State of Michigan

Monitoring the Heartbeat of

Cyber & Infrastructure Security

DTMB | Cybersecurity & Infrastructure Protection

CIP Data Analytics Program

CDAP reporting is the health monitor of CIP services.

State/Agency:	MICHIGAN Department of Technology, Management and Budget (DTMB) Cybersecurity and Infrastructure Protection (CIP) Division
Category:	Data Management-Analytics-Visualization
Project Title:	CIP Data Analytics Program (CDAP)
Project Dates:	1/1/2021 -5/31/2022
Contact:	Michelle Wiseman, Program Manager

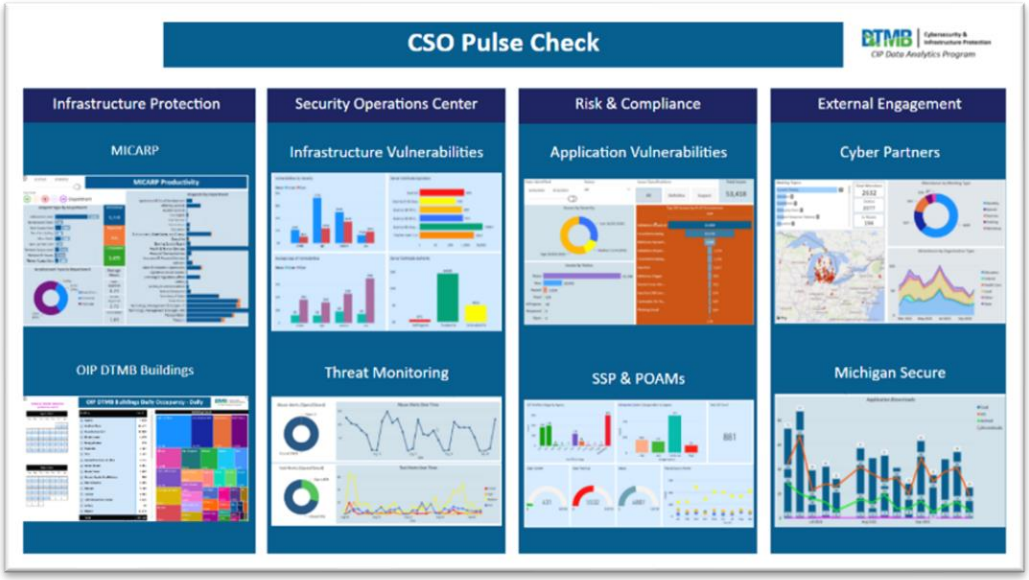
Executive Summary

Keeping watch on the health of building security and cybersecurity is a formidable task.

Security, Protection and Prevention are tough enough to achieve at a personal, family or business level. It is even more challenging when the scope includes 40+ buildings, 50,000+ staff and guests, and all the servers, workstations, laptops, mobile devices, and other endpoints daily.

Having the ability to transform data to help understand trends, recognize hot spots, react to threats, and monitor prevention is a BIG data challenge.

The State of Michigan (SOM) Department of Technology, Management and Budget (DTMB) Cybersecurity and Infrastructure Protection (CIP) division has many programs, processes, teams, and tools that are engaged to monitor, safeguard and defend.


CSO Pulse Check
DTMB | Cybersecurity & Infrastructure Protection
CIP Data Analytics Program
Infrastructure Protection
Security Operations Center
Risk & Compliance
External Engagement
MICARP
Infrastructure Vulnerabilities
Application Vulnerabilities
Cyber Partners
OIP DTMB Buildings
Threat Monitoring
SSP & POAMs
Michigan Secure

CIP is responsible for identifying, managing, and mitigating both virtual and physical security risks and vulnerabilities within the State of Michigan in these areas:

- *Infrastructure* – Responsible for physical security and emergency management at all DTMB-managed facilities as well as select agency-owned and leased properties.
- *Security Operations Center* – Action Teams (Incident Response, Threat Analytics, Forensics, Vulnerability Management) protect SOM enterprise IT security assets and resources.
- *Risk & Compliance* – Sets policy and procedure standards for cyber and physical security. Works with Application owners to ensure each system is registered, and compliant with CISA and NIST standards.
- *External Engagement* – Coordinates advisory boards and committees with local businesses, organizations, industries, towns, and counties to solve Cyber Security concerns and training.

CIP has a wide range of activity data-points that need to be readily available and consumable to leadership and support staff. Staying current and informed on efforts and activities is a near impossible task without the CIP Data Analytics Program (CDAP).

The CDAP objective is to deliver PowerBI reports to CIP and SOM customers and provide a data access portal for CIP external tools and processes. Between 1/1/2021 and 5/31/2022, the CDAP data-engine was designed, built, and delivered 30+ analytic reports to inform about our strengths, weaknesses and to empower action. These efforts showcase the transformative power of data for decision making and insight.

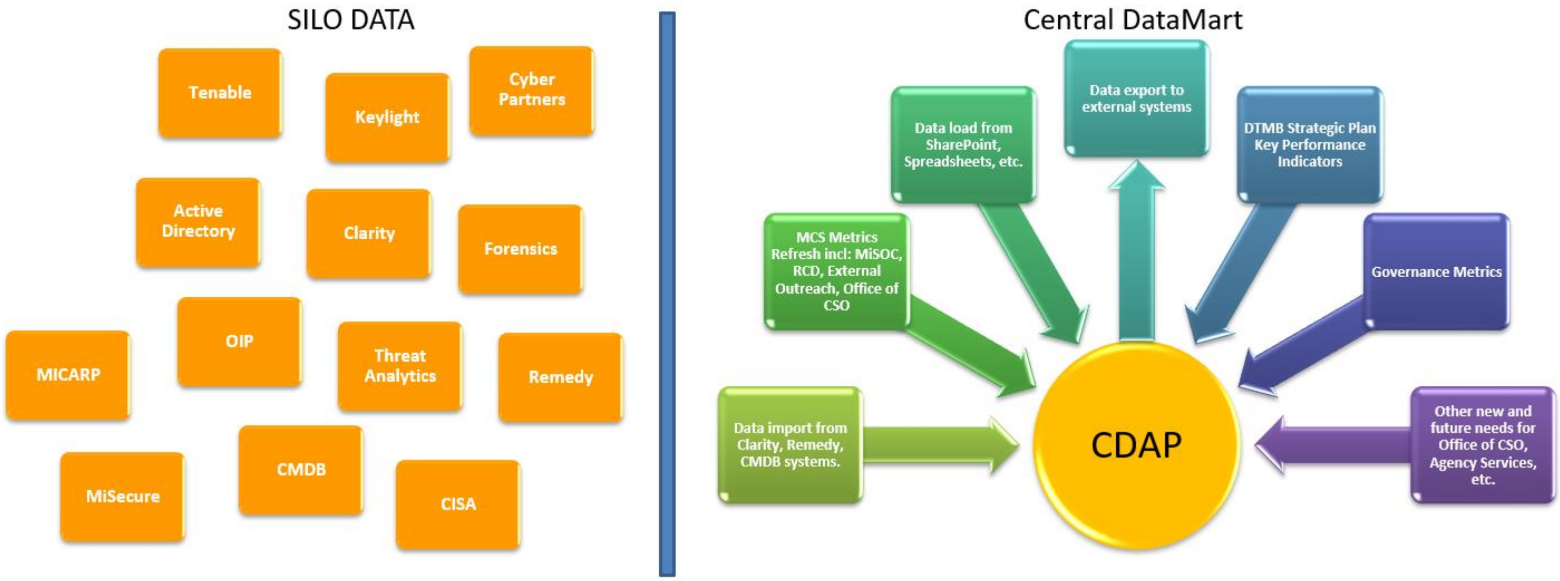
Note: All reporting data results are fictitious

Idea

Just like the human condition, our hardware, software, physical location, virtual environments, polices, processes, business units, and outreach are connected. And, just like a physician relies on data to make medical decisions; our leadership and support staff needed to see and interact with data to help them make informed decisions and act.

The Objective: Bring our CIP data together and provide analytic reports to inform about our strengths and weaknesses and empower action.

The primary struggle to make CDAP a reality was data. The data for this vision was in siloed business units and applications. We needed to be centralized for reporting and accommodate bulk data sharing with other SOM business units and enterprise tools. We created a centralized DataMart, gathering the disparate datasets to enable analytic reporting.


SILO DATA
Tenable
Keylight
Cyber Partners
Active Directory
Clarity
Forensics
MICARP
OIP
Threat Analytics
Remedy
MiSecure
CMDB
CISA
Central DataMart
Data load from SharePoint, Spreadsheets, etc.
Data export to external systems
DTMB Strategic Plan Key Performance Indicators
MCS Metrics Refresh incl: MiSOC, RCD, External Outreach, Office of CSO
Governance Metrics
Data import from Clarity, Remedy, CMDB systems.
CDAP
Other new and future needs for Office of CSO, Agency Services, etc.

Our largest data set was easily the scan results that our Vulnerability Management team generates.

Scan results	6,801,195
Cyber Reference records: Plugins, NIST & CISA	178,214
SOM Users, Servers & Workstations	155,052

- Each record needs to be joined with an agency /support team for the device/endpoint.
- Include external data points like NIST and CISA for Federal Compliance requirements.
- Convert some fields for readability – like actual names instead of look-up numbers.
- Depending on the data request, records need to be grouped or filtered.
- Finally, develop a dynamic report.

Our secondary focus, after data is the report design and delivery. The user experience is important and having the data centralized directly affects report performance. Our reports open and populate the dataset quickly and when the user interacts with the report by changing filters, the responsiveness of data is fast. We have built in automation where possible to keep our datasets current.

Implementation

CDAP reports are utilized by DTMB business units to troubleshoot problems, inform teams on their server vulnerabilities, and show trends in datasets, which improves the effectiveness of work efforts across all DTMB.

CDAP aligns with the DTMB Strategic Plan is these areas:

- ✓ **Mission**: Optimize enterprise-wide business, financial, and technical services to enable a government that works.
- ✓ **Vision**: Help drive efficiency. Connect customers to services. Deliver solutions.
- ✓ **Value**: Go Beyond in Customer Service. Understand your customer. Be understood. Deliver Solutions.
- ✓ **Goal 1** | Improve customer satisfaction for stakeholders receiving DTMB services by implementing data-driven action plans to improve quality of service.
- ✓ **Goal 3** | Reduction of audit findings

How did we make it happen?

Governance

- ✓ Program planning and development
- ✓ Review existing reports to redirect to CDAP
- ✓ Increase awareness / evangelize

Approvals

✓ Create a matrix for approvals. If the end user is:

- MCS leadership
- MCS internal
- DTMB leadership
- External to CIP
- External to DTMB
- External to SOM

CDAP was adopted from a CIP project that needed to deliver large data sets in a simplified presentation to support staff. The program expanded on that need and took shape, there was participation from governance and leadership to establish the scope and objectives. Program planning and development of subject area criteria was developed, then milestones and deliverables were established.

We needed to get the word out to all of CIP and DTMB leadership, so a presentation was developed and the Road Show went to various groups and teams to provide awareness of CDAP and insight on what was coming. We knew that providing visibility and inclusion would be helpful to getting the program underway and successful.

The program has had 9 team members cycle in and out since it started in January 2021. Currently we have a core team of 3 members - developer, database administrator and program manager. We leverage other subject-matter experts as new datasets and reports are added for just-in-time support. The total investment for 17 months is 3,960 hours.

- ✓ Were milestones and deliverables completed, YES!
- ✓ Were the objectives obtained, YES!

Build

Review and improve current processes:

- ✓ Report intake
- ✓ Data Sourcing
- ✓ DataMart management
- ✓ Source control
- ✓ Branding and Standards

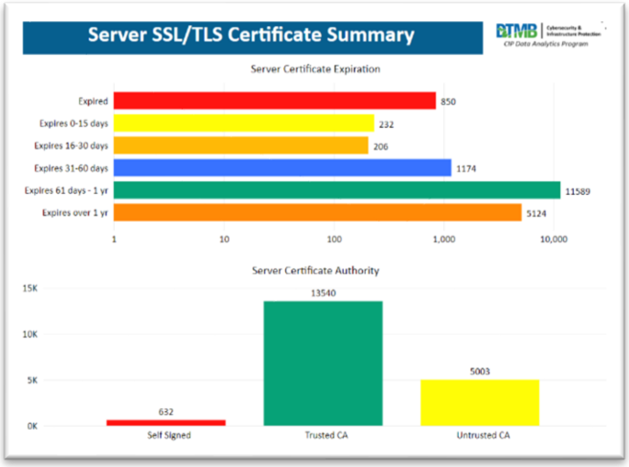
Program SharePoint

- ✓ Determine layout and navigation
- ✓ Review and confirm access points
- ✓ Create a SP list for reports, data sources, new requests, incl: status indicator, etc.
- ✓ Create a SP Request Form to populate list

Impact

Here are a few examples of delivering real impact for the DTMB Strategic Plan:

✓ Goal 1 | *Improve customer satisfaction for stakeholders receiving DTMB services by implementing data-driven action plans to improve quality of service.*


Server SSL/TLS Certificate Summary

Details are on subsequent tabs

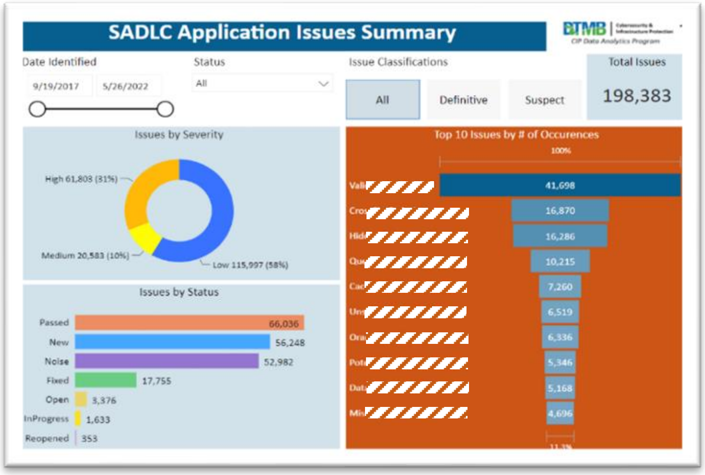
Before CDAP developed the Sever SSL/TLS Certificate report, servers would suddenly stop allowing access to critical access requests and support staff would troubleshoot and determine that a server certificate had expired. This disruption to business was costly and stressful for business and technical staff.

This report provides on-demand information about certificates on servers by expiration date, so that technical support can plan their maintenance cycles to keep business running uninterrupted.

✓ Goal 3 | *Reduction of audit findings*

An Agency can view their application scan results by status and severity. Details of each application is provided on a subsequent tab.

This Summary and detail information provides insight on issues and helps pinpoint what needs to be completed to clear audit findings and define preventative measures.


SADLC Application Issues Summary

Date Identified: 9/19/2017 – 5/26/2022

Status: All

Issue Classifications: All | Definitive | Suspect

Total Issues: 198,383

Details are on subsequent tabs

There is value for leadership and support staff in every CDAP report. When our reports are successful, CIP is delivering its mission objective: *The Cybersecurity and Infrastructure Protection (CIP) is responsible for identifying, managing, and mitigating both virtual and physical security risks and vulnerabilities within the State of Michigan (SOM).*

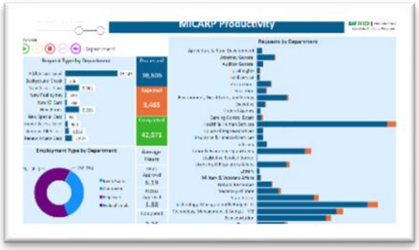
Much like hospital monitors provide information on the patient, CDAP reports are in use across the Enterprise providing data analytics so leaders can make informed decisions and staff can effect change. Getting useful data to people to enable decisions and action has been our directive.

Note: All reporting data results are fictitious

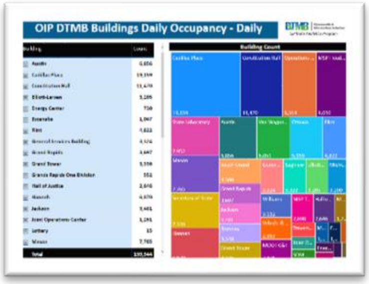
Here are a few of the real business questions that have a CDAP answer:

OIP

✓ What is the status of the Security Access cards I requested?

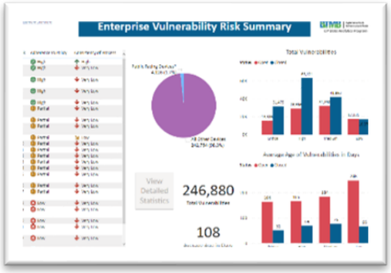


✓ How many people entered my building last Sunday?



MiSOC

✓ What infrastructure vulnerabilities are the highest risk and where are they?


Enterprise Vulnerability Risk Summary
Total Vulnerabilities
Average Age of Vulnerabilities in Days
246,880
108

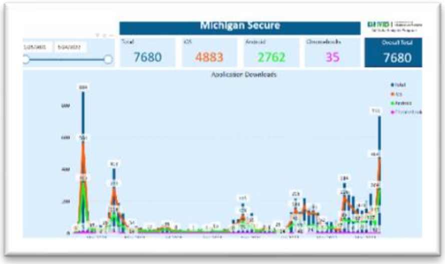
✓ What Cyber Threats have been tracked in the Enterprise?

Risk & Compliance

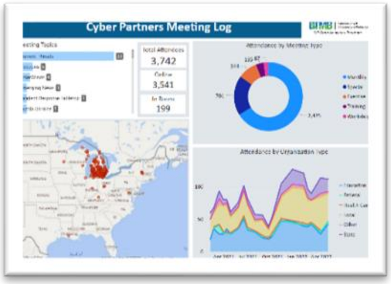
✓ What is the status of my System Security Plan? Have the POAMs been reviewed?

External Engagement

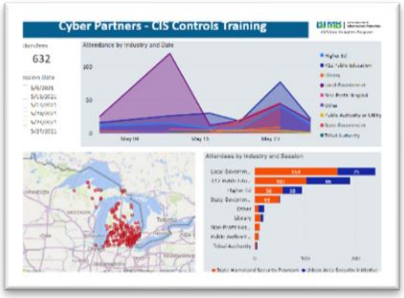
✓ Has marketing influenced the download of our mobile protection app?



✓ How many cyber partners are participating in our program?



✓ What was the most attended training provided last year?



Note: All reporting data results are fictitious

>>CDAP is meeting the information challenge >>

How can providing data in a report be equated to Cost savings? Threat avoidance? Improved protection? Improved awareness?

We know these reports make a difference because we hear from the users, leaders make decisions based on their insight, and changes are made because a team can drill down to the lowest level to find the issue and affect change.

Our next challenge is Role Based Access Control (RBAC). We want users to be able to access data that is specific to their role and areas of support. This will help them to focus on their sphere of influence by narrowing their dataset and blocking the other data that they currently need to filter out.

The CDAP program will continue with the core team to provide insightful reporting and increase automation in data sharing. There is a growing list of reports yet to be developed and data sources to tap. Data sharing and automation requests are increasing, and we will review each request and provide accessibility and support where possible. Maintenance and operational support of existing deliverables is also in our roadmap.

Infrastructure and Cybersecurity protection, prevention and education are complex, and for many – overwhelming. Most are hopeful that 'someone' is taking care of things so they can continue to do their own job. The reality is that security is everyone's responsibility in some way, either from personal awareness, preventing a phish attack, or a team ensuring the building, network, servers, workstations, etc. are protected and monitored.

CDAP reports have raised awareness of building occupancy and secured access, the complexity of cybersecurity, and provided insight to how they are all connected. Our reports offer inclusion to reports that impact the infrastructure protection and cyber health of the State of Michigan's DTMB service and support commitment.

DTMB | Cybersecurity & Infrastructure Protection

CIP Data Analytics Program

CDAP reporting is the health monitor of CIP services