METRO STATE UNIVERSITY

DHS/NSA designated CAE-CD Institution

MN CYBER

Train. Test. Detect. Protect.

Week 15 pitch-698 Capstone

Presenters: Clarence Campbell

METRO STATE UNIVERSITY

DHS/NSA designated CAE-CD Institution

MN CYBER

Train. Test. Detect. Protect.

Why Now / Significance

- Ransomware remains one of the most disruptive threats to state/local organizations.

- Lack of asset visibility and weak monitoring create blind spots attackers exploit.

- *48% of U.S. K–12 districts report compromised devices linked to unmanaged assets*
(Week 4/5 evidence).

METRO STATE UNIVERSITY

DHS/NSA designated CAE-CD Institution

MN CYBER

Train. Test. Detect. Protect.

Evidence Snapshot (Prior Work)

Mini Table

Source	Year	Key Insight
Verizon DBIR	2024	Misconfigured assets drive 68% of initial access events.
CISA MS-ISAC	2023	K–12 attacks increased due to weak monitoring baselines.
NIST 800-161r1	2022	Supplier gaps increase propagation risk.

METRO STATE UNIVERSITY

DHS/NSA designated CAE-CD Institution

MN CYBER

Train. Test. Detect. Protect.

Method (Diagram + Measures)

Data sources → Log Pipeline → Detection Rules → Analysis Notebook → Metrics Output

Measures (from Week 6/11):

Detection Coverage % (events detected ÷ events expected)

Time-to-Detect (TtD)

Risk-Weighted Alert Score (RWAS)

METRO STATE UNIVERSITY

DHS/NSA designated CAE-CD Institution

MN CYBER

Train. Test. Detect. Protect.

Standards Anchors (Crosswalk Excerpt)

CSF Outcome (copy-exact):
DE.CM-01: “Networks and network services are monitored to find potentially adverse events.” — Appendix A, p. 21
One-line rationale:
My design improves monitoring baselines through structured log collection, anomaly detection, and reproducible analysis.
ZTA Element (optional):
SP 800-207 Tenet (summarized):
“All data sources and computing services are considered resources.”
One-line rationale:
Aligns with treating all assets as monitorable resources, not implicitly trusted.

METRO STATE UNIVERSITY

DHS/NSA designated CAE-CD Institution

MN CYBER

Train. Test. Detect. Protect.

Ethics, DMP & C-SCRM (Safeguards)

- **Ethics:** Use only synthetic or non-identifiable log data; avoid capturing personal information.

- **DMP:** Store controlled datasets in /data/; apply least privilege; version only safe artifacts.

- **C-SCRM:** Assess the integrity of dependencies and document supplier risks.

Evaluation Plan (Metrics & Traceability)

SMART Metrics:

Detection Coverage %

Time-to-Detect

RWAS (Risk-Weighted Alert Score)

Traceability Chain:
Risk → 800-171r3 3.3.6 requirement → Metric → Evidence

CSF Current → Target Profile

Required copy-exact text:
DE.CM-01:
“Networks and network services are monitored to find potentially adverse events.”
— Appendix A, p. 21
Additional Outcomes:
ID.AM-02: “Inventories of software, services, and systems managed by the organization are maintained
— p. 18
ID.RA-05: “Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization.”
— p. 19
Current → Target:
•*Current:* Fragmented inventory, inconsistent monitoring, and limited risk scoring.
•*Target:* Unified inventory, continuous monitoring, reproducible risk-driven alerting.

METRO STATE UNIVERSITY

DHS/NSA designated CAE-CD Institution

MN CYBER

Train. Test. Detect. Protect.

Conclusion & Key Takeaways

Headline:

A Measurable, Repeatable Approach to Reducing Ransomware Exposure

Key Takeaways:

Strengthening monitoring and asset visibility directly reduces attack opportunities.

A reproducible workflow provides clear, data-driven evaluation of improvements.

CSF-aligned metrics help translate technical work into governance-level outcomes.