

# STARNOVA - Scalable Technology to Accelerate Research Network Operations Vulnerability Alerts



Extending the UCSD Network Telescope with greynet coverage and ML-based anomaly detection to protect NSF scientific cyberinfrastructure at SDSC

PI Ka Pui (Ricky) Mok · co-PI kc claffy (CAIDA, UC San Diego) · co-PI Fabian E. Bustamante (Northwestern University)

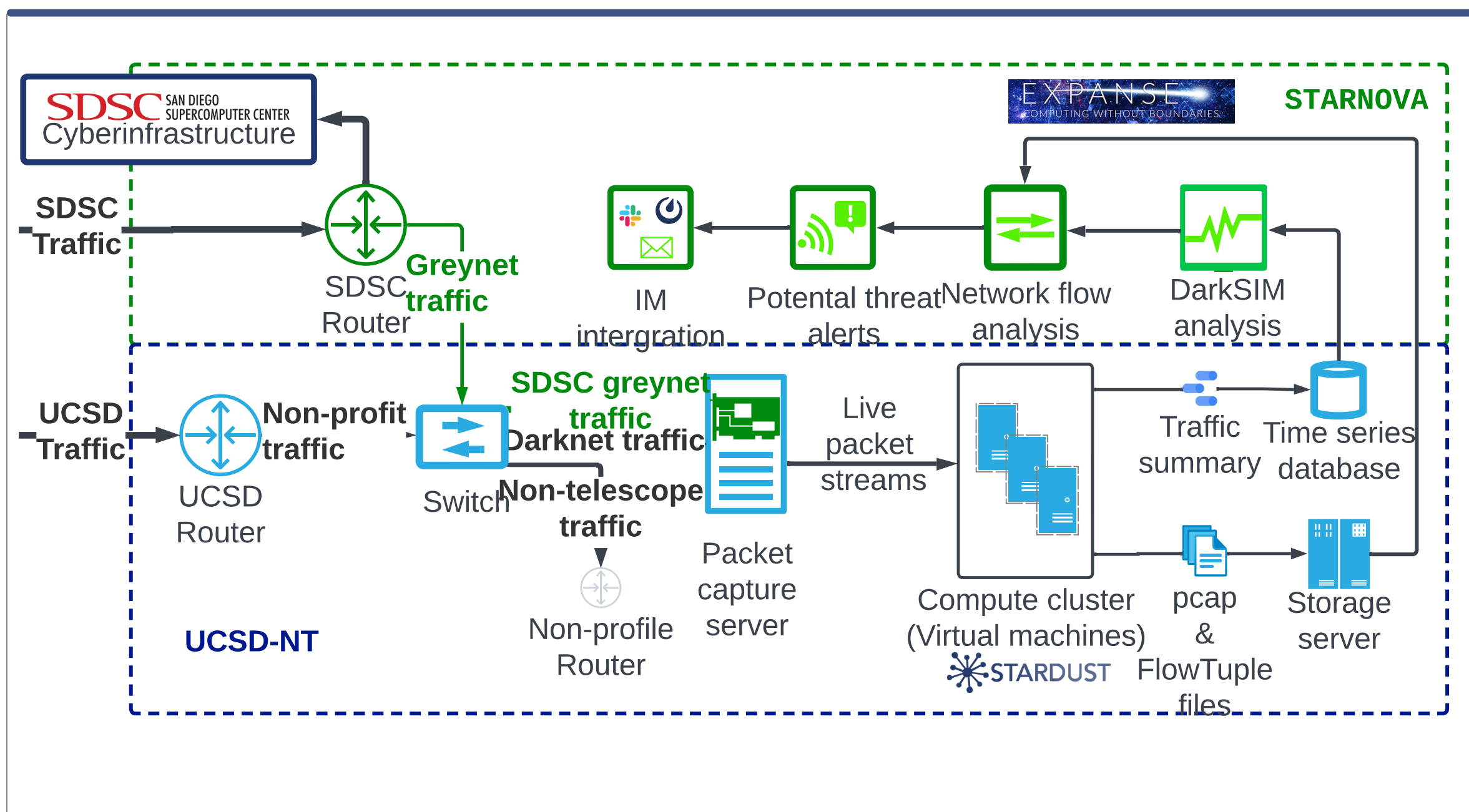
## Motivation

- ▶ Derive threat intelligence from Internet Background Radiation (IBR) sent toward UCSD network telescope (UCSD-NT) and San Diego Supercomputer Center (SDSC)'s production network to improve the robustness, integrity, and resilience of SDSC's cyberinfrastructure
- ▶ Expand the capability of UCSD-NT infrastructure to
  - 1) cope with new traffic source and growing IBR traffic volume
  - 2) facilitate the sharing of data with researchers and industry partners

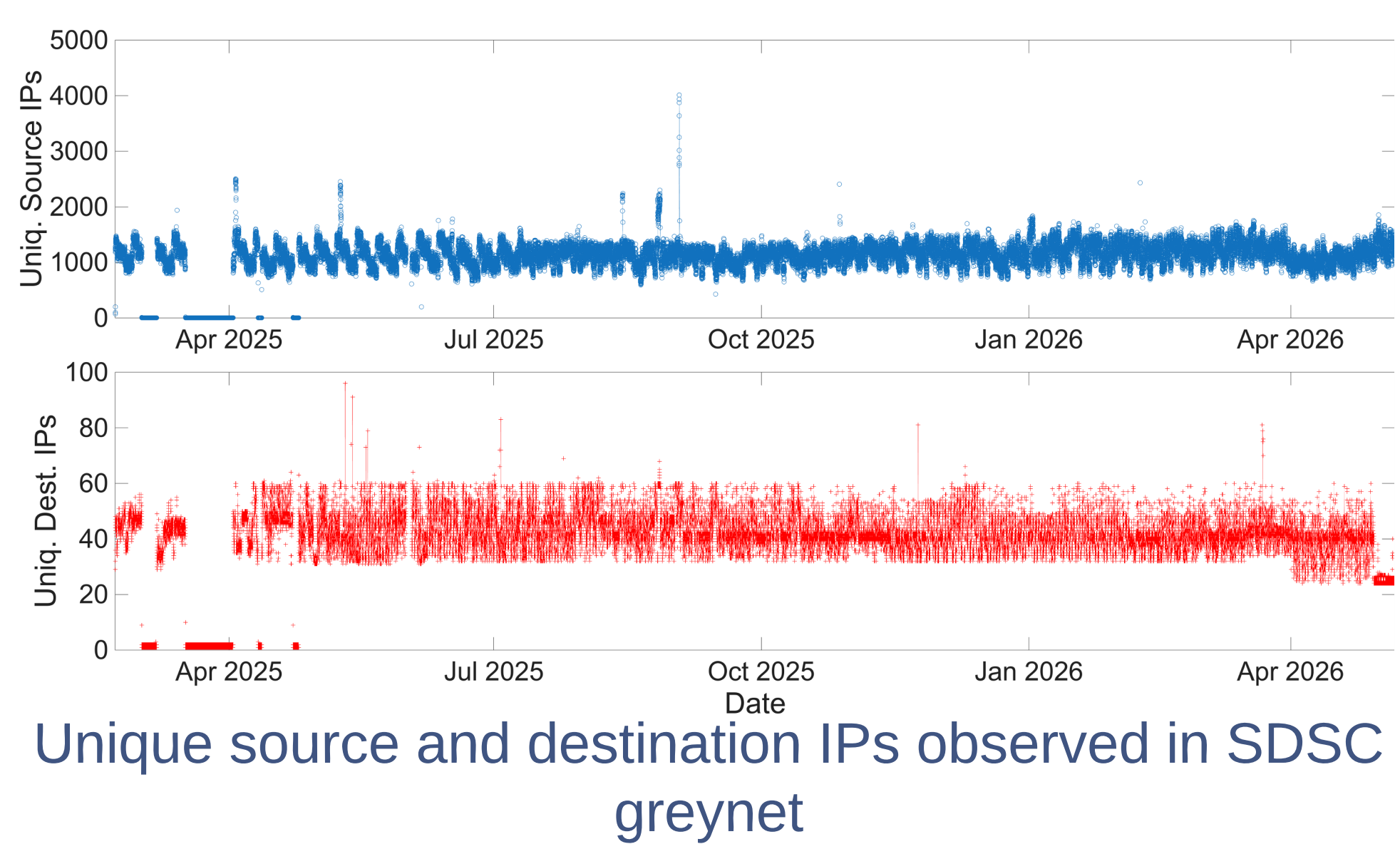
## Progress

- ▶ Deployed 400Gbps traffic aggregators to SDSC production networks
- ▶ Developed software tools to automatically identify usable addresses for monitoring with iBGP tables
- ▶ Migrated traffic processing to new infrastructure supported by this award
- ▶ Developed DarkSIM, a timeseries-based ML method to detect anomalies in IBR

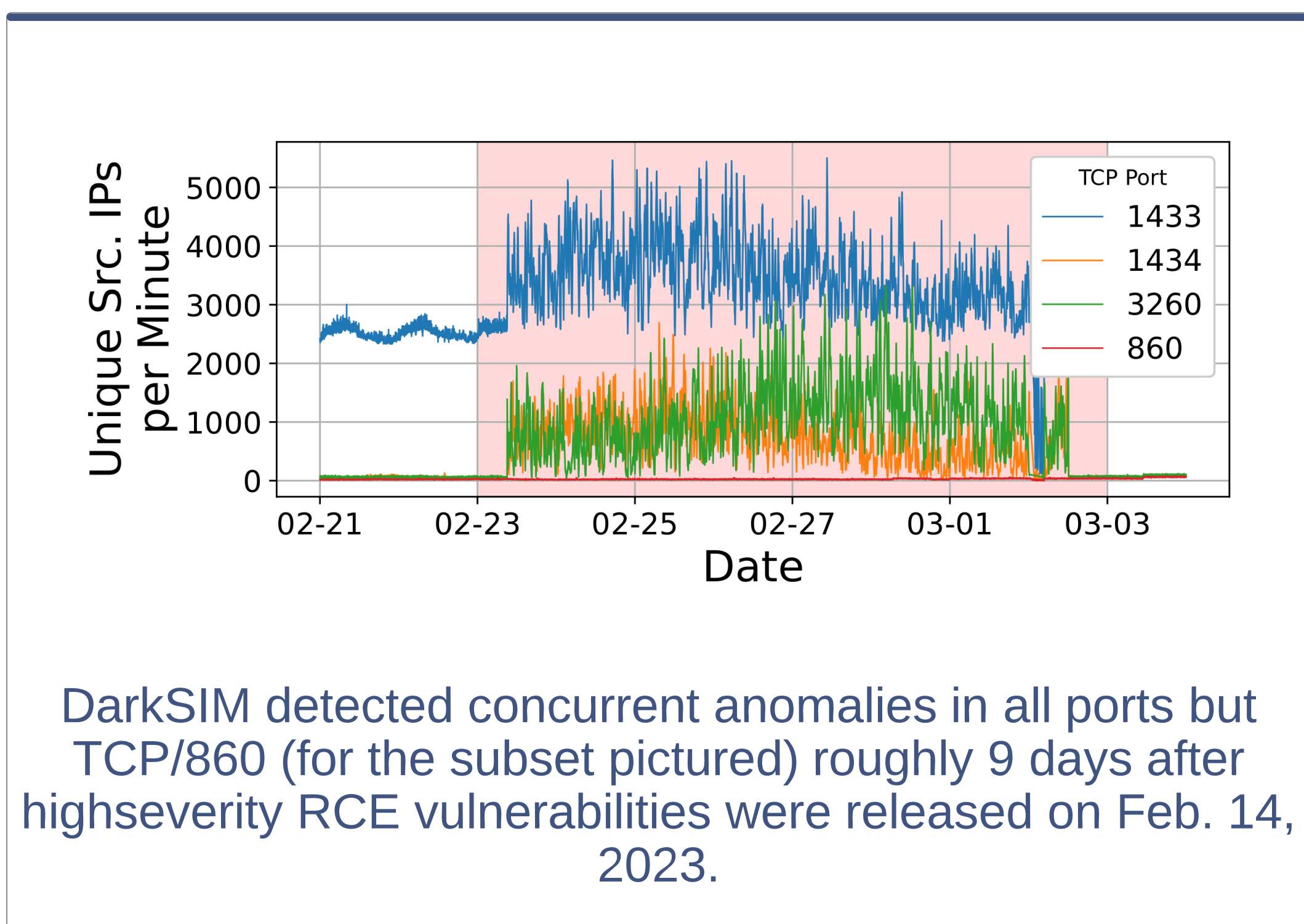
## STARNOVA Infrastructure



## SDSC Greynet



## DarkSIM in action



## Publications

Gao et al., "DarkSim: A Similarity-Based Time Series Analytic Framework for Darknet Traffic", Proc. ACM IMC 2024.

Sultana et al., "Survey on Packet Filtering", ACM CCR Vol. 54 (3) p. 2-9, 2024.

Chan et al., "Analyzing Internet Background Radiation with Reflective Network Telescopes", Proc. ACM/IRTF ANRW 2025.

Männel et al., "Lessons Learned from Operating a Large Network Telescope", Proc. ACM SIGCOMM 2025.

Männel et al., "Hilby: Hilbert Interactive Prefix Plots", Proc. ACM SIGCOMM Demo 2025.

Degen et al., "Through a Smaller Lens: Revisiting Opportunistic Analysis using Network Telescopes", Proc. Passive and Active Measurement Conference, 2026.

