



Goodhue County

Minnesota

Goodhue County Technology Committee

CONFERENCE ROOM 301
GOVERNMENT CENTER, RED WING

JULY 27, 2023

8:30 A.M.

[Click here to join the meeting](#)

Meeting ID: 234 263 075 752

Passcode: Gq94TM

[Download Teams](#) | [Join on the web](#)

Or call in (audio only)

[+1 872-240-8960,,118339372#](#) United States, Chicago

Phone Conference ID: 118 339 372#

1. Broadband Update

County Website Broadband Initiative

Nuvera Community Directed Spending Project

Nuvera White Rock Project

Southeast Minnesota Wi-Fi ARPA Grant Award

Documents:

[NUVERA-WHITEROCKPROJECTMAP.PDF](#)

2. IT Department Staffing Update

3. Information Security Update

Documents:

[SIEM AND USB COMBINED PRESENTATION.PDF](#)

4. 2023 IT Projects Update

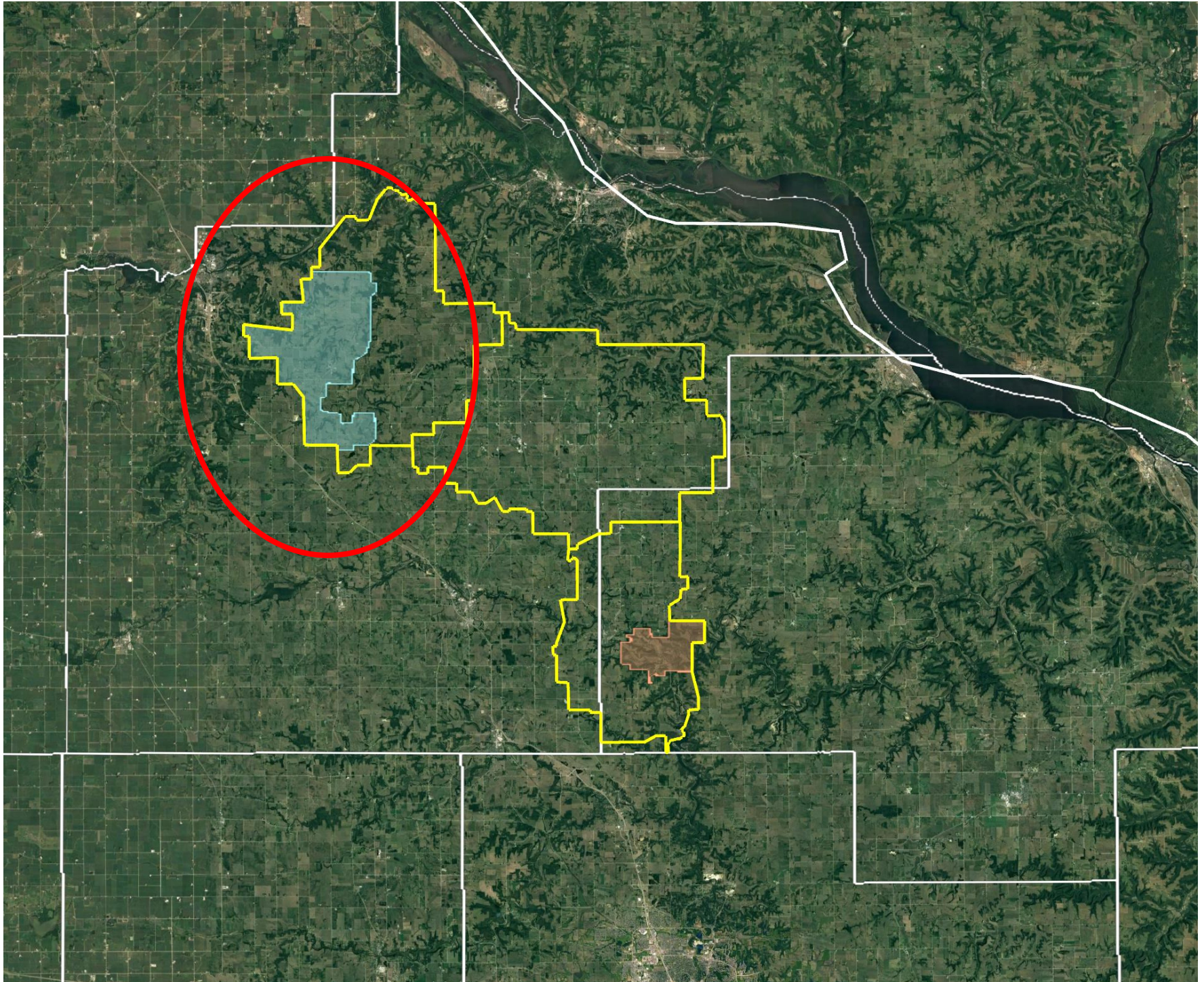
Documents:

[07.27.2023.TECHNOLOGY_PROJECTS_2023.PDF](#)

5. Q & A

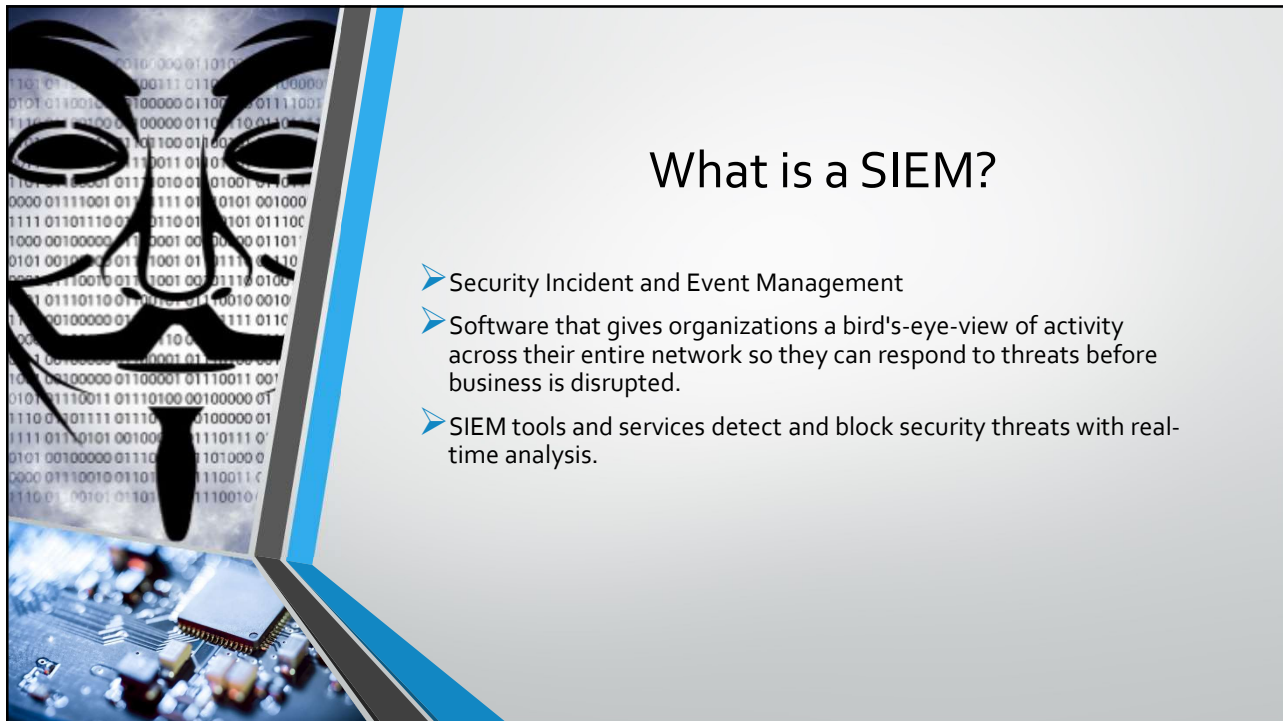
6. Next Meeting Date & Time

Thursday, October 26, 2023 at 8:30 a.m.





1



2

Who Mandates a SIEM solution?

BCA, FBI, NENA(National Emergency Number Association), IRS 1075

2	Expand logging and monitoring capabilities	NOT COMPLIANT
Description	There is no centralized logging, monitoring and alerting solution in place. Logging is inherently configured by default for devices on the network, but there is no monitoring conducted to identify and detect suspicious or malicious activities across the networks.	
Risk	The lack of a logging, monitoring and alerting solution in a decentralized environment makes it difficult to detect critical events that occur on the networks. Breaches and incidents may cause greater impact to the environment if not immediately responded to and mitigated.	
Recommendation	Implement a centralized logging, monitoring and alerting solution such as a SIEM. Ensure that all critical data sources on the network are being captured and monitored. Configure automated alerting on events requiring immediate response by the LEC or County IT. Note: It is important to understand the type of data being ingested to stay within CJIS compliance. Ingesting CJIS data may require further compliance of the controls surrounding where the data is aggregated.	

Item: 6

Section Name: Audit Logs

Question: Is someone in your agency designated to review audit logs at least weekly?

User Answer: No

Compliance Response: FBI CJIS Security Policy, Section 5.4.3 requires that audit logs be reviewed on at least a weekly basis.

NOT COMPLIANT


Agency Response: Your agency will be required to maintain a logging solution that reviews audit logs weekly within the next 6 months and describe how this item will be resolved.
Within six months we will have a process in place to review audit logs weekly.

In addition, Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies (Pub. 1075), requires security-relevant events must enable the detection of unauthorized access to Federal Tax Information (FTI) data. Auditing must also be enabled to the greatest extent possible to capture access, modification, deletion, and movement of FTI by each unique user.

3

Our Selection Process

- Multiple Vendors were evaluated
- Vendors were graded across a multitude of features and functions
- Fortinet was selected
 - Integrates with existing Fortinet Firewalls
 - Satisfies BCA/FBI, IRS 1075, and NENA requirements
 - UEBA – User Behavioral Analysis
 - AI Driven – Artificial Intelligence
- Entered into 3-year contract with Fortinet utilizing ARPA funds



4



USB Security Program for Goodhue County


Eddy Wyld

IT Network Security Analyst

5

Have you ever picked up a free USB from a conference or event?

That USB drive could deliver viruses into your computer and infect your company's network.




52%
Threats exploiting USB media for initial infection, rose 52% in 2021

Reference: [Cyber Readiness Starter Kit - Cybersecurity Awareness Workforce Training \(cyberreadinessinstitute.org\)](#)

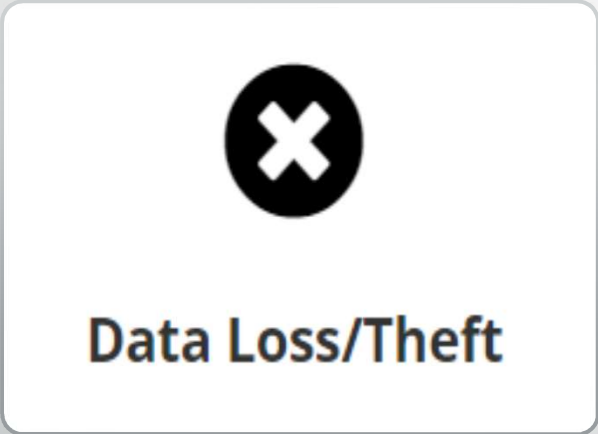
6

- USB drives can be reprogrammed to spread malware across an entire network quickly.
- Hackers will configure these drives to run a malicious program that installs malware, edits files, or locks down a computer.



Reference: [Are USB Drives Safe to Use in Your Organization? \(networkcomputerpros.com\)](https://www.networkcomputerpros.com/are-usb-drives-safe-to-use-in-your-organization/)

7




- Because most USB drives are not encrypted, major problems can arise if they are lost or stolen.
- Organizations that are subject to cybersecurity regulations must pay special attention to the use of USB drives because there may be rules in place that prohibit the storing and disseminating of data via external or unencrypted devices.

Reference: [Are USB Drives Safe to Use in Your Organization? \(networkcomputerpros.com\)](https://www.networkcomputerpros.com/are-usb-drives-safe-to-use-in-your-organization/)

8

How to Protect Against the Dangers of USB Drives

- **Control User Access**
 - Most operating systems control how a USB device functions when connected to a computer. This can allow the county to limit access to certain files like executable files or commonly infected files – such as PDFs and MS Office documents – that can cause significant damage.
- **Leverage the Cloud**
 - Utilize Office365 to share files securely in the cloud
- **Provide Encrypted USB Media**
 - Provide and monitor secured USB media to prevent data loss if devices are lost or stolen.
- **Provide training to county staff on the secure use of USB media**
 - Utilize the county's Information Security Awareness Training program to train staff on how to prevent malware infections and data loss through the secure use of USB media



Reference: [Are USB Drives Safe to Use in Your Organization? \(networkcomputerpros.com\)](https://www.networkcomputerpros.com/are-usb-drives-safe-to-use-in-your-organization/)

9

Who requires USB Blocking?

Criminal Justice Information Services, BCA, FBI – Item 5.8 MP-7 Media Use

NENA – National Emergency Number Association *Audit Failure Listed Below*

1	Removable media is not restricted on workstations	HIGH
Description	Goodhue County does not restrict the use of removable media (e.g., USB storage devices) on workstations. USBs are disabled for ARMER radio.	
Risk	<p>There are two main risks presented when USB storage devices are allowed for widespread use:</p> <ol style="list-style-type: none"> 1. A malicious internal actor may be able to exfiltrate data without detection 2. A malicious internal or external actor may be able to introduce malware to the network <p>This also includes plugging in smartphones for either charging. Smartphones have data capabilities that would allow a compromised smartphone to potentially transfer malicious information, applications, software, etc. to the host workstation.</p>	
Recommendation	<p>Goodhue County should restrict the use of removable media (e.g., USB storage devices) on workstations through policy or technical configurations. This includes using the workstations for charging smartphones. If charging is required, it is recommended to get dedicated power outlets for charging.</p> <p>Exceptions for this restriction can be put in place for those with a valid business need as determined by management. If USB storage devices are used, they should be inventoried and provided by IT staff, and encrypted wherever possible.</p>	

10



John M. Smith

IT Director

Goodhue County

509 W. 5th St.

Red Wing, MN 55066

Phone (651) 385-3224

Fax (651) 267-4870

To: Goodhue County Technology Committee

From: John M. Smith, IT Director

Date: July 27, 2023

Subject: Technology Projects in 2023

Projects Completed:

1. Upgrade Pine Island and Wanamingo GCSO Offices
2. Implement Information Security Awareness Program – ARPA Funding
3. Assist Land Use Management with Cloud Based GIS Infrastructure
4. Develop Policies for Website ADA Compliance – Move to Communications
5. Relocation and Remodel of County Board Room

Projects in Progress:

1. Migrate to Tyler Property Tax System for Auditor/Treasurer Office
2. Implementing Microsoft Office365 – Teams, OneDrive, SharePoint
3. Assist Public Works with Lake Byllesby Park Pavilion Security
4. Network Switch Upgrades – Carryover from 2022
5. Implement Security Incident and Event Management (SIEM) – ARPA Funding
6. Multi-Factor Authentication (MFA) for ALL network connections – ARPA Funding
7. Update Support Agreements with County Police Departments
8. Government Center remodel, phase 1

Projects on Hold:

1. Backup PSAP and Mobile PSAP for GCSO Dispatch
2. Implementation and migration to .gov domain (GoodhueCountyMN.gov)