NASCIO State IT Recognition Awards Nomination

State:	**New York**
Agency:	**Office of Information Technology Services (ITS)**
Award Category:	**Cross-Boundary Collaboration & Partnerships**
Project Title:	**Joint Security Operations Center (JSOC) Initial Stand-Up & Collaborative Technical Implementation**
Project Dates:	**February 22, 2022 – May 15, 2023**
Contact Information:	**Mathan Jebaraj** **Executive Director, ITS Project Management Office (PMO)** **Chief Portfolio Office** **Mathan.Jebaraj@its.ny.gov** **518-949-6964** **6 Empire State Plaza, Swan St. Bldg., Core 4, Fl 2** **Albany, NY 12228**

NY Joint Security Operations Center Initial Stand-Up and Collaborative Technical Implementation

IDEA

What problem or opportunity does the project address?

New York's leadership in finance, energy, transportation, healthcare, and other critical fields makes the State an attractive target for cyberattacks that can disrupt operations, including critical infrastructure and services to citizens. While government entities across New York State (including New York City government, multiple counties, cities, and the State government) have historically taken an independent approach to cyber defense and protecting the safety of their technology assets, acting alone is no longer optimal. As the frequency and sophistication of cyberattacks have grown, so too has the need for a "whole of government" approach and cross-boundary collaboration and partnership within New York.

Why does it matter?

A new type of emerging risk threatens our daily lives, and we must transform how we approach cybersecurity with rigor and seriousness to strengthen our ability to protect New York's institutions, infrastructure, our citizens, and public safety.

What makes it different?

The recently launched NY Joint Security Operations Center - JSOC (now known as the NYSOC) is the nation's first-of-its-kind cyber command center that provides a statewide view of the cyber-threat landscape and improves coordination and agility on threat intelligence and incident response. The highly effective statewide strategy and a shared command space for joint cyber security operations involve significant collaboration and partnership among NY entities.

What makes it universal?

This project addresses one of the State CIO Top 10 Priorities for 2023, Cybersecurity and Risk Management.

IMPLEMENTATION

What was the roadmap?

By September 2022, in less than 7 months, the JSOC Implementation Team determined a strategy, developed a plan, and created the operational foundation for New York Governor's vision of a 24x7x365 hub for cybersecurity coordination for NY. Through a collaborative effort between the NYS Office for Information Technology Services (ITS) and the NYS Department of Homeland Security and Emergency Services (DHSES), a facility to house the JSOC was established; JSOC 24x7 staffing was initiated; the Endpoint Detection and Response (EDR) shared service was developed; EDR deployment was initiated to the counties and the "big 5" cities; and a well-defined procurement (using the NYS Project Based IT Services (PBITS) contract) for the build-out of the JSOC technical infrastructure was developed, released and awarded. The technical, infrastructure build, considered a second (separate) phase of this program, went live in May 2023 providing the technical platform for data collection and a statewide view of the cyber-threat landscape to improve coordination on threat intelligence and incident response across the whole of NY State.

As part of the roadmap, Project Management Institute (PMI) based formal project management methodology was followed by NYS ITS Project Management Office (PMO) and the project met all security standards as well. The project team delivered JSOC implementation very effectively. Success comes from adding subscribers to the services provided by the NYSOC, and the deployment of active endpoints to inform the threat analysis function. With ITS, 48 counties and the "Big 5" cities currently engaged, and 46,000 (and growing) endpoints established, the JSOC continues to strengthen.

Who was involved?

Through leadership from the Governor's Office, Chief Cyber Office, the Office of Information Technology Services and the Division of Homeland Security and Emergency Services brought together cybersecurity teams in a shared command space including federal, state, city, and county governments, critical businesses and utilities, and other state entities like the New York State Police, MTA, Port Authority of New York and New Jersey, the New York Power Authority, among others. Statewide cyber conventions and forums provided a platform to promote the concept and attain buy-in statewide. A formal subscriber package and onboarding process facilitate the statewide entity partnerships needed for success.

How did you do it?

This effort is part of New York State Governor's unprecedented $61.9 Million investment in the state's cybersecurity infrastructure with an additional $30 Million program for localities to help bolster cyber defenses statewide.

NY Joint Security Operations Center Initial Stand-Up and Collaborative Technical Implementation

NYSOC is the nation's first-of-its-kind cyber command center that provides a statewide view of the cyber-threat landscape and improve coordination and agility on threat intelligence and incident response. The technology that powers the NYSOC includes overall security functionalities such as ease of use and management, adherence to a zero-trust security architecture (ZTA), and the ability to scale up performance and capacity to the needs of a true statewide cybersecurity solution. The core functions of the JSOC run on a robust Security Incident and Event Management (SIEM) platform, which receives log data from subscribers. The SIEM then reviews logs ingested in real-time to identify security concerns which in turn generate tickets in an incident management system for analyst review and notification to the subscriber for further action. The NYSOC uses multiple threat intelligence feeds which provide the most up-to-date information and the inclusion of artificial intelligence (AI) and machine learning (ML) to ensure accurate alerts and actions rather than false positives.

The NYSOC also plays a key role in providing shared services across NY state. The deployment of the Endpoint Detection and Response (EDR) software has been a tremendous success with coverage statewide. An Attack Surface Management service, due to be offered next, will provide NYSOC subscribers with a comprehensive view across the current cyber threat landscape. By combining the data received through multiple sources, the NYSOC will have visibility into the cybersecurity posture of the entire state that was never-before possible. This will allow the NYSOC to correlate across multiple alerts and subscribers and provide a source of custom threat intelligence that will be shared with subscribers to improve our collective defenses against ever-increasing threat and cyber risk. This level of data consolidation not only provides a primary source of truth but also becomes crucial in determining what future shared services will be developed and offered to best mature cybersecurity across the State.

IMPACT

What did the project make better?

The initial set up of the NY Joint Security Operations Center (NYSOC) enabled coordinated threat analysis and intelligence sharing between NYC and the state, and initiated the process of onboarding the counties, cities, and major metropolitan entities to "subscribe" to the NYSOC services. The centralized team and newly implemented NYSOC technical infrastructure provide a 24x7x365 whole of state view of the cyber threat landscape enabling faster identification and incident response across the state. Prior to this, counties, cities, and major metropolitan entities were on their own to manage a constant and ever-changing adversary. Considering the serious, emerging risks of wars, cyber-attacks and threats across the world, this project delivers critical protection for our citizens and prevention of most cyber-attacks.

How do you know?

The NYSOC has already had some significant proof of success in the swift detection and containment of a ransomware infection impacting a NYSOC subscriber. Early detection and actions taken through the NYSOC prevented the spread to other systems, allowing for services to be restored much faster than would have been possible before. One of the early success stories was the NYSOC's quick detection of a ransomware at a county hospital that was expediently contained before crippling live saving systems.

What now?

With the groundwork established, NYSOC will grow the subscriber base and continue to add and support more cyber shared services protecting our constituents from cyber threats across the state and ever strengthening our cybersecurity posture. Protecting a county hospital is just a recent testament to NYSOC's extraordinary capabilities. The project has proven to be worthy of the ongoing investment and will continue to deliver cyber protection success.