LIGHTS

Cybersecurity Through Interoperability

Grid-Interop 2011

What is LIGHTS?

About:

Non-profit initiative to provide deployable cybersecurity options to ICS facilities

Purpose:

Visibility into and Control of Cybersecurity and Compliance for ICS Asset Owners

Method:

Open Source Monitoring by LIGHTS-Certified Managed Security Service Providers (MSSPs)

Why LIGHTS?

Why:

Majority of ICS facilities unable to address cybersecurity to meet the National Critical Infrastructure need

Origin:

ICS Asset Owners asking for standardized programs to provide comprehensive cybersecurity solutions

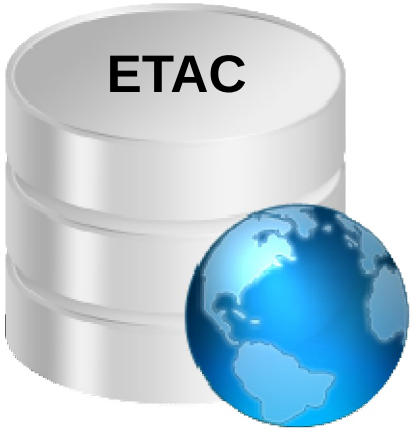
Who:

LIGHTS founders come from industry, vendors and service providers

LIGHTS Overview

- LIGHTS Certifies Vendors, MSSPs and Consultants
- LIGHTS MSSPs offer standard menu to facilities
- Base package:
  - Open Source SIEM sensor installed at utility site
  - MSSP monitors sensor 7x24
  - Energysec Tactical Awareness Center (ETAC)
  - Membership fee includes sensor and installation
  - Flat rate monthly monitoring fee
- Options
  - Unmanaged Open Source SIEM
  - LIGHTS Certified commercial products and services

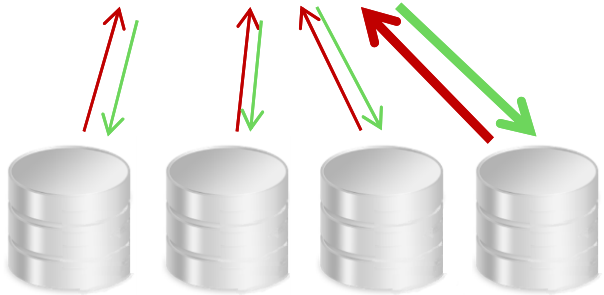
Energysec Tactical Analysis Center



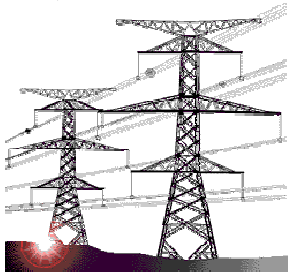
- **Cross Industry and Cross Sector Awareness**
- **Coordinates with other National Centers**

Anonymized Meta Data

LIGHTS Certified MSSPs

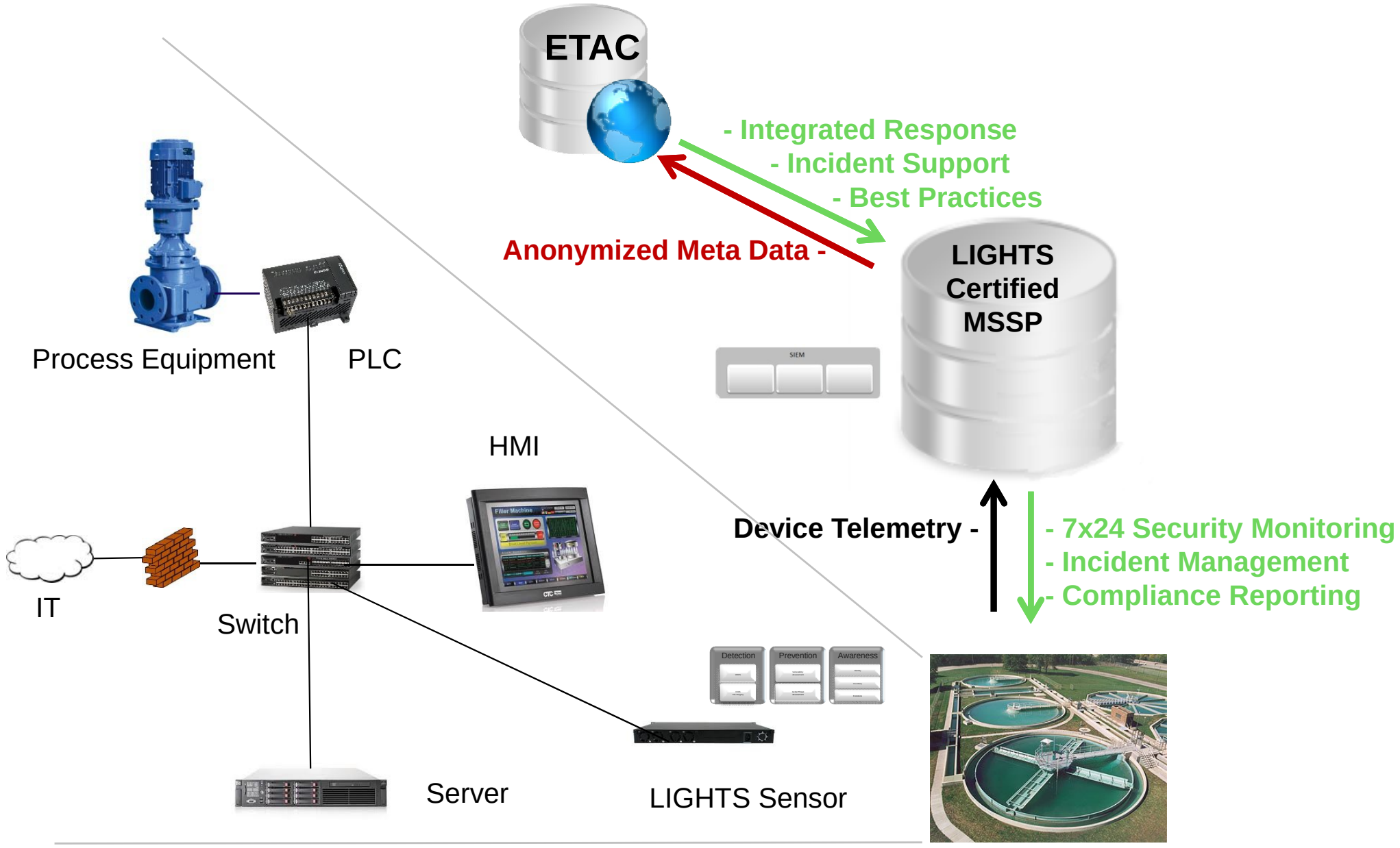


- Incident Management
- Coordinated Response
- Best Practices



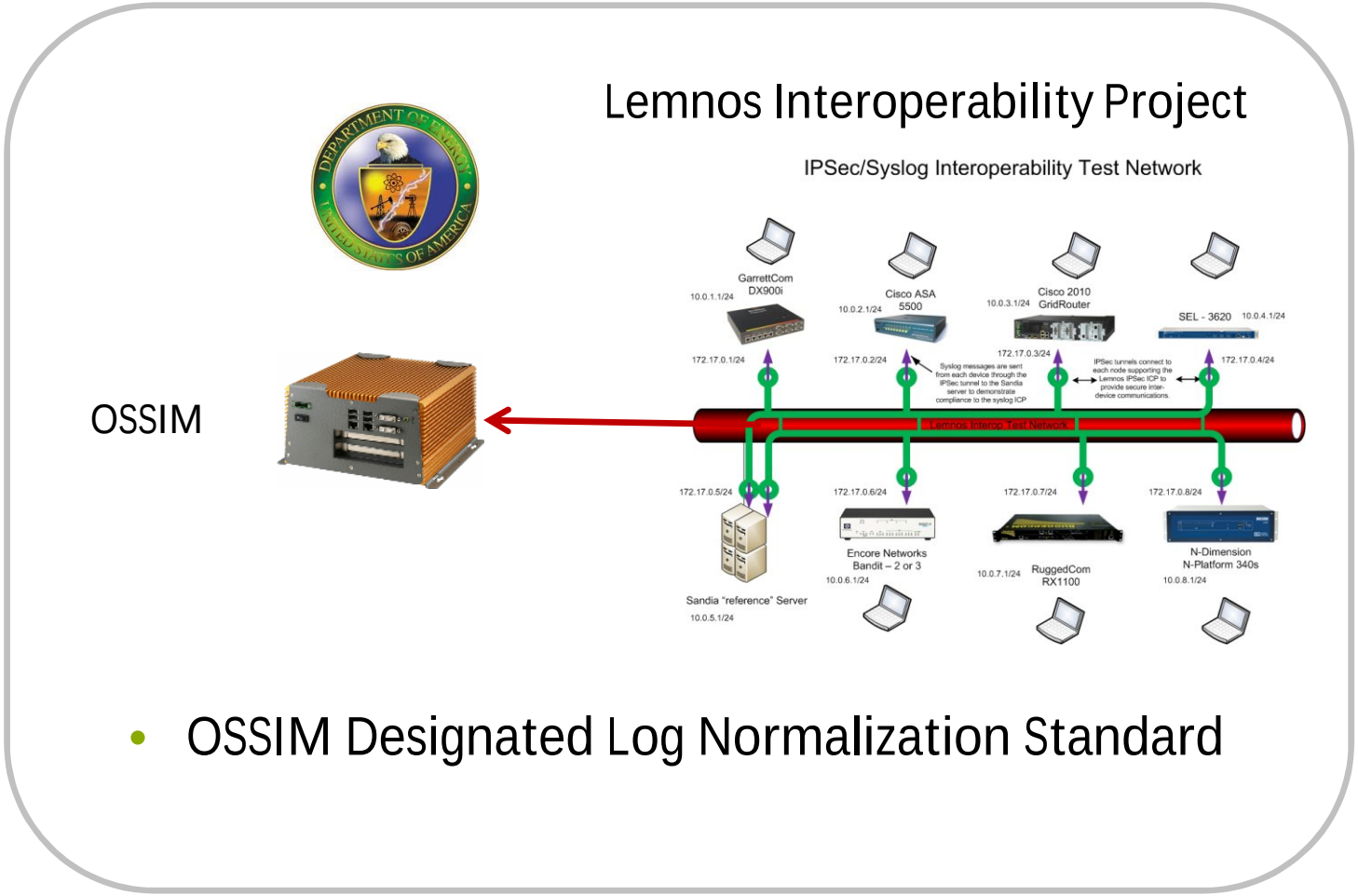
LIGHTS

LIGHTS MSSP Architecture



Standardized Open Source Sensor

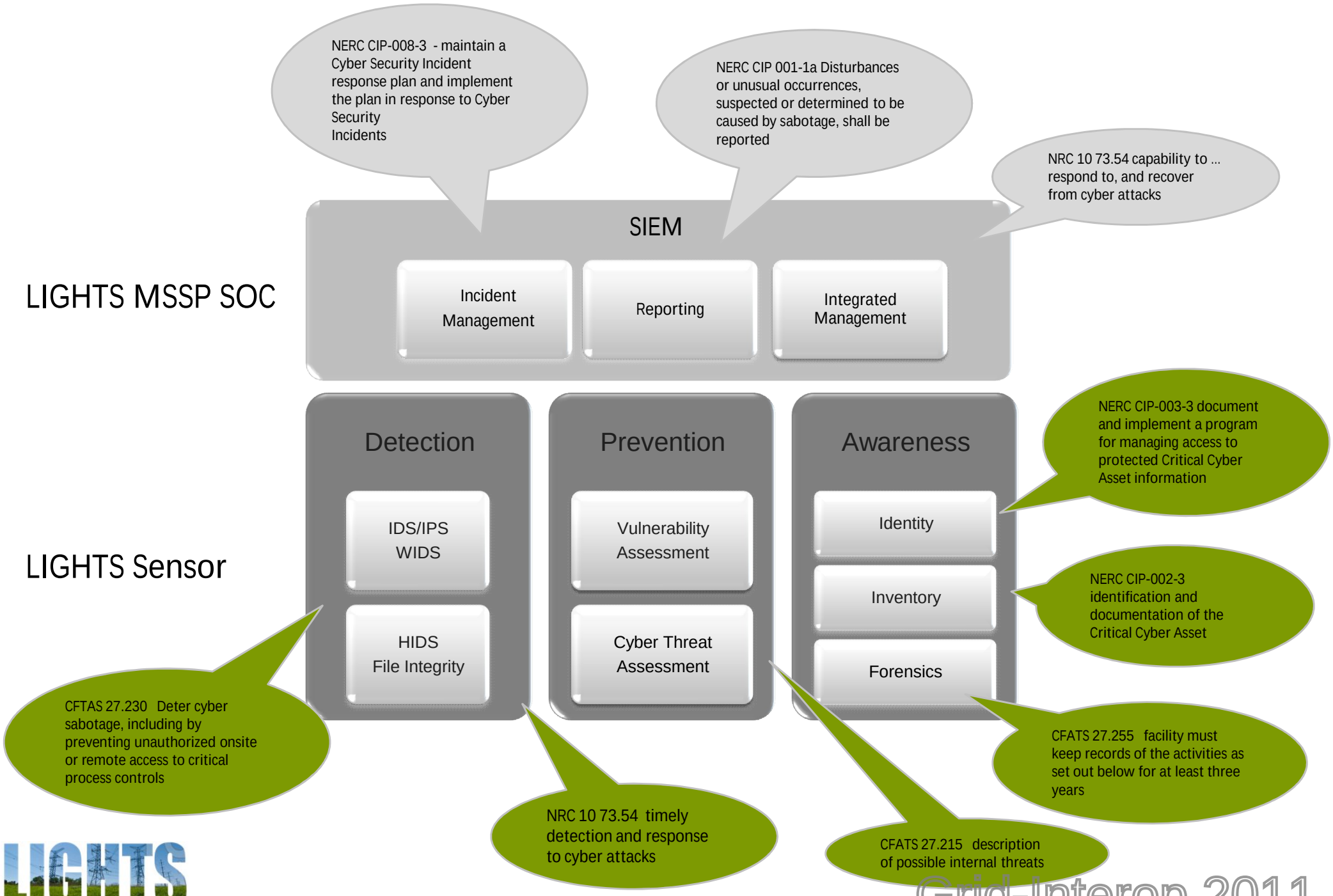
- Consistent Facility and MSSP Model
  - Includes all standard security capabilities
  - Non-commercial tools



- OSSIM Designated Log Normalization Standard

LIGHTS

Capability Architecture



LIGHTS

Grid-Interop 2011

Summary

- Practical and economical framework
  - Non-profit structure ensures vendor neutrality
  - Certified providers offer high security for low resource
- Framework for regulatory requirements
  - Complete auditing framework for compliance
  - Modular capabilities can be exchanged for commercial solutions
- Control of safety and reliability
  - Real-time visibility and monitoring confirms cyber assets' integrity
  - Attacks result in specific actionable response and defense
  - ETAC provides cross-facility and cross-sector awareness

Q&A

?