MiSecure Memorandum of Understanding

Agreement

This Memorandum of Understanding (MOU) is entered into as of _____, by and between the Michigan Association of Intermediate School Administrators, a Michigan nonprofit corporation, whose address is 1001 Centennial Way, Suite 300, Lansing, Michigan 48917 ("MAISA") and _____, a Michigan public school district, whose address is _____, MI _____ (the "DISTRICT") for the purpose of MAISA having access to certain district data for MAISA's MiSecure Security Operations Team.

Definitions

CID: Crowdstrike uses the term “Customer ID” or CID to organize and contain endpoints, vulnerabilities and other data specific to an individual organization.
DASHBOARD: A web-based graphical user interface providing access to information and control over endpoints, vulnerabilities and other data.
DISTRICT: A regional educational service agency such as an ISD, ESA, etc, a local school district or a public school academy.
EDR: Endpoint Detection and Response software includes an agent installed on client computers, a dashboard for management and automated mitigation and reporting
MAISA: The Michigan Association of Intermediate School Administrators is a 501(c)(3) non-profit corporation composed of superintendents and administrators representing the 56 Intermediate School Districts (ISDs) in the State of Michigan. MAISA oversees the operation of MiSecure.
MDR: Managed Detection and Response software purchased with 97g funds, which includes an agent installed on client computers, a dashboard for management and a 3rd party operations center which is operated full time (24x7x365) by a staff that responds to incidents.
SERVERS: Critical technology infrastructure in the form of physical, virtual or cloud-based software providing services within a DISTRICT, the loss of which could inhibit the DISTRICT'S ability to operate effectively.

Purpose

The purpose of the memorandum of understanding (MOU) is to define the working relationship between the MiSecure support structure and the DISTRICT and/or DISTRICT staff. The Crowdstrike End User License Agreement (EULA) provides the legal authority for DISTRICT use and maintenance of the Crowdstrike software.

Background

In the 2023-24 School Aid Fund, section 388.1697g (or simply 97g) allocated $9,000,000 to provide a statewide Security Operations Center (SOC) and MDR services to DISTRICTS 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 this team was utilized to form the new MiSecure Operations Team (MiSecure) to staff the SOC.

MiSecure is dedicated to providing support, advocacy and leadership around cybersecurity tools and practices for all Michigan schools. As directed in the 97g language, MiSecure has now selected and is making available MDR software for all SERVERS in every DISTRICT.

MiSecure selected the Crowdstrike Falcon Complete Managed Detection & Response (Crowdstrike) solution for managing cybersecurity threats on all Michigan K12 SERVERS. DISTRICTS deploying Crowdstrike have agreed to the Crowdstrike End User License Agreement (EULA) when initially on-boarding.

Crowdstrike relies on a “sensor” that is installed on DISTRICT SERVERS. Installing the sensor allows administrators within the CID DASHBOARD to access all information located on the server provided that their account has the proper permissions. Furthermore, administrators of the Parent CID (MiSecure) can likewise access that same information; again, only if they have the proper permissions applied to their account. There are several permissions that a Crowdstrike user account can have. Only accounts with the Real Time Responder (RTR) role are able to access all data on a server. This access is through a command-line interface providing access to files and folders and not a remote console-style interface. Such elevated permissions should only be granted on an as-needed basis and MiSecure’s use of this level of access is outlined below.

MiSecure Will:

- Identify, purchase and provision MDR software for all DISTRICT SERVERS.
- Work with DISTRICTS to ensure all SERVERS are protected from cyber threats.
- Establish, coordinate and support user access to the DASHBOARD for each DISTRICT
- Coordinate CID management between DISTRICTS and MiSecure.

- Make changes to user accounts and roles as requested by DISTRICT authorized user(s).
- Provide leadership and advocacy to DISTRICTS for cybersecurity tools and best practices.
- Provide support and training to DISTRICTS independently and in conjunction with Crowdstrike and/or other organizations.
- Maintain confidentiality of all DISTRICT identifiable data.
- Maintain confidentiality of all DISTRICT identifiable incident activity and reports.
- Ensure continuous 24/7/365 monitoring of DISTRICT SERVERS using the provided Crowdstrike MDR software by the Crowdstrike Overwatch Team.
- MiSecure may contact the DISTRICT confidentially if/when significant issues are identified; however, it is expected that the DISTRICT is acting as the primary responder and investigator.
- Regularly report known threats and vulnerabilities to DISTRICTS; however, MiSecure will not act as a primary source of cybersecurity alerting.
- All data on DISTRICT SERVERS is understood to belong to the DISTRICT. MiSecure will treat data as confidential and not disclose DISTRICT data beyond the MiSecure Operations Team unless requested by the DISTRICT or as required by law.
- Retain the right to report on anonymized and disaggregated data.
- Only access individual files/folders using the Crowdstrike “Real Time Responder” access if and when requested by the DISTRICT.
- Ensure that the use of any personally identifiable information (PII) will be in accordance with State and Federal laws (e.g FERPA).
- Only access DISTRICT SERVERS and data for purposes of an investigation into an existing or potential threat.
- Train, monitor, and track DISTRICT utilization of a toolkit to be identified by the SOC such as MISecure Quick Self-Assessment.
- Provide an annual report to legislators as required in section 97g that demonstrates program efficacy.
- MiSecure will only disclose specific attack details when and if allowed by the DISTRICT unless required by law.

District Will:

- Retain all ownership of the DISTRICT data.
- Act as DISTRICT’s primary incident respondent for cybersecurity incidents.
- To the best of their ability, monitor for and react upon cybersecurity alerts originating from the MDR or MiSecure.
- Report any significant cybersecurity incidents to MiSecure in a timely manner.
- Assign roles/permissions for their DISTRICT’S users as well as any other organization the DISTRICT supports.
- Allow the incorporation of anonymized DISTRICT data into State data sets in order to inform holistic reporting.

- Ensure that it has ownership of, or permission of the owner, for all devices where the Crowdstrike sensor is installed within the DISTRICT.
- Coordinate adjustments to the DISTRICT prevention policy with CrowdStrike support and/or MiSecure.
- Allow MiSecure to access device data provided in the DASHBOARD. Such data does not include actual file or folder data, but rather, machine-specific information such as IP addresses, OS type and version, installed applications, and successful and failed login information.
- Allow MiSecure to access DISTRICT SERVERS and data for maintenance, operations, or purposes of an investigation into an existing threat or a threat investigation at the request of the DISTRICT or law enforcement. (see Data Confidentiality).
- Coordinate incident response with MiSecure (example: we would like to be considered a support partner of the DISTRICT response team during incident response).
- Maintain the Crowdstrike MDR sensor software on DISTRICT SERVERS and notify MiSecure if it intends to remove the MDR sensor permanently from the SERVER.
- Agree that the use of the CrowdStrike product and participation with MiSecure does not guarantee DISTRICT aversion from a cyber incident.
- To hold MAISA and MiSecure harmless for any support and/or incident remediation provided during this project.

Data Confidentiality

As per Michigan PA 442, MCL 15.243 (1)(U), (1)(Y) & (1)(Z), cybersecurity information is not subject to the provisions of the Freedom of Information Act (FOIA). Furthermore, as a 501(c)(3), neither MAISA nor MiSecure are subject to the provisions of FOIA.

The DISTRICT'S students have privacy rights protected by Family Educational Rights and Privacy Act (FERPA), as authorized by §99.31 of Title 34 of the Code of Federal Regulations. The parties agree to share data collected by the DISTRICT in an effort to protect the DISTRICT'S SERVERS, which may identify individual students. The DISTRICT acknowledges that the activities undertaken pursuant to this Agreement may provide a substantial benefit to the DISTRICT, and it is the intent of the parties that the personnel of MiSecure are considered "school officials" under 34 CFR § 99.31(a)(1)(i)(B). The parties, therefore, agree:

1. MiSecure personnel are performing the outsourced institutional, cybersecurity service for the DISTRICT'S benefit.
2. The cybersecurity service under this Agreement is a service or function that would otherwise be performed by the DISTRICT'S employees.
3. With respect to the use and maintenance of the DISTRICT'S information and data, the DISTRICT has direct control over the MiSecure personnel. Accordingly, the parties acknowledge that the DISTRICT may:
    a. terminate this Agreement at any time
    b. control what information and data is shared with MiSecure
    c. direct MiSecure to destroy or return any data or information shared under this Agreement at any time; and

    d. inspect and audit MiSecure’s FERPA-compliance practice and compliance with this Agreement.
4. MiSecure shall comply with the FERPA Regulations governing re-disclosure of personally identifiable information. See 34 CFR § 99.33.
5. The Parties intend for this Agreement to allow MiSecure to access the DISTRICT'S data under any and all possible FERPA provisions, including, but not limited to, the "studies" and "school official/contractor" provisions, being 34 CFR § 99.31(a)(6) and 34 CFR § 99.31(a)(1)(i).