiot-Isabella RESD Technology Team
- November, 2023: MAISA
- November, 2023: Kent ISD Technology Team
- November, 2023: Ottawa Area ISD
- January, 2024: MASA
- March, 2024: MACUL
- March, 2024: GenNET Cybersecurity Summit
- April, 2024: MASA
- April, 2024: MSBO
- May, 2024: MAEDS
- July, 2024: K12ETA Superintendent Retreat
- September, 2024: UP Cybersecurity Symposium
- October, 2024: MAEDS
- October, 2024: MASB

Other activities were focused on helping schools to implement and make the most of the MDR product. These efforts included establishing an email communications group with weekly insights and recommendations, monthly training sessions on specific product features, and the development of a support website and a wiki.

To support district efforts to improve cybersecurity the MiSecure operations team recommended the use of one of several cybersecurity assessment tools such as the Nationwide Cybersecurity Review Guidance (NCSR) or the CIS Controls Self Assessment Tool (CSAT). However, the team provided specific training on a free assessment tool previously developed by the METL MiSecure Task Force: the “MiSecure Quick Self-Audit.”

Each participating ISD will complete the assessment annually and provide feedback to the MiSecure operations team in order to identify areas for improvement as well as areas in which schools are strong.

Finally, while the 97g grant provided funding for MDR, the grant also allowed for “any remaining fund” to be used for “additional cybersecurity services as technologies evolve and budget allows.” To this end, the team monitored various other cybersecurity tools and worked with

providers to share the benefits of those tools. Surveys were conducted to determine the most needed tools and the advisory was engaged to help identify areas for improvement.

Conclusion/Summary

The average cost of a cybersecurity incident for K-12 schools can vary significantly based on the severity of the attack and the specific circumstances. Recent reports indicate that the costs are substantial and rising. For instance, in response to a ransomware attack, a Texas school district paid over $547,000 to protect sensitive data from being published. Additionally, the ongoing recovery costs from similar incidents can exceed millions of dollars - Baltimore County Public Schools faced nearly $9.7 million in recovery costs following a ransomware attack, while the Buffalo School Board spent about $9.4 million on external IT consultants after an attack (THE Journal, K12 SIX).

Defending against such attacks requires a “defense in depth” approach. Districts need to implement cyber defenses at every stage: the firewall, end-user training, multi-factor authentication, regular vulnerability scanning, patching and updating and server and device monitoring. Only by providing holistic protection can districts ensure the cyber safety of their organization. Each stage presents challenges, most often these are financial. The 97g program has helped the majority of schools within the state to address the financial burden of protecting its most critical technology assets.

Supporting the cybersecurity efforts of K12 using the “whole of State” model has proven to be the most effective strategy. This has proven true with previous efforts. Specifically, the MiSEN state educational fiber optic network and the Michigan data hub projects have both shown that addressing the needs common to every district at a statewide level has consistently saved schools money and effort, freeing up resources for more localized needs. MiSecure has demonstrated that a small, specialized team of cybersecurity experts can support all districts at a level few could afford individually. Statewide purchasing of MDR software results in lower prices than any district could have leveraged individually. Adoption by districts has confirmed the need for MDR software.

There remain several additional areas in cybersecurity that could benefit from this whole-of-state protection.

- Broadening the program beyond server protection to also include staff and student devices.
- A state-wide cybersecurity training program to provide staff with cybersecurity training
- Firewalls are currently purchased individually making the sharing of knowledge difficult and cost savings done individually.
- Few districts can afford to hire a Chief Information Security Officer (CISO) - a state-level program to organize these cybersecurity-focused administrative positions could be established using the MiSecure model of support.

- Migration to the cloud provides additional layers of security. By building on the existing MiCloud effort, schools could leverage cloud computing for increased security, decreased costs and increased reliability.
- MDR addresses one of several cybersecurity needs for districts, but

Appendices

Appendix A: Definitions and Terms

MDR: Managed Detection and Response (MDR) is a cybersecurity service that combines technology with human expertise to rapidly identify and limit the impact of threats by performing threat hunting, monitoring, and response.

EDR: Endpoint Detection and Response (EDR) is a cybersecurity tool that records and stores behaviors, and events on endpoints and feeds them into rules-based automated responses and analysis systems. When an anomaly is detected, it is sent to the security team for human investigation.

SLCGP: The State, Local Cybersecurity Grant Program is a federal funding program intended for state, local, tribal & territorial (SLTT) governmental organizations, such as schools, to improved their cybersecurity efforts.

MS-ISAC: The Multi-State Information Sharing and Analysis Center is a trusted cybersecurity partner for 17,000+ U.S. State, Local, Tribal, and Territorial (SLTT) government organizations. The MS-ISAC is federally funded by CISA and a division of the Center for Internet Security (CIS)

CIS: The Center for Internet Security is an independent, nonprofit organization providing cybersecurity leadership to people, businesses and governments through leadership and the support of tools and projects such as CIS Controls® and CIS Benchmarks™. They are also home to the MS-ISAC.

CISA: The Cybersecurity and Infrastructure Security Agency (CISA) is a component of the United States Department of Homeland Security (DHS) responsible for cybersecurity and infrastructure protection across all levels of government, coordinating cybersecurity programs with U.S. states, and improving the government's cybersecurity protections against private and nation-state hackers.

MC3: A division of the Michigan State Police, the Michigan Cyber Command Center (MC3) investigates the criminal aspect of network intrusions for cyber incidents involving Michigan businesses and public entities, including those incidents related to ransomware, phishing, business email compromises (BEC), and malicious insiders.

METL: The Michigan Education Technology Leaders are a leadership network within MAISA. Formed in October 2016, METL consists primarily of ISD/ESA/RESA senior technology leaders from across the state. The idea behind METL is how to organize and align collective efforts to

work both on issues held in common and also those larger, transformative, statewide, and systemic issues.

Cybersecurity detection: Any anomalous activity that occurs in a network or device. Such activity ranges from benign end-user activity to the execution of malicious code. All detections require IT review and sometimes action.

Cybersecurity event: Any occurrence that has the potential to affect the security of a computer or network or the data it processes, stores, or transmits. Not all cybersecurity events lead to a security incident.

Cybersecurity incident: An incident is a specific type of event that negatively impacts the confidentiality, integrity, or availability of networks, devices or data, requiring an organized response.

Appendix B: Advisory Board Members

- Michael Coats, Kalamazoo RESA
- Tammy Evans, MiCH IT/MAISA
- Christopher Hammond, Oakland Schools
- Scott Hartman, Genesee ISD
- Nicholas Hay, Monroe ISD
- Josh Hiner, REMC 1
- Bobby Hodges, Wayne RESA
- Dwight Levens, Oakland Schools
- Mike Lilly, Ingham ISD
- Nick Morse, Kent ISD
- Brandi Reynolds, Northwest Education Services
- Kurt Rheaume, Wayne RESA
- Joe Smith, Gratiot-Isabella RESD
- Corey Spade, St. Joseph County ISD
- Merri Lynn Colligan, Michigan Statewide Educational Network (MISEN)
- Danny Cook, CISA
- Jim Ellis, Michigan State Police, Michigan Cyber Command Center (MC3)
- Michelle McClish, DTMB
- Joe Polasek, MDE

Appendix C:
Ingham ISD Superintendent Jason Mellema Email:

Dear Senator Anthony and Representative Witwer,

On behalf of Ingham ISD and MAISA, we would like to thank you for your advocacy and support of the work to include Cybersecurity Funding in 97g for this current year's budget (FY 24). This week, a bad actor was able to remotely connect to a Michigan school and attack the school's servers. However, the school had already configured the software funded by this legislation and this attack was thwarted because the servers were protected. Further still, the Security Operations Center which serves as an escalation point of contact at MAISA as part of 97g, was notified and was able to provide additional support to the school in reviewing the aftermath of this event. Unfortunately, this will not be an isolated incident, as bad actors will continue to attack schools as they see us as an easy target. But we use this to highlight the protection that worked because of your support and bring awareness for something that happened behind the scenes - the attack that was stopped.

We do everything possible to keep student and school data safe and thanks to your advocacy, a school that almost certainly would have been ransomed instead, safely had school. Thank you for your continued support of students.

Thanks,
Jason

Jason Mellema, Superintendent

Appendix D: Incident Executive Briefing

MiSECURE EXECUTIVE BRIEFING

Crowdstrike incident, 7/19/2024

Summary

Over 8.5 million devices crashed last Friday due to a bug in a Crowdstrike patch and its impact on the Microsoft operating system. This MiSecure Executive Briefing has been developed to review how this incident occurred, the impact on Michigan K12 systems, district IT staff response, and how statewide leadership through the MiSecure project helped to support and assist them in their efforts.

> *Technology interruptions having global impact are prevailing as the world increases our reliance on digital transformation in effort to increase efficiency and expediency.* ***We are especially proud of the statewide model MiSecure provided with immediate response and 24/x7 available support for all of K12 in Michigan.***

Background

Crowdstrike is a cybersecurity company that provides several packages of software to protect machines from cyber-attacks. These packages include a “sensor” that is installed on a machine in order to protect it, a “channel file” containing updates on the latest cyber threats that is pushed to the sensor throughout the day, a web-based dashboard that district technicians log into in order to monitor the machines protected by the sensor, and most importantly, a team of dedicated cybersecurity experts monitoring protected machines 24/7/365.

MiSecure launched in the 23-24 Michigan state budget to protect schools through the implementation of MDR software and the development of a Security Operations Team to oversee the implementation and operations of software. The MiSecure team also has visibility into participating districts through their own “parent dashboard.” This high-level visibility allows MiSecure to detect threats, make remediation recommendations, provide suggestions for improvements, and share best practices to district cybersecurity staff.

Incident

Shortly after midnight on July 19, 2024, Crowdstrike pushed out a routine channel file update that contained a logic error. This error caused many Windows machines to lock up and cease normal operations. This bad channel file was corrected around 1:30 am and any machines still functioning normally after 1:30 am were not impacted; however, machines that were impacted required manual intervention to be restored. While these restoration steps weren’t very difficult or time-consuming individually, the process of identifying and addressing each service was. The

fact that most districts were able to recover in such a short time is a testament to their dedication and skill.

Crowdstrike is used world-wide and this incident had a world-wide impact. Microsoft estimates that 8.5 million machines crashed, interfering with airlines, banking, medical services and impacting vendors schools rely on. So while district servers may have been recovered fairly quickly, other services that schools use may have amplified the impact.

Unfortunately, it isn't uncommon for schools to be impacted by global outages whether directly by a software bug or update failure or indirectly by a service partner failure. IT staff have become adept at responding and communicating in such events. The response by Michigan's K12 community was professional and fast.

MiSecure's Response

MiSecure was made aware of the issue around 6:30 AM at which point, we immediately set up a support Zoom channel and began helping end-users walk through the recovery process. We also sent out communications to Crowdstrike users; participated in discussions in the K12 IT email list (tech-c), informed MichIT leadership and opened up channels with Crowdstrike. MiSecure streamlined communications to these stakeholder groups, providing a coherent voice minimizing confusion, and keeping district staff resources focused on recovery. In past events (e.g. Windows update failures, testing server failures) districts were left to find their own solutions and vendors struggled to reach all clients. Coordinated leadership at the state level was critical to the timely resolution of this incident.