Augmenting Defenses Across Minnesota: Modernizing the Statewide Security Monitoring Initiative

State of Minnesota — Minnesota IT Services

CATEGORY:
Cross-Boundary Collaboration

CONTACT:
Emily Dornfeld
Director of Communications
emily.dornfeld@state.mn.us
(O) 651-201-1011
(C) 651-485-1354

INITIATION DATE:
August 2020

END DATE:
December 2021

MINNESOTA IT SERVICES

Executive Summary

Minnesota IT Services (MNIT) modernized the Statewide Security Monitoring Initiative (SSMI), a program funded by a federal grant and devoted to protecting the data of all Minnesotans. SSMI provides cybersecurity tools and services to participating county governments, port cities, and tribal nations. SSMI helps monitor, detect, and protect their systems across the state from cyber criminals who seek to disrupt government operations. The SSMI modernization project was designed specifically to empower counties for their own success. By helping counties to be self-sufficient and self-supporting in cybersecurity efforts, we all protect systems statewide.

The redesigned, modernized SSMI program creates a view into all cyber-attacks against the state, identifying patterns and trends that help stop cyber criminals in their tracks. Grant funds provide SSMI-participating organizations with advanced, updated infrastructure, hardware, and software. Before this initiative, a large percentage of counties had nothing—no equipment, no training, or staff to monitor, detect, and prevent cyber-attacks.

The advanced features directly led to an increased number of entities participating in SSMI. Of the 67 counties, port cities, and tribal nations participating in SSMI, 49 are currently taking advantage of Endpoint Detection and Response, which enables MNIT's Security Operations Center to help monitor and respond to incidents. This accelerated adoption far outpaces the gains in adoption under the previous SSMI program. The updated SSMI program has quickly raised maturity levels and security capabilities for participating entities who often have few, if any, cybersecurity resources or staff.

In addition to these resources, MNIT developed deeper relationships with local government teams statewide through its new Security Operations Center Cyber Navigator program, which coordinates response to emerging cyber threats and active incidents wherever they occur.

By protecting the smallest entities, we are safeguarding the entire state as a whole. We protect taxpayer dollars by preventing expensive and dangerous cybersecurity incidents, and we protect the reputation of the State of Minnesota as trusted stewards of sensitive citizen data – which is a priceless value.

Idea

What problem or opportunity does the project address?

Minnesota IT Services (MNIT) embarked on a groundbreaking project unique in scale and scope. The Statewide Security Monitoring Initiative (SSMI) is a grant-funded program that is designed to drastically enhance the cyber defenses of all counties, port cities, and tribal governments in the state. There are three problems that this proactive SSMI program addresses:

1. **Reduce the state's risk profile:** Minnesota is one of the few states with a dedicated, statewide network—Minnesota's Network for Enterprise Telecommunications (MNET)—that connects branches of government, plus all 87 counties and 1,500+ locations that serve cities, public safety, health care, Minnesota's tribal nations, K-12, education consortiums, and 200 public

education and higher education campuses including the University of Minnesota, and Minnesota State Colleges and Universities. While this is a huge benefit, it also raises our cybersecurity risk profile, because a breach with one organization can threaten the entire state.

2. **Equity:** SSMI creates equity for small and large governmental entities alike in terms of cyber defense, leaving no easy targets for threat actors.
3. **Cost savings:** Volume pricing results in cost reductions that, when coupled with grant funding, allows smaller government entities to gain access to cybersecurity tools through SSMI.

Why does it matter?

Cybersecurity protects all categories of data from theft and damage. For Minnesotans who use government services, that can include sensitive data, personally identifiable information (PII), protected health information (PHI) personal information, intellectual property, data, and access to governmental and industry information systems.

As part of MNIT's 2022 Tactical Plan, which aligns with MNIT's Strategic Plan and the Security Strategic Plan, MNIT introduced new features to SSMI participating counties, including vulnerability management, incident response, log collection and monitoring, and risk and compliance. This advances a strategy defined in MNIT's Strategic Plan – bolster successful state cybersecurity efforts – combatting the cybersecurity threat facing IT infrastructure, data, and systems that Minnesotans depend on.

What makes it different?

The revised SSMI program is a holistic, proactive approach to shoring up Minnesota's network defenses from border to border.

- The services MNIT provides through SSMI complement services available through CISA, MS-ISAC, and other free or low-cost services – they all include research, monitoring, and assessments by MNIT's subject matter experts. Partners can choose which elements of the program to use, dovetailing SSMI launches to coincide with current service license expirations.
- SSMI participants do not need to be cybersecurity experts to take advantage of the resources offered to them and can focus their efforts where they matter most – whether that is combatting a piece of malware, or deciding which vulnerabilities need to be patched first based on data and expert guidance provided through SSMI resources.
- MNIT Security Operations Center (SOC) staff provide wellness checks for partner networks and share powerful tools which can be used to remediate issues, bolster defenses, and increase awareness of emerging threats and events.
- MNIT security teams actively connect with eligible partners to encourage participation, and help to set up systems and tools.

What makes it universal?

Cybersecurity and Risk Management is at the top of the State CIO Top 10 Priorities. Project development and implementation has been fully documented from its inception. Because it was structured with

iterative phases, the program model could be used for any size state with any number of counties, or expanded to include other local government organizations.

Implementation

What was the roadmap?

MNIT's Tactical Plan identified two priority tactics to drive this effort: SSMI Modernization and Managed Detection and Response. The roadmap included:

- **Modernizing** the current SSMI program to better enable statewide cybersecurity.
- **Negotiating volume pricing** to achieve cost reductions, and increase participation.
- **Reducing costs**: MNIT worked aggressively to reduce the cost of a top-tier Next Generation Antivirus (NGAV) program, and later, Threat and Vulnerability scanning. Offset by grant funding, this allowed these two services to be offered at no cost to participants for the first calendar year of the program.
- **Promoting participation**: The project team collaborated with MNIT's Customer Service and Communications teams to implement a communications outreach plan.
- Hiring a **Cyber Navigator** to interact directly with participants.

Who was involved?

Staff from the Security Operations Center and Threat and Vulnerability Management Unit (TVMU) spearheaded the program. Staff from across the agency, from Financial Management to Communications, contributed to its success. Roles included:

- **Advocacy and oversight**: Championed the project and ensured it met goals and objectives.
    - Deputy Chief Information Security Officer
    - SOC Manager
    - TVMU Manager
    - Finance and Billing
    - Customer Service Manager
- **Implementation**: Worked with end users and leaders.
    - MNIT SOC Cyber Navigator (new position)
    - MNIT Security SOC Team
    - MNIT Security TVMU
    - County/City/Tribal partner IT departments
- **End users**:
    - MNIT SOC analysts
    - County/City/Tribal partner end users

How did you do it?

The SSMI redesign was implemented in manageable phases to incorporate best practices that are consistent, sustainable, and have proven success. Partner agency data is limited to meta-data only and

stored in the Government Cloud (an isolated environment designed to allow customers and the U.S. Government to move their confidential data into the cloud to address their compliance and specific regulatory requirements).

MNIT hired a Security Operations Center Cyber Navigator as the primary liaison for participants. MNIT can now communicate more effectively across the entire state when an emerging cyber incident or threat is discovered, enabling partner agencies to protect themselves in real-time from these events almost before they are even aware of them. This single source also helps to aggregate information shared across the state, and share information instantly with all other partners throughout the state.

The SOC and TVMU teams worked with SSMI partners to roll out their respective programs, providing information and tools along with expertise as needed. The local government IT departments ultimately had to do all the "hands-on" work, learning as they went.

Service offerings were redesigned to include:

- Enhanced baseline security through the MNIT SOC:
    - Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS)
    - Security Monitoring
    - DDoS (on-premises/cloud)
    - SOC Incident Response
    - SOC Alerts and Briefs
    - Incident Response/Threat Intelligence
    - Network Security
- Next Generation AntiVirus/Endpoint Detection and Response (EDR): Backed by artificial intelligence, this industry-leading software watches for processes, scripts, shortcuts that circumvent traditional techniques and flags/blocks them as suspicious.
    - MNIT Security Operations Center oversight – each enrolled county/city/tribe is visible under our hierarchy.
    - 24/7 Threat Hunting – up to the minute protections from emerging threats across the globe, all monitored 24 hours a day, 365 days a year.
- Internal Threat and Vulnerability Scanning: Identify security weaknesses and flaws in systems and the software running on them.
    - Tenable/Nessus internal IP address scanning
    - TVMU Cyber Security Agent individual security review with partner organization
- Advanced Log Collection/Security Information and Event Management (SIEM) with analytics and metrics.

Impact

What did the project make better?

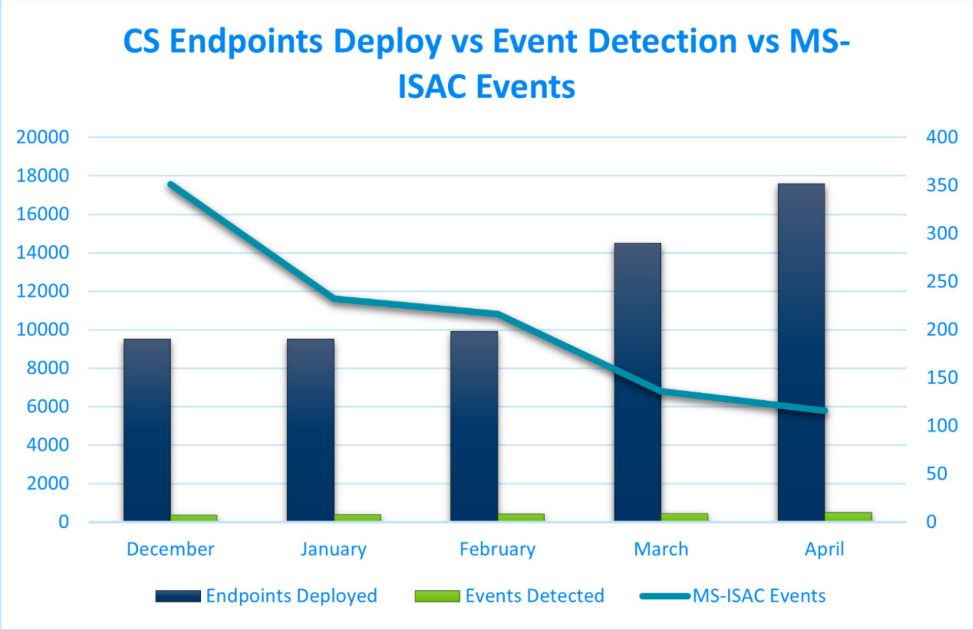
This project added EDR software and proactive threat intelligence in the form of scanning, analysis, and remediation. As the project matured, partner organizations reached out to colleagues to share their success, the value they found in the program, and their expertise as needed. Partners appreciated

consultation from MNIT's analysts; the general consensus is that cybersecurity communication has drastically increased between participating counties and the state cybersecurity teams.

How do you know?

- **Decreased cyber-attacks**: The success of modernized SSMI is defined by the things we don't see – high-profile cyber-attacks. During the project, MNIT and its partners encountered varying levels of cyber incidents. Most organizations found that they had some form of vulnerability or malware within their network and were able to begin immediate remediation. Even deploying the EDR software on all machines within a network in "learning mode" had a sobering effect when vulnerabilities became apparent in their environment.
- **Continued grant awards**: Success is also gauged by the four individual successive grants received from Federal Homeland Security. Grants are issued only to projects with proven, continued success. The grants for the modernization efforts run through the end of 2022, with a total expected spend of $3.8 million.
- **Participation**: Throughout the lifetime of the SSMI program, 67 eligible entities have taken advantage of SSMI resources. Of those entities, 49 are currently taking advantage of Endpoint Detection and Response. They received training for their staff and equipment to help them maintain their security risk at a low level.
- **Cost savings**: Partner organizations saved 100% of their software costs in the first year of the redesign.
- **Reduced cybersecurity events**: Figure 1 shows that as the state's host numbers increased (strengthening security posture), events reported by MS-ISAC (Multi-State Information Sharing and Analysis Center) decreased by about 200 per month.

Figure 1: Graph showing a comparison of endpoints deployed versus detected over the past year.



What now?

Along with the EDR and Threat Scanning software, MNIT continues to move forward with acquiring advanced SIEM software to provide proactive advanced logging and IDS monitoring. MNIT is working with a vendor to architect this new service offering across MNET to SSMI partners. This service will also have a subject matter expert/cybersecurity engineer to advise partner organizations how to configure and customize their IDS/IPS rules. The logs will be pushed into a common SIEM where MNIT analysts will perform threat hunting – giving insight not only to the participants but to the greater MNET subscriber base.

The modernized SSMI program is built around continually responding to common and emerging cyber-threat vectors while being cognizant of pain points for our partner organizations. The best solutions will be chosen based on their ability to address both of these important issues.

Implementing a program of this enormity requires long-term commitment for many years to come. SSMI is an investment in our government community for Minnesotans. By engaging the counties as partners, MNIT builds enduring relationships that are based on understanding and listening to the needs of county governments. In addition to our increased ability to detect and repel cyber-attacks, these partnerships are one of the most important outcomes.

Our partnerships, careful consideration, and extensive planning ensure long-lasting cybersecurity efforts are embedded in the way we do the business of government and provide services for Minnesotans.