www.misecure.org

2025 MiSecure Legislative Report

Dear Legislators and Stakeholders,

On behalf of the MiSecure partnership, I am pleased to submit the enclosed report detailing the progress and impact of the MiSecure program during the 2024–25 fiscal year.

Authorized under **Section 97g** of the 2023-24 State School Aid Act, MiSecure was established to provide a unified defense against the increasing volume and sophistication of cyber threats targeting Michigan's K-12 infrastructure. I am proud to report that the program has successfully transitioned from a startup phase to a robust, high-impact operation that now protects **98% of Michigan's Intermediate School Districts.**

The attached report highlights several key performance milestones, including:

- **Exceptional ROI:** A **425% return** on the initial legislative investment through unified purchasing power and avoided breach costs.
- **Proactive Defense:** The prevention of **9 major ransomware attacks** that would have otherwise led to school closures and significant financial loss.
- **Equity in Protection:** The successful extension of enterprise-level security to districts of all sizes, ensuring that student data safety is no longer dependent on local budget constraints.

While we have secured Michigan's "digital front door," the threat landscape is evolving rapidly with the rise of AI-driven attacks. We look forward to continuing our work with the Legislature to ensure that our schools remain resilient, our students' data remains private, and our instructional time remains uninterrupted.

Thank you for your continued leadership and support of Michigan's educational community. We are available to meet with you or your staff to discuss the findings of this report in greater detail.

Sincerely,

Jason Mellema
Superintendent
Ingham Intermediate School District

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

Michael Lilly
Associate Superintendent 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

Table of Contents

1. Executive Summary

Cyber threats to K–12 schools continue to increase in frequency, sophistication, and impact. Ransomware, phishing, credential compromise, and third-party breaches put student data, instructional continuity, and public funds at risk.

To address these challenges, the State of Michigan established **MiSecure**, a statewide K–12 cybersecurity initiative authorized under Section 388.1697g. MiSecure was designed to provide equitable, cost-effective cybersecurity protection for all public school districts—regardless of size or local resources.

MiSecure provides three statewide capabilities:

- **24×7×365 monitoring and response** through Michigan's first K–12 Security Operations Center (SOC)
- **Managed Detection and Response (MDR)** protection for district servers and critical infrastructure
- **Centralized expertise, coordination, and training** to support districts before, during, and after incidents

In its first two years, MiSecure transformed Michigan's approach to school cybersecurity—from isolated, district-by-district efforts to a coordinated statewide defense model.

Program highlights include:

- MDR protection available to every Intermediate School District (ISD), Local Education Agency (LEA), and Public School Academy (PSA)
- Ransomware attacks detected and stopped before disrupting instruction
- Faster, more consistent incident response across districts
- Tens of thousands of devices protected using negotiated, below-market pricing
- At least nine ransomware incidents prevented

Financial impact:

- $5.3 million saved through statewide MDR licensing
- $12.5 million in district savings from optional, discounted licenses
- $20.5 million in estimated avoided costs from prevented incidents
- **$38.3 million in total value** generated from a $9 million investment **- 425% ROI**

Beyond technology, MiSecure has established a collaborative cybersecurity community across Michigan K–12 education. Districts now share intelligence, receive coordinated support, and have access to trusted cybersecurity expertise when incidents occur.

Cyber threats will continue to evolve. MiSecure has proven that a statewide approach improves security, reduces costs, and strengthens district readiness. With continued legislative support, the program is positioned to expand protections, address remaining gaps, and ensure Michigan schools remain safe, resilient, and focused on learning.

> *Our district cannot afford to have someone dedicated to cybersecurity on a daily basis. The service and monitoring provided by our [MDR] implementation and the support from the MiSecure team is invaluable!*
>
> - Cory Jodoin, EUPISD

2. Background and Purpose of MiSecure

2.1 Origins and Legislative Authorization (Section 388.1697g)

In 2023, Michigan launched **MiSecure**, a statewide initiative to strengthen cybersecurity protections for K–12 schools. Supported by **$9 million in legislative funding**, MiSecure established Michigan's first fully staffed **K–12 Security Operations Center (SOC)** and implemented a **Managed Detection and Response (MDR)** platform to protect school networks, servers, and sensitive data.

MiSecure was developed through collaboration between **Ingham Intermediate School District (IISD)**, the **Michigan Educational Technology Leaders (METL)**, the **Michigan Association of Intermediate School Administrators (MAISA)**, and legislative sponsors **Senator Sarah Anthony** and **Representative Angela Witwer**. Together, these partners created a first-of-its-kind, statewide cybersecurity capability.

2.2 Michigan's K–12 Cybersecurity Landscape

Before MiSecure, Michigan districts largely addressed cyber threats independently, often with limited coordination or state support. Large districts could purchase commercial cybersecurity solutions, but costs were prohibitive for smaller districts, leaving many without 24×7×365 monitoring and response. This resulted in inconsistent cybersecurity capabilities statewide and increased exposure for under-resourced districts.

2.3 The Case for a Statewide Approach

MiSecure provides **equitable protection statewide** through a centralized SOC and a consolidated MDR platform, ensuring all districts—regardless of size or budget—have continuous monitoring and protection.

Benefits include:

- **Equitable cybersecurity coverage** for all districts
- **Operational efficiency** for larger districts to focus on advanced protections
- **Expert support** via the MiSecure Operations Team, offering:
    - Cybersecurity training and guidance
    - Incident response assistance

    - Post-incident support

The SOC complements district IT teams, acting as a **statewide resource before, during or after cybersecurity incidents**.

2.4 Origin, Vision, Mission, and Goals

MiSecure originated in **2018** when ISD technology leaders formed a cybersecurity task force to advocate for statewide resources and best practices. The program's objectives include:

- **Protect instructional continuity**
- **Ensure equitable cybersecurity protections across all districts**
- **Improve statewide cyber readiness**

With Section 388.1697g funding, these goals became achievable, transforming planning into an operational statewide cybersecurity program.

> *This partnership has not only reduced risk but has also provided peace of mind to our staff, students, and families.*
> - Rick Webb, Kenowa Hills Public Schools

3. Governance and Organizational Structure

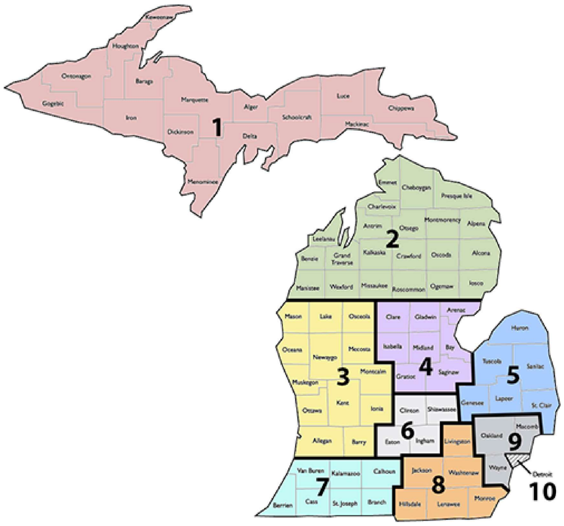
3.1 Oversight and Fiscal Management

Ingham ISD holds fiscal oversight for MiSecure, designating **MAISA** to manage the SOC and ensure compliance with legislative performance measures. MAISA established an **advisory board** to provide guidance and oversee implementation.

3.2 Advisory Board Composition and Activities

The MiSecure **Advisory Board** includes representatives from each of **MAISA's 10 regions**, ensuring equitable district access. State and federal partners include:

- **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)**



This structure strengthens collaboration, information sharing, and alignment with broader cybersecurity efforts. *A full list of advisory members is available in Appendix A.*

> *As an ISD, our overall security response strategy … relies heavily on MiSecure's active involvement. Their support includes incident response, cybersecurity awareness initiatives, training, and expert consultation, ensuring a comprehensive and resilient security posture across our environment.*
>
> \- Uyi Osifo, Kalamazoo RESA

4. Work Project Review

4.1 Year One in Review

Beginning in 2023, MAISA established the **first Michigan K–12 SOC** and selected a 24×7 MDR platform. Onboarding began in **May 2024**, and by **December 31, 2024**:

- **8,800+ workstations** and **3,500 servers** protected
- **47 ISDs onboarded** (≈84% of all ISDs)
- Licensing extended through **June 30, 2027**, saving **$5.37 million** over three years

The SOC handled thousands of automatic detections and **6 major incidents**, including:

- Prevented ransomware on the first day of school
- Stopped unauthorized server encryption
- Blocked remote intrusion attempts

A statewide K–12 cybersecurity community emerged through proactive monitoring, training, and partnerships, reducing costs and instructional disruption.

4.2 Strategic Objectives for Year Two

Year Two focused on:

- Completing ISD onboarding statewide
- Offering discounted coverage for additional non-grant-eligible devices
- Strengthening district partnerships through in-person and virtual work sessions on:
    - Cybersecurity assessments
    - Incident response planning
    - Tabletop exercises

The SOC became Michigan's **primary K–12 cybersecurity resource**, delivering training at events such as:

- **MSBO Annual Meeting**
- **MAEDS Spring PD and Fall Conference**
- **MACUL Conference**
- **MASB Training**

4.3 Program Enhancements 2024 → 2025

- **Expanded device coverage options** to include workstations, improving detection across all district assets
- **Rapid onboarding** reduced provisioning from days to minutes, critical for districts responding to active attacks
- **Tool evaluation and negotiated pricing** enabled districts to address unmet cybersecurity needs using local or grant funds

> *The MiSecure [MDR] solution has disrupted multiple critical attacks targeting Wayne County schools. The MiSecure SOC and MDR solution provides tremendous value to our schools*
>
> - Bobby Hodges, Wayne RESA

5. Statewide Participation and Coverage

5.1 Participation by ISDs, Districts, and PSAs

Year Two exceeded expectations. As of December, 2025:

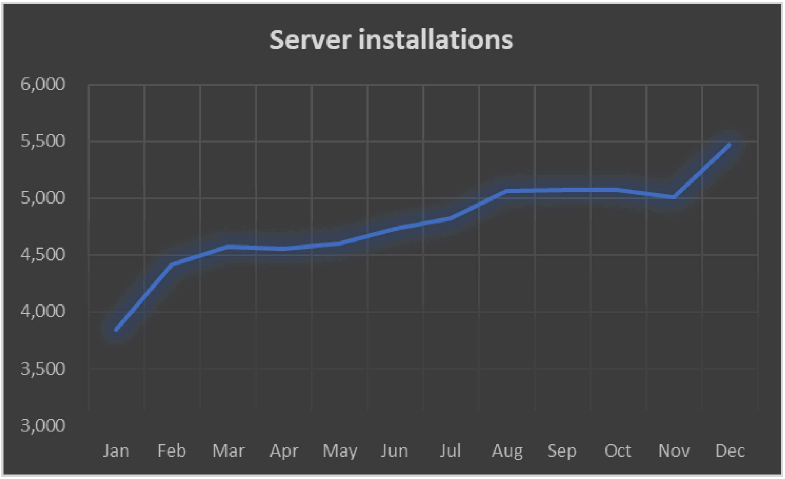
- Workstation installations increased **367%**
- Server deployments reached **90% of projected levels**
- **98% of eligible ISDs** onboarded

All districts, including **ISDs, LEAs and PSAs**, are eligible for MiSecure MDR. SOC onboarding takes **minutes.** Although some districts remain under contract with other solutions, **67% of districts** have adopted the MiSecure MDR software while **100% have access to the SOC**.

5.2 Device and Infrastructure Coverage

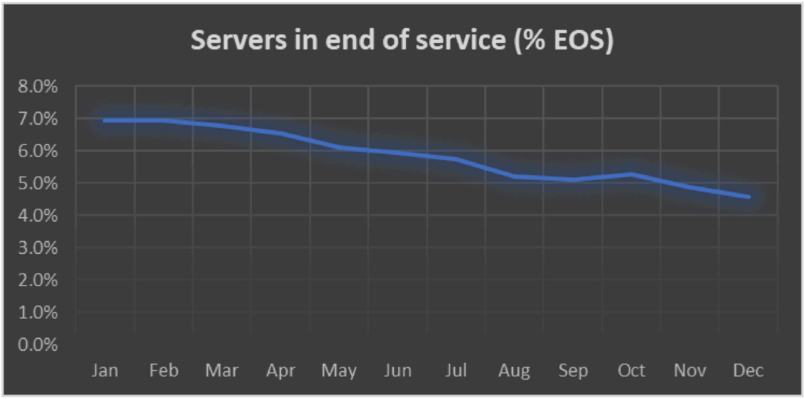
5.2.1 Server Installations

- Projected: 6,140 servers statewide
- 2024: 3,532 servers onboarded
- 2025: 5,484 servers onboarded
- Full projections expected to be met by **2026**



> *A game changer. Having their expertise as part of our team approach has helped safeguard our systems and data.*
> - Paul Mulder, Allendale Public Schools

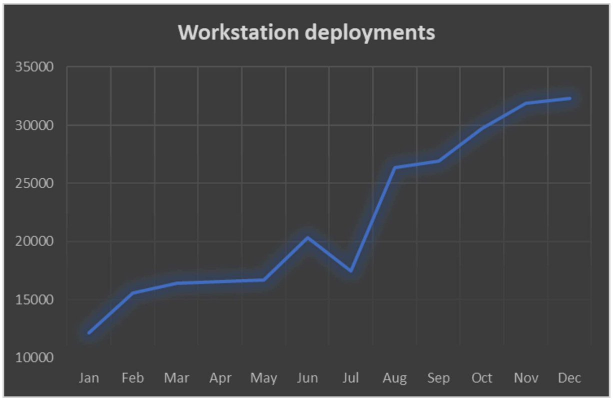
5.2.2 Server End of Service (EOS)

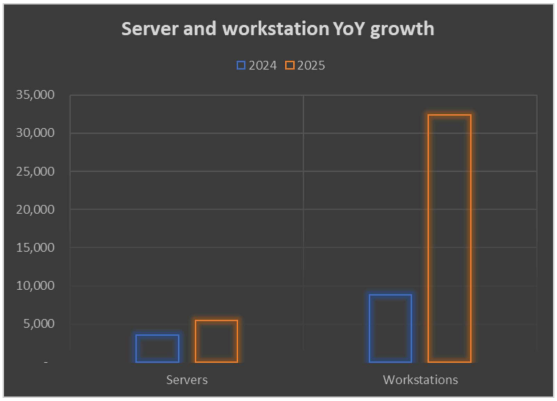


MiSecure MDR provides visibility into servers approaching **EOS**, allowing districts to remediate vulnerabilities and reduce overall EOS servers.

5.2.3 Workstation Installations

- Expanded to 32,354 workstations in 2025 (**367% increase** from 2024)
- Benefits: affordability and improved visibility for both MDR and district IT teams





5.2.4 Growth and Cloud Adoption

- Supports initiatives like **MiCloud**, aiding migration from on-premises to cloud infrastructure
- 245 cloud servers currently identified, expected to increase in 2026

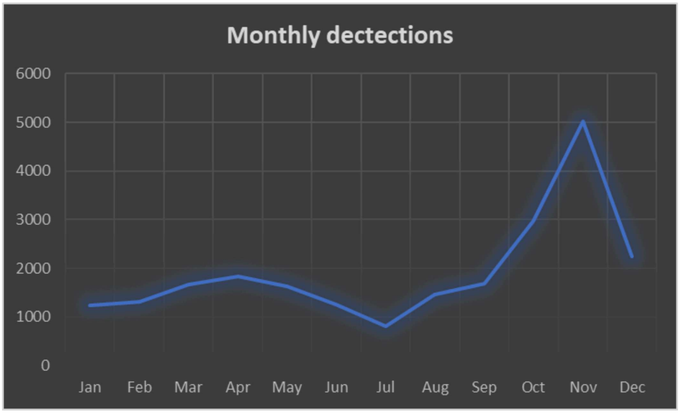
6. Security Operations Center (SOC) Performance

6.1 Threat Trends

- SOC monitors MDR alerts, assists onboarding, and responds to incidents
- 2025: **18 incidents**, a 300% increase over 2024
- Typical attack pattern: phishing → credential theft → privilege escalation → ransomware or data theft
- MiSecure MDR stops attacks during **privilege escalation and deployment phases**

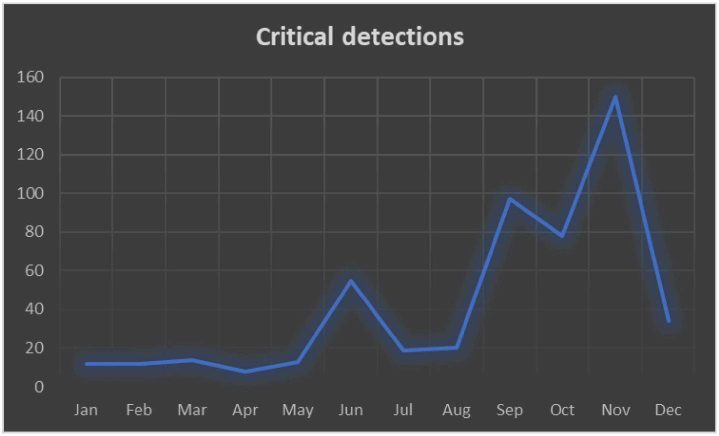
6.1.1 Detections

- Early warning signals flagged as **detections**
- Automatically mitigated and reviewed by SOC and local IT
- 2025: **23,000+ detections** managed



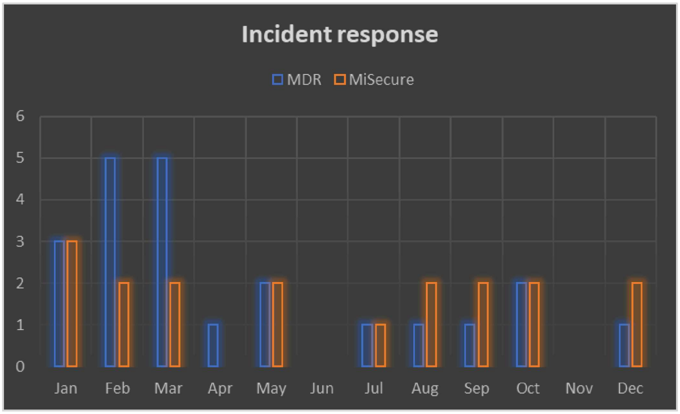
6.1.2 Critical Detections

- Severity: low → high → critical
- Critical detections indicate targeted attacks, including command-and-control software
- 2025: **512 critical detections**, any of which could have caused significant harm without MiSecure



6.1.3 Incidents

- Escalated detections handled by SOC and MDR response team
- SOC provides guidance, remediation, and coordinates with district IT
- Prevented potential losses: funds, PII exposure, server compromise, and instructional disruption



> *The interactive reports make it much easier to remedy vulnerabilities and the detailed reports allow us to dig in deep while also seeing a good top level view.*
>
> - Robin Paredez, Northview Public Schools

7. Incident Response Highlights

7.1 Overview

- MiSecure SOC team responded to **18 major incidents** in 2025
- Thousands of automatic detections were resolved without escalation

7.2 Case Studies

1. Stopped Ransomware – Compromised account prevented from deploying ransomware on 9 servers; no instructional impact.

2. Compromised Firewall – SOC isolated servers, blocked attacker access; operations restored without insurance claims.

3. PowerSchool Data Incident – Early alerts issued to Michigan districts prior to public disclosure, mitigating risk.

4. EFT Redirect – Phishing led to redirected funds; financial loss mitigated via insurance, lessons shared statewide.

Complete details for each of the above four case studies is included in Appendix B.

> *On July 4th of 2025, our district's firewall was breached and [attackers] managed to get to one of our servers. Fortunately, we had [the MDR] client installed on the server and immediately [it] shut all the services down and prevented any further penetrations from taking place.*
>
> *No-one knows how important this really is until it happens. Thank you for your continued support for this initiative.*
>
> - Phillip Stier, Morley Stanwood Community Schools

7.3 Lessons Learned

- **67% of incidents** began with compromised accounts
- **MFA adoption** remains inconsistent; many breaches could have been prevented
- **Software patching** effective, though two incidents involved unpatched vulnerabilities
- SOC provides independent investigation support for false positives
- Led response to **three statewide incidents**, serving as a single point of contact
- Verified reports of PII exposure; no confirmed leaks
- Rapid sharing of external alerts reduced delays in district response

Without MiSecure, districts would face greater risk, reduced situational awareness, and limited state-level support.

> *As a small district, I am a one man show for 700 students and over 100 staff. It gives us that piece of mind that the servers are being watched so I can focus on just keeping the school operational. Without this software, we would be a juicy steak for one of these bad actors.*
>
> - Michael Suitor, Alcona Community Schools

8. Cost Savings & Economic Impact

8.1 Strategic Licensing Savings

In alignment with Section 97g legislation, MiSecure leveraged Michigan’s massive "whole-of-state" purchasing power to negotiate software contracts that were previously unattainable for individual districts.

- **Core MDR Licensing:** By purchasing on behalf of all Michigan K-12 districts, MiSecure secured a three-year contract with a **$5.3 million initial saving**—pricing that represents less than 20% of standard retail costs.
- **Optional Expansion (EDR):** MiSecure further negotiated an **80% discount** for additional endpoint licenses. In 2025 alone, this is estimated to have saved Michigan schools **$12.5 million**, enabling tens of thousands of additional student and staff devices to be protected at a fraction of the market rate.

8.2 Scaling the "Whole-of-State" Model

The MiSecure team is constantly identifying new gaps in the K-12 ecosystem. Since phishing remains the primary entry point for cyberattacks, MiSecure recently negotiated a statewide deal for an industry-leading **email security solution**.

- **90% Market Discount:** Despite not requiring a mandatory purchase, the vendor offered Michigan a roughly 90% discount from retail based on the program's reach.
- **Unified Visibility:** Both the MDR and email security solutions feed into a single dashboard. This allows the MiSecure Operations Team to monitor statewide data in real-time, providing a sanitized, "big-picture" view of threats across all participating districts.

8.3 Cost Avoidance: Preventing High-Impact Incidents

The financial impact of a successful cyberattack extends far beyond the ransom itself; it includes digital forensics, system restoration, and legal fees.

According to the **Sophos "State of Ransomware in Education 2025"** report, the average recovery cost for a K-12 organization following a ransomware attack is **$2.28 million per incident**. Based on forensic reviews, MiSecure directly prevented at least **nine (9) major ransomware attacks** that would have otherwise crippled district operations.

- **Total Avoided Costs:** 9 incidents × $2.28M = **$20.5 million in savings.**

8.4 Summary: Return on Investment (ROI)

The $9 million legislative investment in MiSecure has yielded a massive financial return for Michigan taxpayers and school districts.

Benefit Category	Estimated Value
Direct Licensing Savings	$5.3 Million
Negotiated District Discounts	$12.5 Million
Avoided Incident Costs (9 Ransomware Blocks)	$20.5 Million
Total Economic Impact	**$38.3 Million**

Bottom Line: For every $1 of legislative funding, MiSecure has returned **over $4.25** in direct savings and cost avoidance—a **425% Return on Investment.**

> *This year our constituent districts saved approximately $26,000 by switching to MiSecure. MAISD, at its renewal in March, will save approximately $20,000 annually by switching to MiSecure.*
>
> *The cost savings will allow MAISD and its constituent districts to further strengthen our cybersecurity posture by investing in other essential cybersecurity products and services.*
>
> - Jeff Fielstra, Muskegon Area Intermediate School District

9. Training, Capacity Building, and Outreach

MiSecure continues to build statewide cybersecurity capacity through **partnerships, training, and coordinated initiatives**.

9.1 Statewide Partnerships and Coordination

MiSecure collaborates with several key organizations to maximize impact:

- **Michigan Department of Education (MDE)** – Worked with the State E-Rate Coordinator to advocate for federal **E-Rate funding** supporting cybersecurity initiatives.

- **Michigan Statewide Educational Network (MiSEN)** – Partnered to form a **MiSEN Security Subcommittee**, establishing security expectations for districts and applying for **State Local Cybersecurity Grant Program (SLCGP)** funding for statewide IT staff training.

- **Michigan State Police, Cyber Command Center (MC3)** – Coordinated on attacker tactics, threat intelligence, and best practices.

- **Cybersecurity insurance providers (SET SEG and Gallagher)** – Maintained coverage and kept costs low for Michigan schools.

- **Federal Funding Coordination** – MiSecure supported districts in leveraging **$9.6M SLCGP funds** to purchase additional **Endpoint Detection and Response (EDR)** licenses integrated into the MiSecure MDR platform.

- **Statewide Technology Services Coordination** – Works with **MiCloud, MiCHDev, Michigan DataHub, MiSEN, and MiServiceDesk** under the **MichIT umbrella** to extend cybersecurity support for cloud, data, and statewide IT infrastructure.

Additionally, MiSecure has begun planning for **network intrusion monitoring** between the SEN and the Internet, as directed by the legislation.

9.2 Training and Outreach Activities

MiSecure supports districts through multiple training and engagement initiatives:

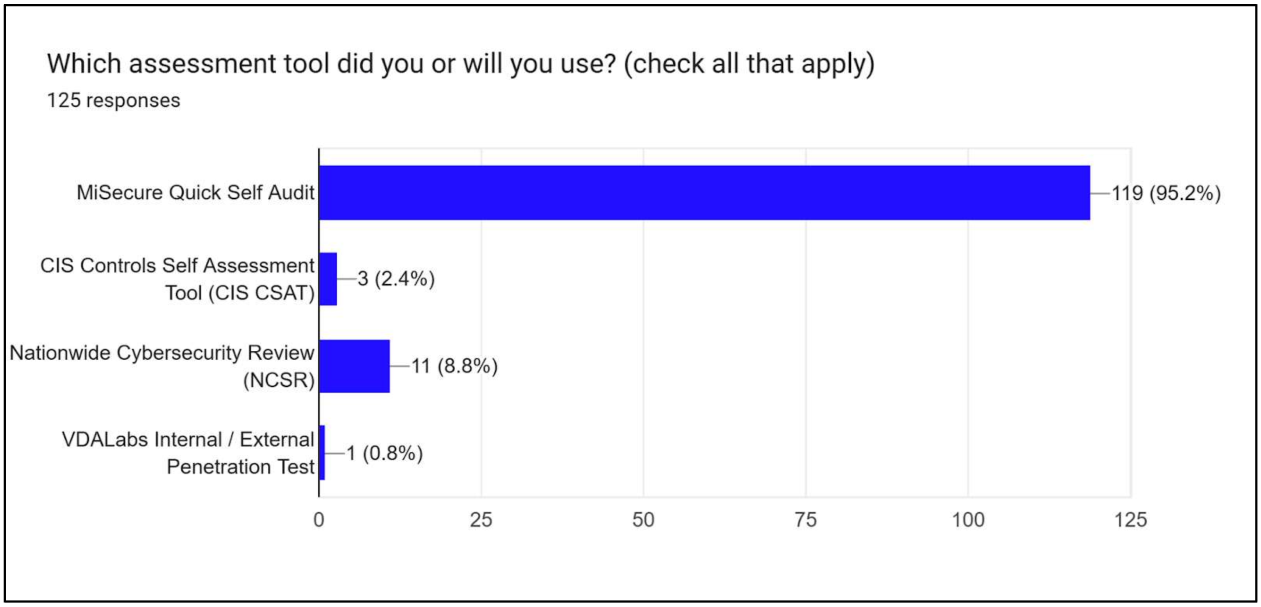
- **Regular email updates** with cybersecurity insights and product recommendations

- **Monthly product training sessions** on MDR functionality

- **Support website and wiki** for self-guided assistance

- **In-person and virtual training sessions** on the **MiSecure Quick Self Audit (QSA)**

- Support and monitoring of **cybersecurity self-assessments**
    - October 2025 survey: **95% of respondents** reported using the QSA tool



MiSecure also regularly delivers **presentations and workshops** to hundreds of educators and K–12 teams across the state, fostering a statewide cybersecurity community**.**

9.3 Areas of Improvement and Outcomes

Surveyed districts reported measurable progress in several cybersecurity domains:

Strengths / Areas of Improvement

- **Multi-Factor Authentication (MFA):** Widespread staff implementation, secure admin accounts, and 2FA adoption

- **Backups:** Implementation of immutable backups and overall process improvements

- **Awareness and Training:** Increased cybersecurity knowledge, staff engagement, and internal communication about “People and Access”

- **Endpoint and Access Security:** Enhanced EDR/MDR protection, secured/segregated accounts, device lockdowns, and controlled internal network access

Challenges / Ongoing Needs

- **Logging and Auditing:** Log management, retention, aggregation, and internal threat monitoring remain difficult

- **Administrative Engagement:** Ensuring leadership prioritizes cybersecurity and participates in the Incident Response Plan (IRP)

- **User Behavior and Training:** Overcoming language barriers, time constraints, and staff resistance to MFA; emphasizing cybersecurity as a "people problem"

- **Funding and Resources:** Budget limitations, need for ongoing funding, access to affordable tools, and insufficient staff expertise

Through training, audits, and coordinated outreach, MiSecure continues to **build capacity, share best practices, and provide districts with actionable tools and guidance** to improve cybersecurity statewide.

> *This project has provided an incredible value to Marshall Public Schools. It has helped secure our critical data and provide a solid point of confidence for our district and constituents.*
>
> *The provided industry standard … tool, we would not have otherwise been able to afford. This is critical to our security posture now and going forward.*
>
> - Joshua Collins, Marshall Public Schools

10. Program Opportunities

10.1 Remaining Cybersecurity Gaps Across Districts

The **MiSecure Managed Detection and Response (MDR)** platform provides districts with **24×7×365 monitoring**, significantly reducing the likelihood of server compromises. The **MiSecure SOC** supports districts during incidents and provides guidance for risk mitigation.

However, MDR coverage does **not extend to all devices**, and sophisticated attackers may exploit gaps that do not trigger alerts. MDR is a **critical but partial component** of a district's overall cybersecurity posture.

Typical gaps identified through cybersecurity assessments include:

- End-user and IT staff training
- Password policies and credential management
- Backups and recovery procedures
- Incident response planning
- Network segmentation and access controls

The **MiSecure Operations Team** assists districts in addressing these gaps through education, best practices, and guidance on potential solutions.

10.2 Evolving Threat Landscape

Cyber threats continue to advance rapidly. Key trends include:

- **AI-enabled phishing and social engineering**
- Use of **legitimate tools** rather than malware to evade detection
- Targeting **trusted district software and SaaS applications** to access PII and network resources

The MiSecure MDR platform adapts to these evolving threats through:

- **AI-driven response engines** to accelerate detection and mitigation
- **User behavior monitoring** rather than reliance solely on malware signatures
- **SaaS monitoring** to identify vulnerabilities in third-party applications

These features enable districts to **stay ahead of attackers** while maintaining operational continuity.

10.3 Opportunities for Expanded Statewide Impact

While current MiSecure efforts focus on MDR deployment—delivering **immediate, measurable protection for district servers**—other cybersecurity gaps remain.

Through coordination with statewide initiatives, MiSecure has leveraged partnerships to extend impact:

- **MiSEN:** Network detection and IT staff training
- **MiCloud:** Immutable backups for districts

Additional areas that could benefit from a statewide approach include:

- Identity and Access Management
- Email security
- Cybersecurity services (e.g., incident response planning, assessments, improvement plans)
- Vulnerability scanning
- End-user training and awareness
- Patch and vulnerability management
- Remote access services

Addressing these areas would further **reduce risk, enhance resilience, and standardize best practices across Michigan K–12 districts**.

10.4 Resource Constraints

At the project midpoint:

- **50% of initial funding remains**, in line with original projections
- Remaining funds are allocated to:
    - Extend **MDR coverage for at least one additional year**
    - Provide **additional network security services** in partnership with MiSEN
    - Deliver **supplemental cybersecurity services** to districts

Strategic use of resources ensures **sustained protection, capacity building, and ongoing statewide coordination**, even within current legislative funding limitations.

> *I firmly believe the continued support for these services is not only important but absolutely necessary for the short and long term cybersecurity safety of our K12 community.*
>
> - Joshua Hiner, Copper Country ISD and Gogebic Ontonagon ISD

11. Conclusion

The MiSecure project demonstrates the value of a coordinated, statewide approach to K–12 cybersecurity. In its first two years, MiSecure has established foundational protections, improved incident response, and reduced both risk and cost for Michigan school districts.

Key outcomes include:

- **Statewide cybersecurity capability established**
  - Michigan's first K–12 Security Operations Center (SOC) is fully operational.
  - Managed Detection and Response (MDR) protection is available to every district in the state.
  - Districts of all sizes receive 24×7×365 monitoring and incident support.
- **Cyber incidents detected, contained, and prevented**
  - Ransomware attacks were stopped before impacting instruction.
  - Financial fraud, credential compromise, and third-party incidents were investigated and mitigated.
  - Districts experienced faster response times and reduced recovery effort.
- **Stronger collaboration and shared intelligence**
  - Districts now operate as part of a coordinated cybersecurity community.
  - Incident details are safely shared and translated into actionable guidance.
  - Partnerships with state, federal, and education agencies improved threat awareness and response.
- **Significant financial impact**
  - Whole-of-state purchasing reduced software costs well below retail pricing.
  - Districts expanded protection to additional devices using negotiated discounts.
  - At least nine ransomware incidents were prevented, avoiding substantial recovery costs.

    - The initial $9 million investment generated an estimated **$38.3 million in total value** – a **425% Return On Investment (ROI)**

- **Improved district readiness and capacity**
    - Training, assessments, and outreach increased cybersecurity maturity.
    - Districts reported progress in multi-factor authentication, backups, and endpoint security.
    - Technology leaders gained access to trusted expertise during investigations and incidents.

Cyber threats continue to evolve, and no single control is sufficient on its own. MiSecure has established a strong foundation through MDR deployment and statewide coordination. Continued progress will require sustained investment and expansion into complementary areas such as identity management, training, and network security.

MiSecure has proven to be an effective, scalable model for protecting Michigan's K–12 schools. With continued legislative support, the program is positioned to adapt to emerging threats while preserving instructional continuity and safeguarding student and staff data statewide.

> *Implementing [the] MDR platform has changed how I sleep at night. Knowing that we have a team of experts monitoring our district 24/7 gives me a peace of mind I didn't have before.*
>
> - John Ross, Taylor School District

Appendices

Appendix A: Advisory board members

Education Advisory Members
Mike Lilly (Chair)
Christopher Hammond
Scott Hartman
Nicholas Hay
Josh Hiner
Bobby Hodges
Dwight Levens
Nick Morse
Brandi Reynolds
Kurt Rheaume
Mark Quaderer
Corey Spade
Michael Coats (MiCloud)
Merri Lynn Colligan (MiSEN)
Tammy Evans (MiCHIT)

Strategic Partner Members
Open (CISA)
Jeff Hoffman (MC3)
Michelle McClish (DTMB)
Joe Polasek (MDE)

Staff
Matt McMahon (Director)
Eric Feldhusen
Mike Schonert
Beth Soggs
Zach Taylor
Diana Urbina

Appendix B: Case Studies

Case Study 1: Ransomware Attack Prevented

A user account at a district was compromised and used by an attacker to access the district's network through a VPN connection. Once inside the network, the attacker was able to escalate privileges and obtain an administrative-level account. Using that account, the attacker accessed a district server and uploaded several malicious tools, which triggered a critical alert in the MiSecure Managed Detection and Response (MDR) software.

The MDR response team reviewed the alerts and contacted the district at approximately 2:00 a.m. while simultaneously containing the affected server. At that time, the attacker was still actively moving through the network, pivoting to additional servers and attempting to deploy tools to steal credentials and initiate a ransomware attack. Each of these processes was automatically detected and blocked, and the affected servers were isolated from the network to prevent further spread.

In total, nine (9) servers were contained as a result of the attacker's activity. Working closely with the MDR response team and the MiSecure Security Operations Center (SOC), the district was able to fully stop the attacker's access. There was no loss of data and no disruption to instruction.

Without the MiSecure MDR software installed on the district's servers, the attacker would likely have been able to deploy ransomware, almost certainly resulting in one or more days of canceled instruction and significant recovery costs.

Case Study 2: Compromised Firewall

In this incident, a district’s firewall was compromised, allowing an attacker to use the firewall itself as a platform to target internal district servers. Two of the targeted servers were protected by the MiSecure MDR software, and the attacker’s activity triggered alerts to the MDR response team.

The MDR response team immediately isolated the impacted servers from the network, preventing the attacker from continuing their activity. At the time of the incident, the district’s primary technology staff member was on vacation. The Intermediate School District (ISD) technology director was able to contact the MiSecure SOC, which assisted by disabling the attacker’s remote access and blocking the compromised accounts.

A MiSecure cybersecurity analyst traveled onsite to assist with the response and investigation. The analyst confirmed that no data had been exfiltrated, vulnerabilities were addressed, and normal district operations were safely restored.

Without the MiSecure MDR software and the availability of the MiSecure SOC, the attacker would likely have been able to compromise the servers, potentially disrupting district operations. No cybersecurity insurance claim was required as a result of this incident.

Case Study 3: PowerSchool Data Incident

During the Christmas break in late 2024, PowerSchool—one of the largest cloud-based student information systems used by K-12 schools across North America—experienced a major cybersecurity breach. An unauthorized party gained access to PowerSchool systems using compromised login credentials and was able to copy large volumes of sensitive personal data belonging to students, teachers, and school staff. This data included names, contact information, dates of birth, and in many cases Social Security numbers, medical information, and academic records.

PowerSchool first publicly acknowledged the breach in January 2025 and has since worked with law enforcement and cybersecurity experts to investigate, contain, and notify affected organizations.

While PowerSchool was conducting its internal investigation, MiSecure was alerted to suspicious activity reported by a Michigan district—one day prior to PowerSchool's public announcement. Based on MiSecure's independent research and analysis, an alert email was sent to state education technology contacts shortly before PowerSchool made the incident public.

This early notification allowed districts to prepare for communications and response activities. A full MiSecure report on this incident is included in Appendix C.

Case Study 4: Electronic Funds Transfer (EFT) Redirect Fraud

In this incident, an attacker used a phishing email to obtain the credentials of a district business office official. After gaining access, the attacker monitored the user's email activity for nearly two months. When the opportunity arose, the attacker inserted themselves into an ongoing email conversation, impersonating a known and trusted vendor.

Using this impersonation, the attacker convinced the district to change the vendor's electronic funds transfer (EFT) banking information to an account controlled by the attacker. As a result, the district suffered a financial loss. Fortunately, the district's cybersecurity insurance coverage helped mitigate the impact of the loss.

Recognizing the importance of shared learning, the district chose to work with MiSecure to document and share the details of the incident. MiSecure developed a detailed report so that other districts could take steps to protect themselves against similar attacks. This report is included as Appendix D.

Appendix C: PowerSchool incident report

The MiSecure team has been made aware of a concern detected on a district's on-site PowerSchool servers (we haven't confirmed similar activity on hosted servers yet). On or around 12/22-12/23 the district detected that their PowerSchool servers had been accessed using **valid** support credentials. During that access, at least 2 tables were transferred back by the support user: a teacher table and a student table. This raised concerns by the district since (1) there was no active support case open and therefore no reason for a PowerSchool support technician to use their credentials, (2) the files transferred did not appear to be simple diagnostic data, and (3) at least one of the source IPs was registered to Kiev, Ukraine.

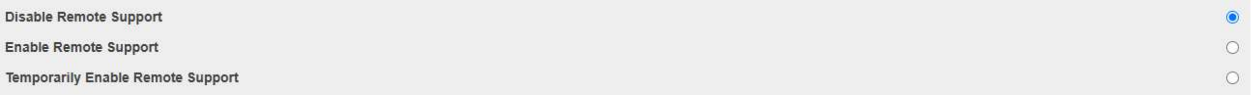
The district investigated other PowerSchool servers and found similar (nearly identical) indicators. They also contacted another district and that district had similar findings. Right now 35 districts have noticed this traffic. We are all hopeful that there is a completely reasonable explanation for this, but based on current evidence, there is concern that sensitive data may have been exfiltrated to a foreign country.

The district has opened a support case with PowerSchool and is awaiting a response. They recommend that any district with similar findings open up a support ticket for each server individually.

MiSecure is recommending that districts only enable remote support as needed:

Review remote support remote access:

1. Log into PowerSchool Admin portal
2. System Management > Security > System Security Settings
3. Ensure "Disable Remote Support" is selected



Disable Remote Support ●
Enable Remote Support ○
Temporarily Enable Remote Support ○

Furthermore, we recommend that districts review their servers for similar activity:

Review currently logged in users. Remote support users seem to stay logged in until the next server restart.

- System Management > Security > Current Users

If you have direct access to your PowerSchool server, review PowerSchool server logs

1. Log into PowerSchool server
2. Navigate to <install path>\PowerSchool\logs\tomcat-oltp
    a. Ps-log-audit.log
        i. Search for the string "supportUser". This indicates attempted access through the remote support feature.
        ii. Search for any other activity in the log from that IP address if found.
    b. Mass-data-import-export.x.log

        i. This log shows any exports done though data export manager and can be matched up with sessions from ps-log-audit.log based on the timestamps

- If you don't have direct access, there are some plugins that allow for viewing historical logins such as PSCB System Administration. You would be looking for any users with type of "Maintenance" (UserType=200 in the Logins table)

IPs Observed:

- 91.218.50.11
- 169.150.203.39
- 137.135.85.33

MiSecure is not alleging that PowerSchool is or has done anything wrong at this time. We are merely passing along a report of a concern from a district and hoping that someone can provide additional information. You can either post to the list or directly to me.

Thank you to the district that shared the information and for providing clear, actionable instructions. Please understand that our team has no first-hand knowledge of the event, nor do we have any significant experience with PowerSchool. Also, no [MDR] events or incidents were recorded during the events since the actions are all “normal.”

Finally, do not disseminate this information beyond your own support teams without our express permission.

Appendix D: EFT misdirect

MiSecure Post-Incident Review

A local school district recently lost money in a fraudulent electronic funds transfer (EFT) after a criminal pretended to be one of the district's trusted vendors.

The incident began in October 2025, when an employee's email account was hacked through a phishing email. Because the account did not have multi-factor authentication (MFA), the attacker was able to get in easily and the employee did not realize their account had been compromised. The attacker quietly stayed in the account for nearly **two months** and logged in more than 200 times.

While reading the employee's emails, the attacker found messages about two vendor payments that were coming due: one for $69,000 and another for more than $200,000. The attacker created a domain that was almost identical to one of the real vendors and used that domain to inject a message into the ongoing email conversation. The message claimed that the vendor had changed bank accounts and asked the district to send the $69,000 payment to the new account.

Because the message used the correct names, dates, and payment amounts, the district believed it was legitimate and completed the transfer. The fraud wasn't discovered until a few days later, when the attacker attempted the same trick with the larger $200,000 payment and the employee became suspicious. IT staff investigated and uncovered the ongoing email compromise.

The district contacted its bank, but too much time had passed to recover the stolen funds. Fortunately, the district had cybersecurity insurance, which reimbursed the loss minus a small deductible. The district also reported the crime to the FBI's Internet Crimes Complaint Center (IC3) and the Michigan State Police Cyber Command Center (MC3).

Recommendations:

1. Strengthen Verification for Electronic Payments

- When sending an EFT to a **new or previously unused bank account**, even for a trusted vendor, confirm the change using a **verified, trusted method**—such as calling the vendor using the phone number already on file (not one provided in the email).
- Review internal procedures to determine **which types of EFTs the district will allow.** Whenever possible, use payment methods that provide enough time to reverse a transfer if fraud is detected.

2. Increase Staff Awareness and Training

- Provide regular training to help staff recognize suspicious emails. This should include checking the **actual sender's email address**, not just the display name, and watching for unusual requests or changes to financial procedures.
- Emphasize that phishing attempts and fake invoices have become significantly more sophisticated, making careful review more important than ever.

3. Recognize the Risks of Compromised Email Accounts

- Make users aware that if an attacker gains access to email or shared documents, they can craft **highly convincing fake messages** using real purchase orders, dates, amounts, and other details. This increases the likelihood that fraudulent requests will appear legitimate.

4. Strengthen Account Security

- Ensure that **multi-factor authentication (MFA)**, passkeys, or other secondary verification methods are enabled on all accounts to protect against phishing and password-based attacks.

5. Monitor for Unusual Account Activity

- Set up systems to detect and alert on unusual login activity, such as logins from unexpected locations or "impossible travel" events (e.g., two distant logins within minutes).
- Use any available security tools to flag anomalies and notify IT staff promptly.

Special thanks to the district and ISD for sharing this information and additional details and suggestions for districts to strengthen their cybersecurity.

Appendix E: SOC Glossary of Terms

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™.

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.

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.

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, security teams are alerted for human investigation.

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.

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.

METL: Michigan Education Technology Leaders are a leadership network within MAISA. METL consists primarily of ISD/ESA/RESA senior technology leaders from across the state, formed to align collective efforts to work both on issues held in common and also those larger, transformative, statewide, and systemic issues.

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 improve their cybersecurity efforts.