CICI: RSSD: Massive Internal System Traffic Research Analysis and Logging (Award #2232819)

Alexander Merck, Tracy Futhey, Charley Kneifel, Neil Gong

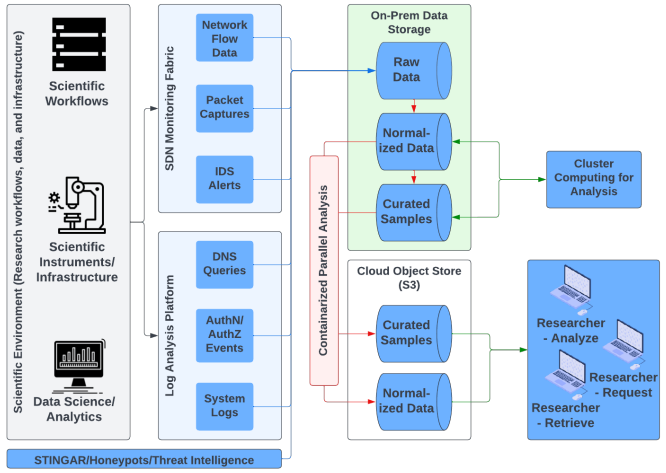
Duke University

NSF

Problem and Motivation

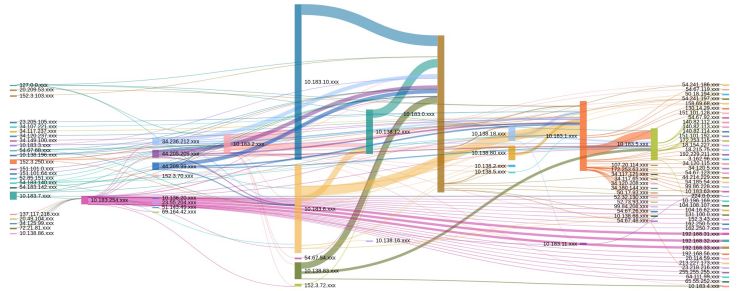
- Research infrastructure has different characteristics than traditional enterprise systems and present unique security challenges
- Cybersecurity practitioners and researchers need access to network data to identify, classify and defend against security threats within research environments
- Sustaining such a dataset would require a monitoring and data collection framework and infrastructure to capture, analyze and share the relevant data

Approach



Results

- Relationships established between network connected lab devices
- Understanding of communication channels and protocols used by lab devices

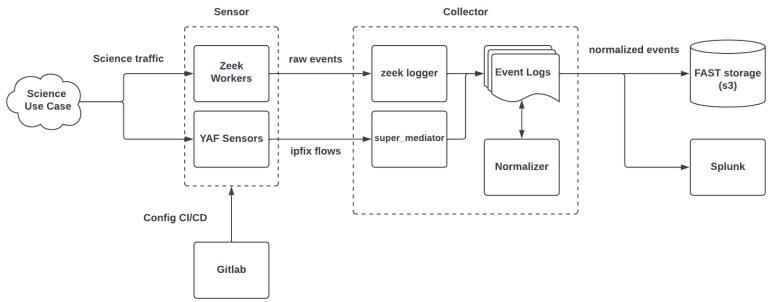


Sample traffic relationship of research networks

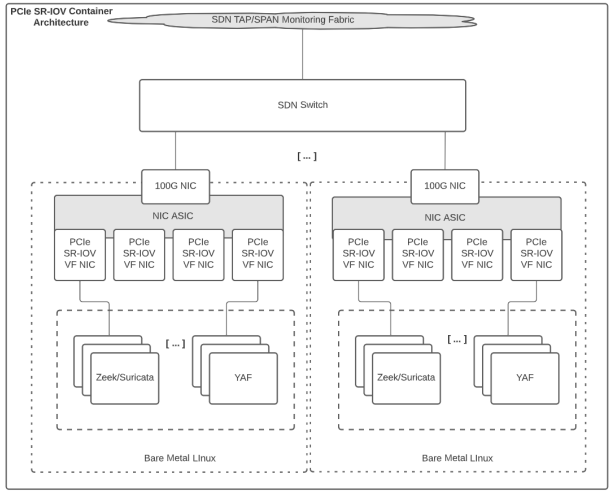
- Visibility and analysis of hardware and network failures within lab environments
- Detection of security threats within research environments
- Privacy-preserving framework for public datasets using salted hashes and ASNs

Technical Solution

- Containerized sensing software using Docker
- Line-rate network speeds via SR-IOV passthrough
- Privacy preservation via data collector systems and data normalizers
- Automated configuration and orchestration via CI/CD pipelines



Monitoring infrastructure architecture



SR-IOV passthrough architecture

Projects Using MISTRAL Datasets

- Code+ and Data+ research projects in 2024 and 2025
- Unauthorized VPN service analysis and detection
- Undergraduate penetration testing course labs
- STINGAR honeypot monitoring and augmentation
- Network security analysis of public student VMs

Data Sharing

- Data will be shared via OSDF
- Deidentified data will be shared via public namespace
- Identifiable data will be shared via private namespace

MISTRAL