# NOIRLab - ITOps

Christopher Morrison, Mauricio Rojas, Eduardo Toro

SA3CC Meeting 2024

AURA NSF NOIR Lab

# Agenda

- NOIRLab IT Operations (ITOps)
  - Cybersecurity Incident
- Backbone Networks Activities
  - La Serena Center, Tucson Center
- NOIRLab Program Integration
  - CSDC
  - Gemini and MSO
- NOIRLab/ITOPs Network Upgrade Project
  - Current Status

# NOIRLab IT Operations

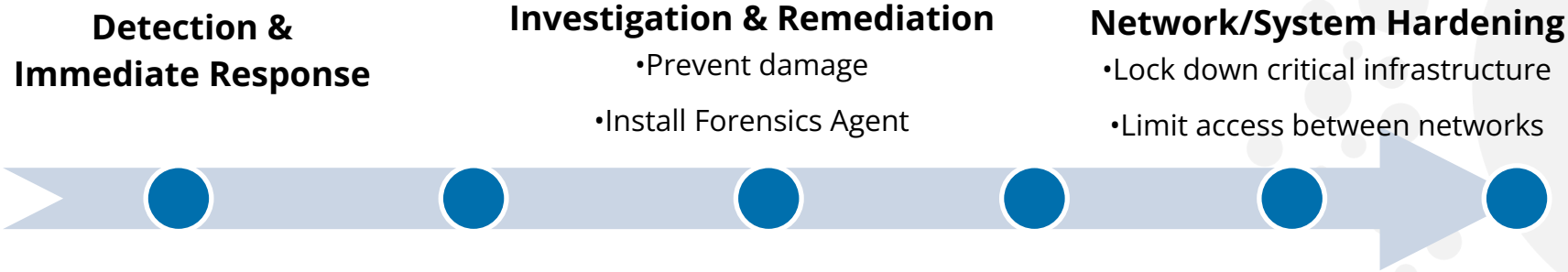
**Cybersecurity Incident Summary**

- NOIRLab's Systems were compromised on August 1,2023
- The incident was detected in real time and interrupted within 40 minutes
- Cybersecurity Incident Response Plan was activated
- Professionals in cybersecurity brought in to assist with response & forensics

# NOIRLab IT Operations

**Cybersecurity Incident Summary**

## Cybersecurity Incident Response Plan is Critical



**Detection & Immediate Response**

**Investigation & Remediation**

- Prevent damage
- Install Forensics Agent

**Network/System Hardening**

- Lock down critical infrastructure
- Limit access between networks

**Engage Outside Experts**

- Legal
- IR Vendor
- **Communications**

**Plan to Restore and Return to Operations**

- Coordinate with Observatory Operations
- Review new security protocols

**Communicate Lessons learned**

# NOIRLab IT Operations

Infrastructure Enhancement

- Systems and services locked down and hardened
- Secure administrator account management & Role-Based Access Control (RBAC)
- Privileged Access Management (PAM)
- End-Point Detection and Response (EDR)
- Multi-factor authentication (MFA) on all services, external **and internal**

# NOIRLab IT Operations

Infrastructure Enhancement

- Network segmentation & Isolation
  - Controlled access management between network segments
- Tools and service to provide access to critical infrastructure and control access to network segments
- Restricted inbound & outbound traffic flow
- Limited outward-facing services - stop and question each process - **everywhere**!

# NOIRLab IT Operations

Infrastructure Enhancement

- Recovering Remote Access
  - Remote access solutions for staff to **restricted** resources
  - Remote access for external collaborators to **internal** resources
  - Remote access for vendors to **do specific tasks** only
- Outside of the box solutions to minimize risk
- All remote access must be justified and approved

# NOIRLab IT Operations

**Next Generation Firewalls**

- Advance in Hardware/Software standardization : **Tucson Data Center**
- Increased number of **limited** Tunnel Profiles for Remote Observing Functionalities (CTIO & SOAR) → Deployment in StandBy due to modifications of Authentication services
- **Implementation 2FA / MFA : Using PingOne Cloud Service to NOIRLab**
- ResearchSOC Initiative (https://researchsoc.iu.edu/)

**Network Tasks on Backbone devices**

- Evaluating new Backbone devices at AURA/NOIRLab
  - Planning new Topology using HA implementation

**Network Services & Collaborative Tools**

- Implementing Virtualization and Storage Clusters (CTIO, GN and **Tucson**)
- Unified productivity suite deployed to all NOIRLab Staff

# Backbone Network activities

**La Serena Center (LSC)**

- Chile to USA links
  - **Fixing ACL in Border Router**
- La Serena <-> Santiago
- Cerro Pachon <-> La Serena
- DWDM Equalization

**Tucson Center (TUC)**

- **Internet 2 Link (Sun Corridor)**
- **Tucson <-> Kitt Peak**
- **Fiber Optic recovery**

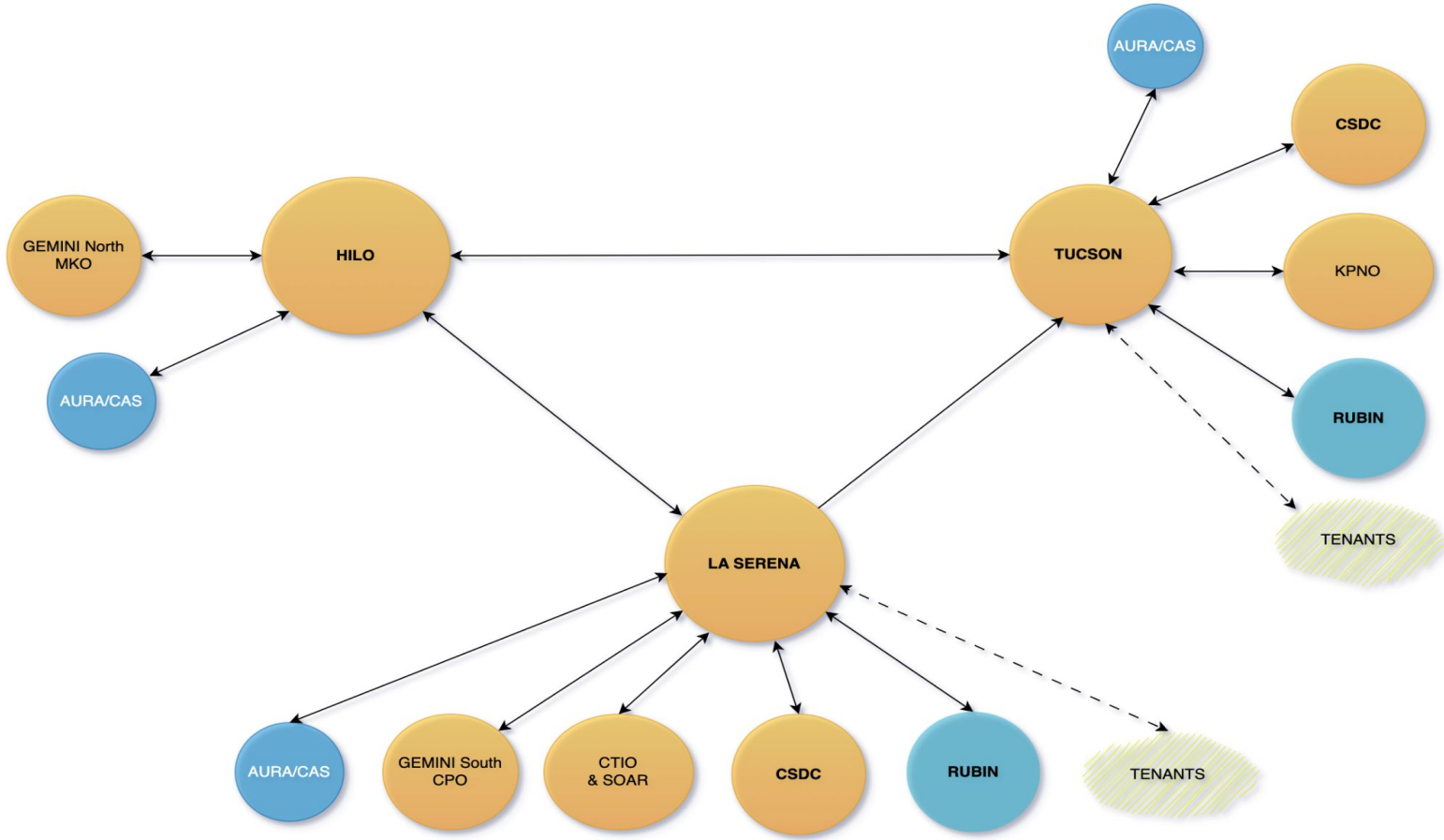
**Hilo Center (HBC)**

- Internet 2 Link
- Hilo <-> Mauna Kea

# NOIRLab Program Integration

- CSDC (Community Science & Data Center)
  - https://noirlab.edu/science/programs/csdc
  - Working together to implement improvements to:
    - Benefit service delivery
    - Establish high-availability, reliable, resilient and secure services
    - Offload system administration to service teams
- Gemini & MSO Integration
  - Continued implementation of secure interconnections between Programs
  - Leveraging new NOIRLab IT infrastructure to improve inward and outward-facing services.

# NOIRLab Program Integration



# NOIRLab Network Upgrade Project

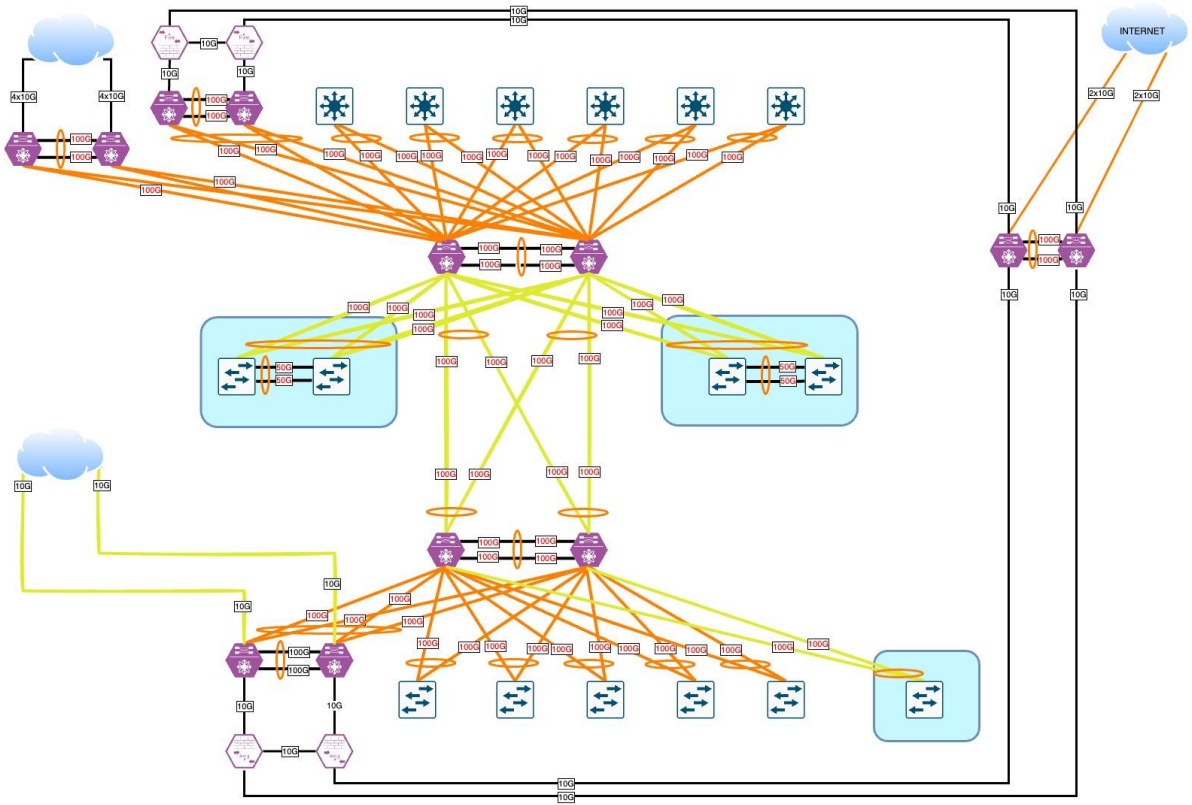
**NOIRLab Networking Upgrade Project**

- LAN Design in all Locations : Still in progress
  - Priority : Tucson Base facilities (Design and Purchase equipment) **-> In progress**
- WiFi Upgrade : Implementation In Progress at La Serena Center**-> Pending**
- WAN Design (VPN S2S Matrix updated, NGFW and Border routers standardization in HA): -> **Updated**

**Planning Implementation based on standard technologies (LSC) :**

- Preparing Setup in BDC La Serena (Optics Hardware / Unified Management Tools)

# NOIRLab LAN Design : Integrated with AURA Backbone



# NOIRLab - ITOps

Christopher Morrison, Mauricio Rojas, Eduardo Toro

SA3CC Meeting 2022

AURA NSF NOIR Lab