MiSecure 2025 Incident Review

A summary of Michigan K12 cybersecurity incidents in 2025

The MiSecure Security Operations Center (SOC) provides a team of cybersecurity analysts that manages and monitors the MDR platform. This includes district onboarding, responding to sensor alerts, and addressing high-severity vulnerabilities. In addition, the team is available to assist any Michigan K12 school district in their response to a cybersecurity investigation or confirmed incident. This report documents the findings and takeaways from 18 individual cybersecurity responses handled by the MiSecure SOC team in 2025.

Credentials

75% of the incidents originated with an account compromise. This pattern is consistent with other industries and other states. Users tend to still be the weakest area in our cyber defenses and the primary target for attackers. Phishing emails are still the primary method of obtaining user passwords; however, in nearly half the cases, either an end-user has used their school email address and their school password on another site which was later compromised or their password was weak and/or included in a list of compromised passwords used by the attacker. Our recommendations include:

- Utilize the Identity module within Crowdstrike to monitor for compromised and weak passwords
- Train users to use unique passwords
- Consider the use of password manager tools
- Require long, complex passwords
- Monitor for logins from unusual locations or devices and consider geo-fencing
- Require occasional password changes
- Require MFA - over half of the attacks would have been stopped by simply requiring MFA

Remote Access

Once the attacker has a user's credentials, their next step is to look for remote access opportunities. Many districts provided remote VPN access to all users by default when initially setup. This is rarely if ever actually necessary and all districts should audit this service. The consequences of a VPN compromise without MDR is almost always a key component in a ransomware event. Michigan schools experienced five VPN/compromised account attacks in 2025. Three of the five were stopped when the MDR software contained the targeted servers and notified the district. The other two occurred within a district that did not use the MiSecure recommended MDR solution. To help protect against remote access-based attacks, the MiSecure team recommends:

- Provide remote access strictly to those that need it, when they need it
- Require separate MFA for all remote access
- Ensure MDR is installed on all servers
- Limit network access to unprotected resources
- Monitor remote access usage regularly - attackers often take days to initiate an attack
- Provide VPN access to only those accounts which absolutely must have it
- Regularly audit VPN authorized accounts

Updates

Regularly updating software is critical but also time consuming. Schools notoriously operate with limited IT capacity and updating is a procedure that is often deprioritized in favor of those needs that have a more immediate impact on teaching or operations. Unfortunately, in two cases in 2025, districts had external resources compromised. That is, servers or services that were directly accessible on the internet. In both cases, if those systems had been patched to address known vulnerabilities, the incidents could have been avoided. Recommendations include:

- Maintain a complete inventory of all systems attached to your network
- Establish regular "maintenance windows" to apply software patches
- Utilize Service as a Software (SaaS) tools to audit 3rd party software against established compliance standards
- Prioritize external facing servers, while not foregoing internal and SaaS systems
- Maintain proper credential audits and policies in third party systems

SOC Support

The MiSecure SOC team was asked to provide support for two cybersecurity investigations into suspicious activity. While the best qualified investigators are those with the best knowledge of the district IT operations, it is often helpful to have the support of “outside eyes.” The MiSecure SOC provides precisely that - an external team with a different, complimentary toolset. The team acts as an adjunct to the district IT staff. In two cases, the MiSecure SOC team was asked to aid in an investigation into suspicious activity. Fortunately, in both cases, the activity was found to be non-threatening. As is typical, some questions remained unanswered, but due to the teamwork of the SOC and local IT, it was mutually agreed that the activity (if ever) was no longer a threat to the district. Some suggestions to help improve your cybersecurity efforts include:

- Don’t hesitate to contact the MiSecure SOC for investigative support
- Be paranoid
- Keep the SOC in the LOOP - call 517-550-LOOP (5667) if you need any support
- Use the SOC to anonymize incident take-aways. It may be hard to admit a mistake, but by sharing your “lessons learned,” we’re all stronger

Statewide support

In three separate instances, the MiSecure SOC was able to provide leadership involving cybersecurity issues that impacted the majority of Michigan K12 districts. These included an explosion of phishing (credential harvesting) emails, reported widespread command and control activity and a 3rd party software compromise that resulted in the exposure of millions of student and staff data nationally. In each case, the MiSecure team provided a single point of contact to filter truth from hysteria and to recommend reasonable responses. Through the quick response of local district tech staff, these potential incidents were either contained or proactively addressed to minimize impact. Furthermore, in two cases, MiSecure was asked by state or national cybersecurity organizations to alert local districts of potential data breaches. In both cases, the district was able to confirm that the data exposure was benign or outright false and get out ahead of the claims. The MiSecure SOC provides a single point of contact between Michigan schools and state and national cybersecurity organizations. This communications channel helps to strengthen the state's cybersecurity posture. We need to continue to:

- Subscribe to and participate in statewide cybersecurity communities
- Maintain a trust-but-verify posture with third party providers
- Regularly audit settings on SaaS services
- Maintain relationships with state and national cybersecurity organizations such as the Michigan State Police, CISA and the FBI