NYSCIO REGIONAL SECURITY OPERATIONS CENTER (RSOC) THINK TANK EXECUTIVE SUMMARY

June 2025

membership@nysernet.org

Contents

cb20
COHESITY
denodo
FORTINET
Hewlett Packard Enterprise
HOWARDedu
HPE aruba
Lenovo
Mainline
NRI
paloalto
PURESTORAGE

angelo.edu
ARISTA
cb20
COHESITY
denodo
FORTINET
Hewlett Packard Enterprise
HOWARDedu
HPE aruba networking
Lenovo
Mainline
NRI
paloal

Overview

At NYSCIO 2025 we convened 45 participants to explore models for a Regional Security Operations Center (RSOC) powered by NYSERNet. The purpose: identify collaborative and sustainable approaches to cybersecurity across New York State's education and research institutions. Institutions face mounting cyber threats, workforce shortages, and budget constraints. An RSOC aims to address these challenges through shared resources, coordinated threat detection and workforce development.

Why an RSOC?

- Addresses resource-constrained environments (financial, personnel, time)
- Multiplies impact through collaboration and shared expertise
- Provides proactive, relevant threat intelligence
- Enables faster response to emerging threats
- Builds a sustainable pipeline for cybersecurity workforce development

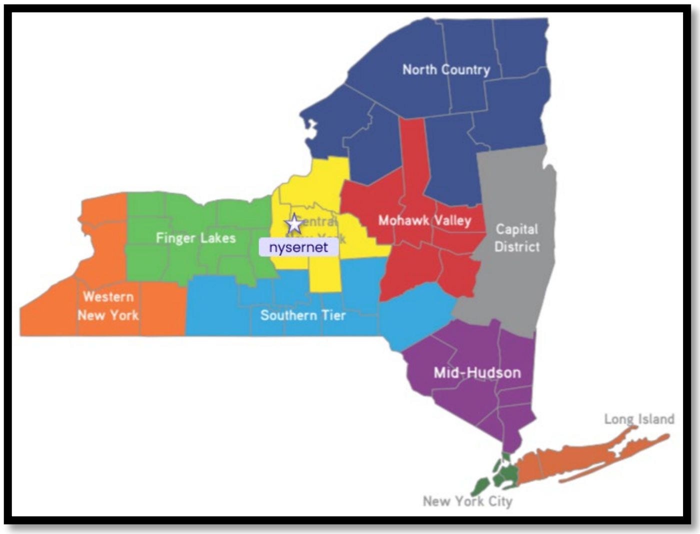
What We Explored: 4 Models for Impact

Model	Description	Key Features
Model 1	NYSERNet-hosted RSOC	24/7/365 support, free for public orgs, student pipeline across NYS
Model 2	Campus-hosted RSOCs with NYSERNet centralized threat correlation	Distributed resilience, regional engagement, state-funded
Model 3	Campus RSOCs backed by NYSERNet 24/7/365	Hybrid model, SIEM/tool savings, extended IR, business continuity
Model 4	Choose-your-own-adventure	What other models should we consider?

RSOC Models Explored

Model 1: Centralized NYSERNet-Operated RSOC

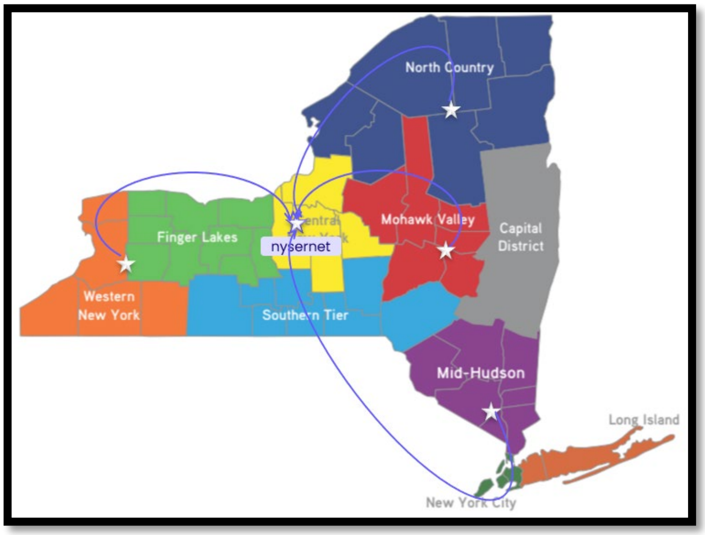
A single 24/7/365 SOC hosted by NYSERNet, which supports statewide member organizations.



- **Strengths**: Easy to launch, affordable, strong student pipeline, statewide threat visibility
- **Weaknesses**: Scalability limitations, liability risks, lower brand recognition, intern capacity limits
- **Opportunities**: Pilot for expansion of additional RSOCs, shared services, affordable access for all
- **Threats**: Sustainability concerns, rural infrastructure gaps, institutional buy-in challenges

Model 2: Distributed Campus-Hosted SOCs with NYSERNet Threat Correlation

Individual campuses operate SOCs with NYSERNet aggregating and correlating threat intelligence.

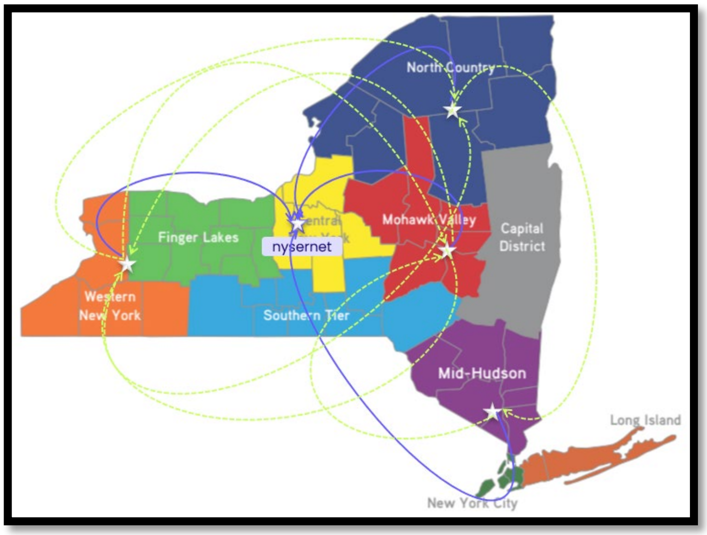


- **Strengths**: Regional resilience, community collaboration, responsiveness, workforce development
- **Weaknesses**: Distributed complexity, staffing challenges, political considerations
- **Opportunities**: NYS Joint Security Operations Center expansion, regional funding advocacy, staff retention
- **Threats**: Higher operational risk, sustainability and insurance costs

Model 3: Hybrid Model - Campus SOCs with NYSERNet 24/7/365 Support

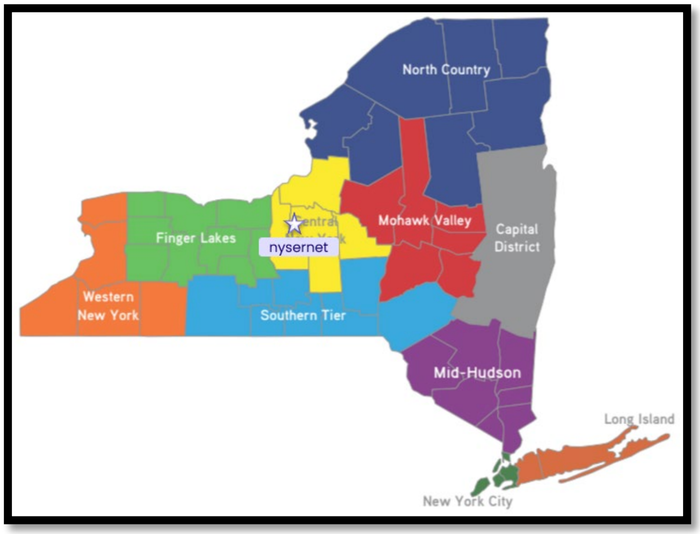
Campus RSOCs backed by centralized 24/7 NYSERNet SOC support and shared threat visibility.

- **Strengths**: Flexible and redundant, shared tools/SIEMs, cost efficiencies, career mobility
- **Weaknesses**: Compliance complexity, log failover challenges
- **Opportunities**: Cyber insurance requirements, curriculum development, community outreach
- **Threats**: Tool interoperability, regional disparities, governance complexity



Model 4: Community-Guided/Choose-Your-Own-Adventure Model

A customizable, trust-based approach where communities shape their RSOC participation level.



- **Strengths**: Empowers underserved regions, trust building, flexible threat management
- **Weaknesses**: Needs education/outreach, may lack structure or unified direction
- **Opportunities**: Public-private collaboration, anonymized threat data for early warnings
- **Threats**: Staffing and funding gaps, unclear jurisdiction, varied compliance requirements

RSOC Model Comparison Matrix

Criteria	Model 1 Centralized	Model 2 Campus-Distributed	Model 3 Hybrid (Campus + NYSERNet)	Model 4 Community-Guided
Implementation Complexity	Low	High	Medium	Variable
Initial Cost to Launch	Low	High	Medium	Variable
Ongoing Sustainability	Medium	Low	Medium–High	Depends on design
Scalability	Low	Medium	High	High
Threat Visibility Statewide	High	Medium	High	Medium
24/7/365 Response Coverage	Yes	No	Yes (via NYSERNet)	Optional
Supports Workforce Development	Strong (central co-ops)	Strong (regional pipeline)	Strong (local-to-central growth)	Depends on implementation
Tool and Licensing Efficiency	Medium	Low	High	Variable
Community Trust/Engagement	Medium	High	High	Very High
Compliance Complexity	Medium	High	High	High
Risk Distribution	Centralized (high risk)	Decentralized (distributed risk)	Shared/Redundant	Variable
Innovation/Flexibility	Low	Medium	High	Very High
Policy/Funding Alignment	Clear pilot potential	Requires broader advocacy	Aligns with scalable investment	Needs storytelling

Strategic Opportunities: Applicability by Model

Strategic Opportunity	Model 1 Centralized	Model 2 Campus-Distributed	Model 3 Hybrid	Model 4 Community-Guided
Leverage Shared State Services (ITEC, SICAS, ISOC)	✔ Strongly Aligned	✔ Some Alignment	✔ Strongly Aligned	⚠ Depends On Implementation
Create Cybersecurity Jobs In Underserved Regions	⚠ Indirectly Supports	✔ Directly Supports	✔ Directly Supports	✔ Directly Supports
Build Student-To-Professional Pipelines	✔ Strongly Supports	✔ Strongly Supports	✔ Strongly Supports	⚠ Depends On Local Participation
Offer Affordable Security For All Sectors	✔ Centralized Control	⚠ More Difficult Regionally	✔ Balanced Model	⚠ May Vary Greatly
Aggregate Licensing And Tools Across Institutions	⚠ Limited Flexibility	⚠ Challenging To Standardize	✔ Direct support	⚠ Varies Widely
Enable Anonymized Community-Wide Threat Data Sharing	✔ Built-In	✔ Possible Via Aggregation	✔ Designed In	⚠ Requires Structure
Engage Private Universities And Nonprofit Partners Equally	✔ If Access Is Open	✔ Regionally	✔ Easily Scalable	✔ Highly Flexible
Use Model To Support Early Warning Systems Statewide	✔ Central View	✔ Requires Coordination	✔ Designed In	⚠ Depends On Participation

Conclusion

The Think Tank discussions revealed strong community interest in **Model 3: the Hybrid RSOC**, which blends local campus engagement with centralized NYSERNet support. Participants valued this model's flexibility, scalability and potential to balance cost-efficiency with regional resilience. While no single model is universally ideal, Model 3 emerged as the most promising framework to pilot, offering both robust security coverage and workforce development benefits.

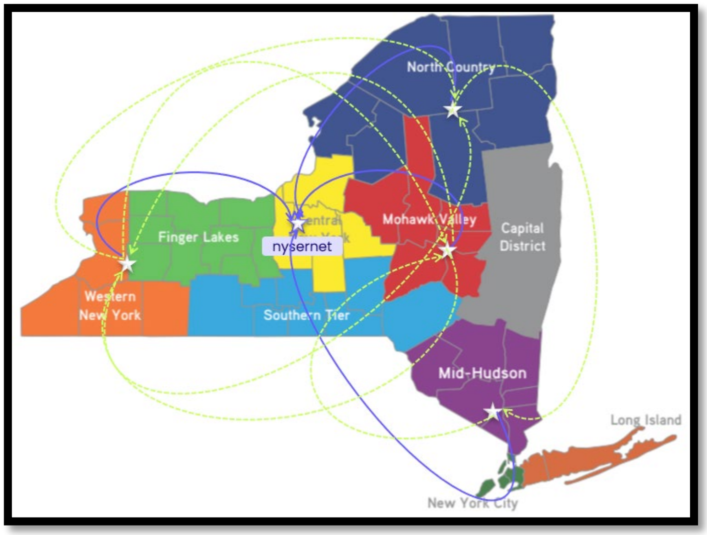
Based on the detailed SWOT feedback from the RSOC Think Tank (Appendix A), there are strong indicators that the **community is most energized by Model 3: the Hybrid Model**.

Why Model 3 Resonates Most with the Community

→Balance of Local Engagement and Central Support
Model 3 offers the flexibility of campus-level RSOCs — giving institutions autonomy and ownership — while leveraging NYSERNet's 24/7 expertise for correlation and extended incident response. This blend struck the right chord between independence and statewide collaboration.

→Clear Benefits for Workforce Development
The model supports distributed career paths and cross-campus professional development, which helps with retention and recruitment in both rural and urban areas.

→Cost Efficiency and Tool Standardization
The ability to share SIEM tools and licenses, as well as provide cloud-based services, directly answers institutional concerns about budget and tool fragmentation.



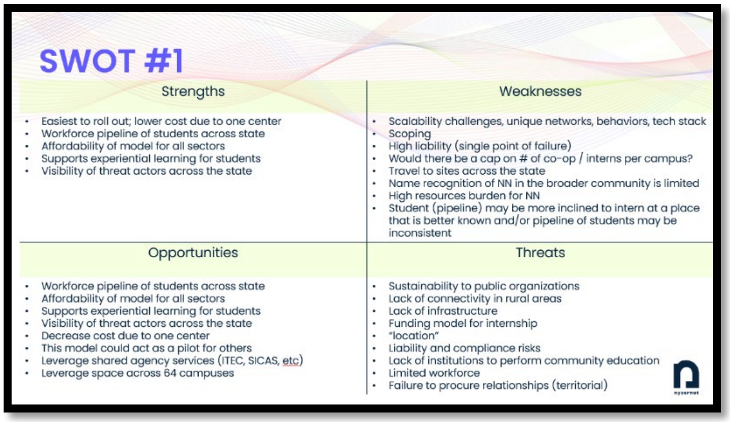
→Built-In Redundancy and Scalability
With multiple campuses using the same tools and protocols, institutions gain confidence in the model's resilience and ability to scale.

→Remaining Concerns (But Not Dealbreakers)

- Compliance challenges across institutions (especially HIPAA)
- Log management and failover across disparate systems
- Need for strong governance and clear shared standards

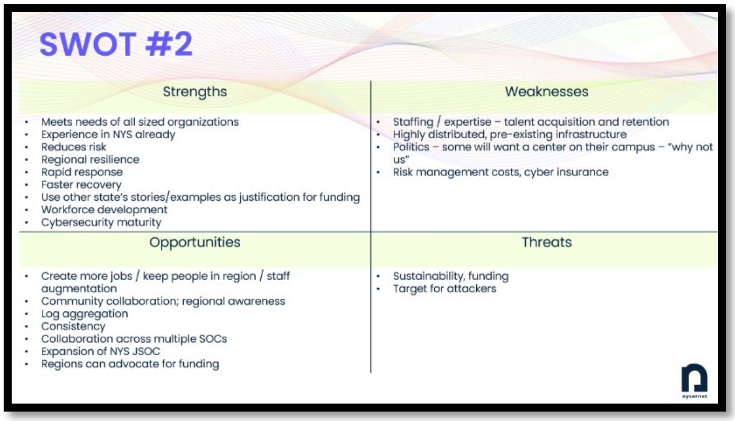
Next Steps: NYSERNet will develop a design advisory group to continue to refine this hybrid approach, secure funding support and implement a scalable RSOC that strengthens New York's research and education cybersecurity landscape.

Appendix A: Participant SWOT Raw Input



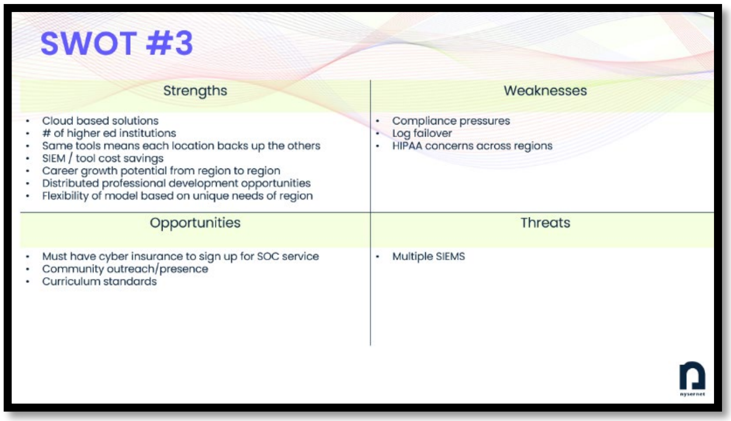
SWOT #1

Strengths	Weaknesses
• Easiest to roll out; lower cost due to one center • Workforce pipeline of students across state • Affordability of model for all sectors • Supports experiential learning for students • Visibility of threat actors across the state	• Scalability challenges, unique networks, behaviors, tech stack • Scoping • High liability (single point of failure) • Would there be a cap on # of co-op / interns per campus? • Travel to sites across the state • Name recognition of NN in the broader community is limited • High resources burden for NN • Student (pipeline) may be more inclined to intern at a place that is better known and/or pipeline of students may be inconsistent
Opportunities	**Threats**
• Workforce pipeline of students across state • Affordability of model for all sectors • Supports experiential learning for students • Visibility of threat actors across the state • Decrease cost due to one center • This model could act as a pilot for others • Leverage shared agency services (ITEC, SICAS, etc) • Leverage space across 64 campuses	• Sustainability to public organizations • Lack of connectivity in rural areas • Lack of infrastructure • Funding model for internship • "location" • Liability and compliance risks • Lack of institutions to perform community education • Limited workforce • Failure to procure relationships (territorial)



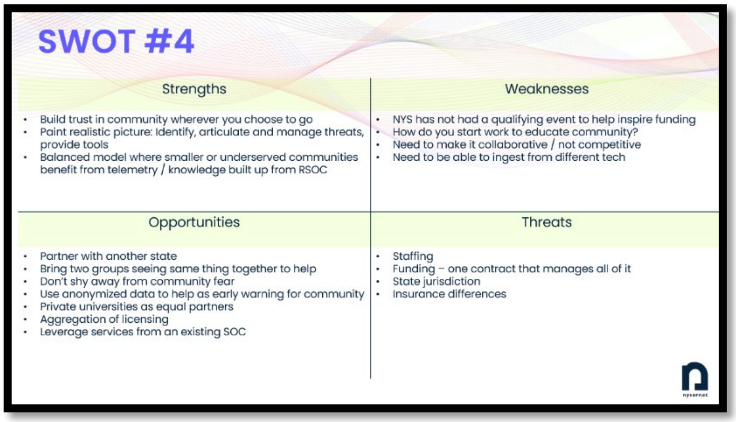
SWOT #2

Strengths	Weaknesses
• Meets needs of all sized organizations • Experience in NYS already • Reduces risk • Regional resilience • Rapid response • Faster recovery • Use other state's stories/examples as justification for funding • Workforce development • Cybersecurity maturity	• Staffing / expertise – talent acquisition and retention • Highly distributed, pre-existing infrastructure • Politics – some will want a center on their campus – "why not us" • Risk management costs, cyber insurance
Opportunities	**Threats**
• Create more jobs / keep people in region / staff augmentation • Community collaboration; regional awareness • Log aggregation • Consistency • Collaboration across multiple SOCs • Expansion of NYS JSOC • Regions can advocate for funding	• Sustainability, funding • Target for attackers



SWOT #3

Strengths	Weaknesses
• Cloud based solutions • # of higher ed institutions • Same tools means each location backs up the others • SIEM / tool cost savings • Career growth potential from region to region • Distributed professional development opportunities • Flexibility of model based on unique needs of region	• Compliance pressures • Log failover • HIPAA concerns across regions
Opportunities	**Threats**
• Must have cyber insurance to sign up for SOC service • Community outreach/presence • Curriculum standards	• Multiple SIEMS



SWOT #4

Strengths	Weaknesses
• Build trust in community wherever you choose to go • Paint realistic picture: Identify, articulate and manage threats, provide tools • Balanced model where smaller or underserved communities benefit from telemetry / knowledge built up from RSOC	• NYS has not had a qualifying event to help inspire funding • How do you start work to educate community? • Need to make it collaborative / not competitive • Need to be able to ingest from different tech
Opportunities	**Threats**
• Partner with another state • Bring two groups seeing same thing together to help • Don't shy away from community fear • Use anonymized data to help as early warning for community • Private universities as equal partners • Aggregation of licensing • Leverage services from an existing SOC	• Staffing • Funding – one contract that manages all of it • State jurisdiction • Insurance differences