Intelligence & National Security Forum

Achieving Resilience in Our Nation's Mission Critical Architectures with Real-Time Situational Awareness

May 11, 2018

Critical Asset Mapping

Brian Biesecker
Technical Director, Intelligence Community

May 11, 2018

This presentation is unclassified in its entirety

Fundamental Problems that GIS can help you solve

- Identify impacts to your mission, operations, business activities, critical systems, or critical infrastructure from a Cyber Attack, IT outage or impairment

- Prioritize the work of your IT Team or Cyber Security Team in the context of your most important missions, operations, business activities, critical systems, or critical infrastructure

- Provide shared situational awareness across your organization

- Refine your Cyber Forensics Analysis efforts

Cyberspace Re-Considered

It's mappable

Social / Persona Layer

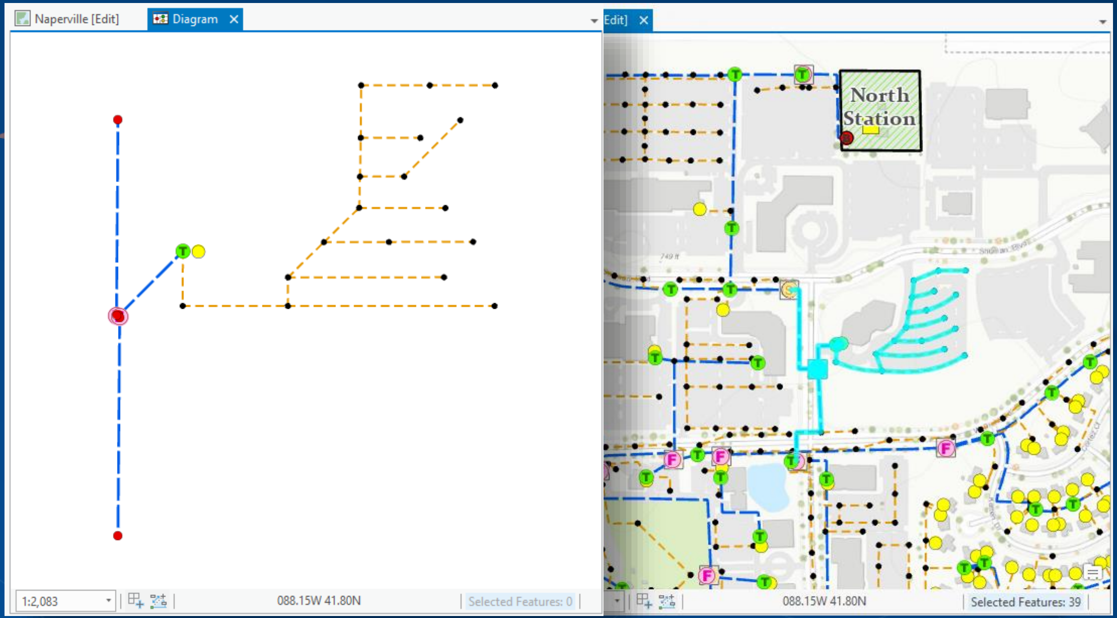
Device Layer

Logical Network Layer

Physical Network Layer

Geographic Layer

Utility Network

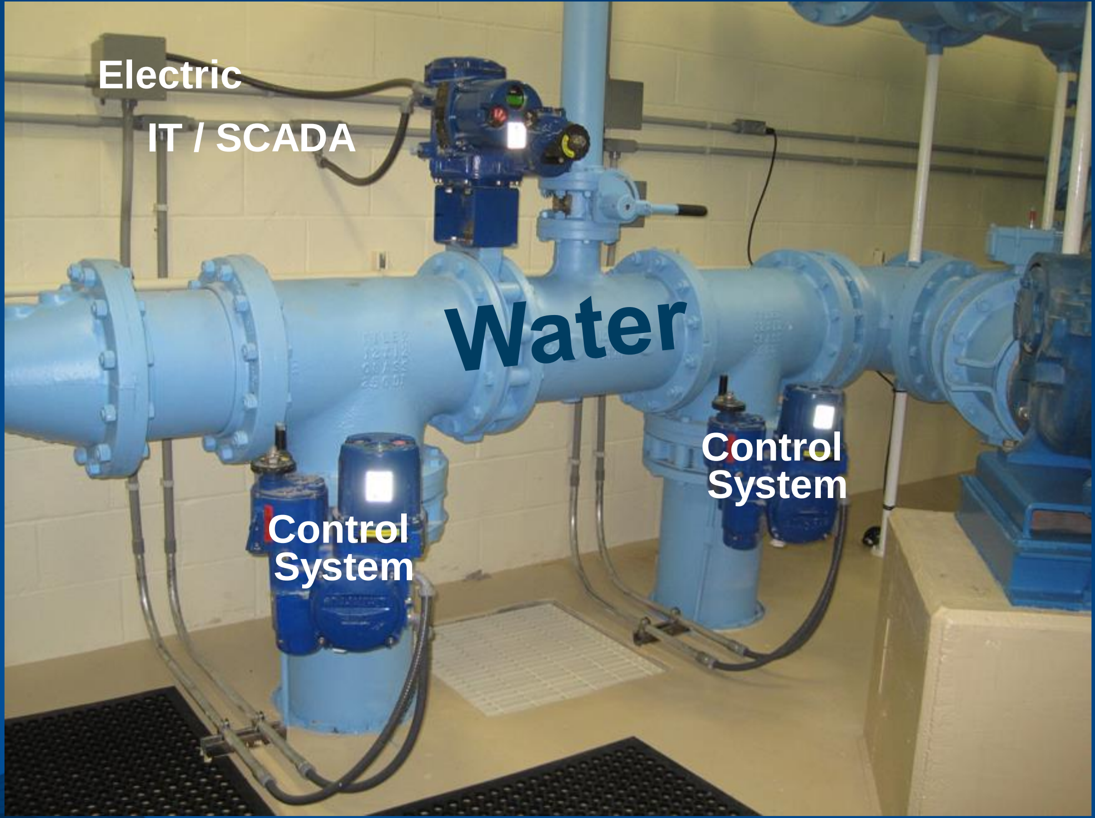


1:2,083 | 088.15W 41.80N | Selected Features: 0

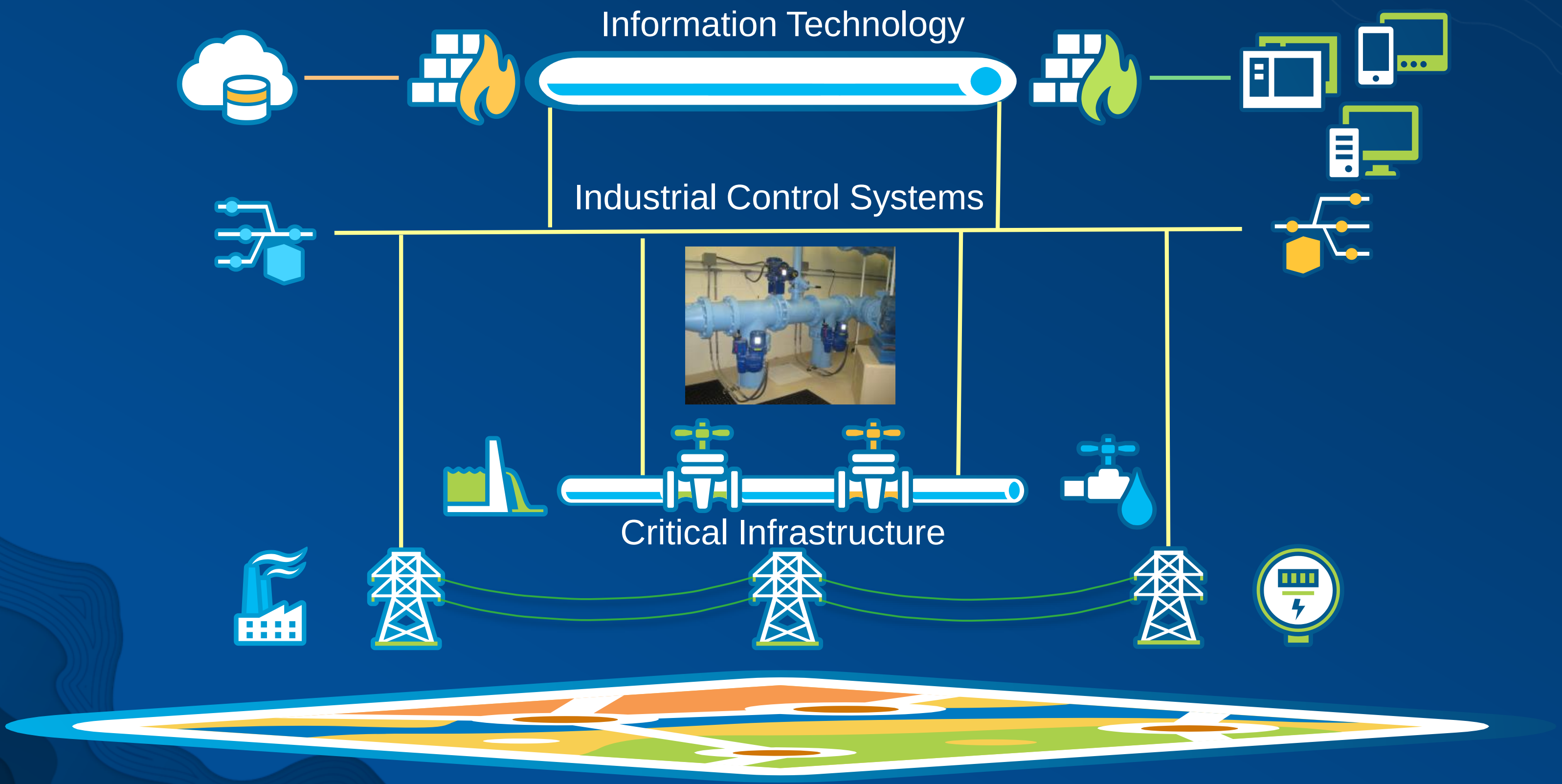
088.15W 41.80N | Selected Features: 39

- Each device in cyberspace is owned by someone (no 'global commons')
- Electro-mechanical devices exist in space-time and interact with physical events
- Geography is required to integrate and align cyberspace with other data

Cross Domain Consequence Analysis

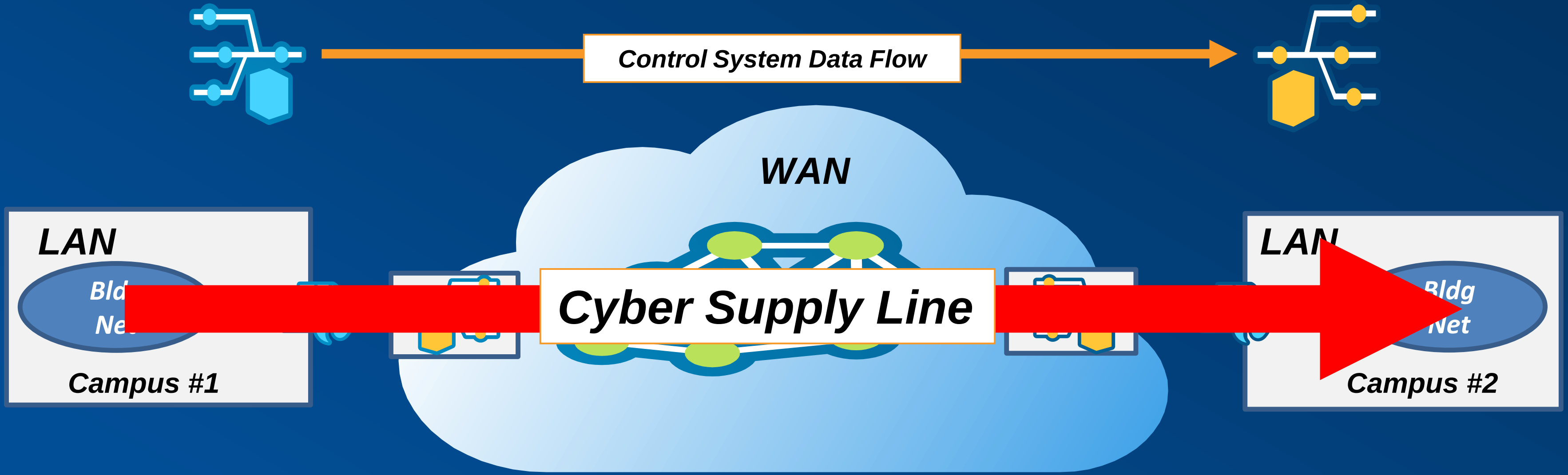


Cross Domain Consequence Analysis



The Cyber Supply Line

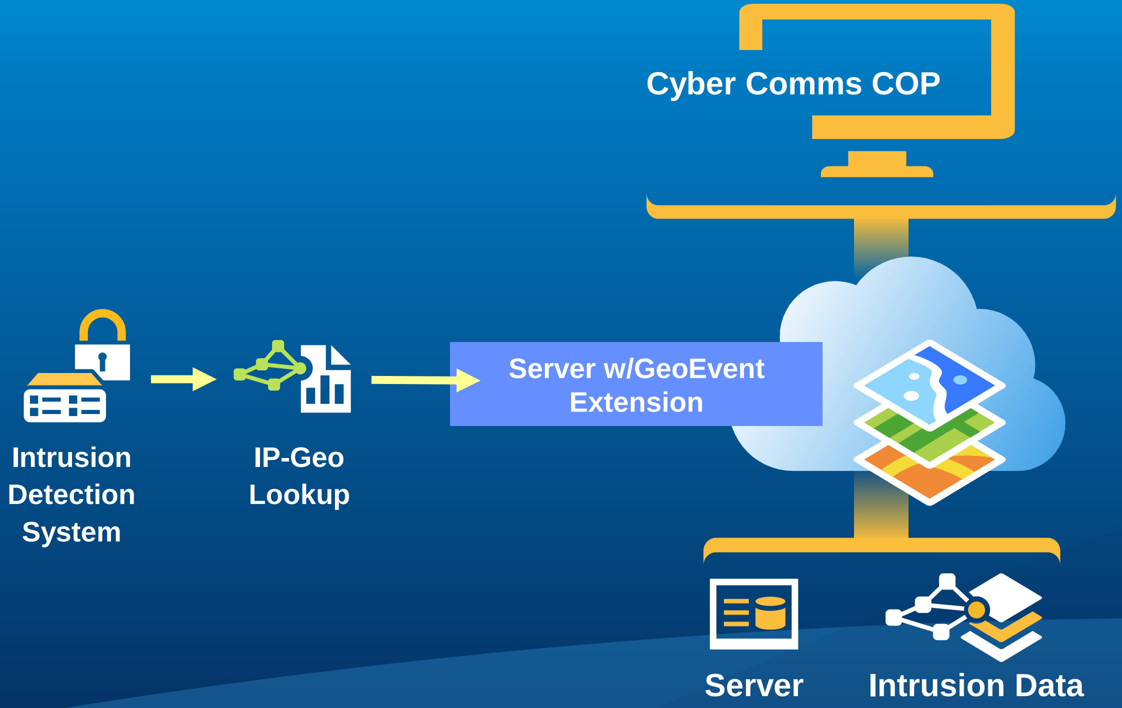
A vector of devices and network paths



- Cyber Supply Line (CSL) is a *consistent* path through the infrastructure
- CSL focuses resources on only the devices that are critical
- Managing data flows is similar to traffic routing; an Esri core competency

Enhancing Cyber Common Operating Pictures

Geography provides deeper understanding



Cyber Comms COP

Intrusion Detection System

IP-Geo Lookup

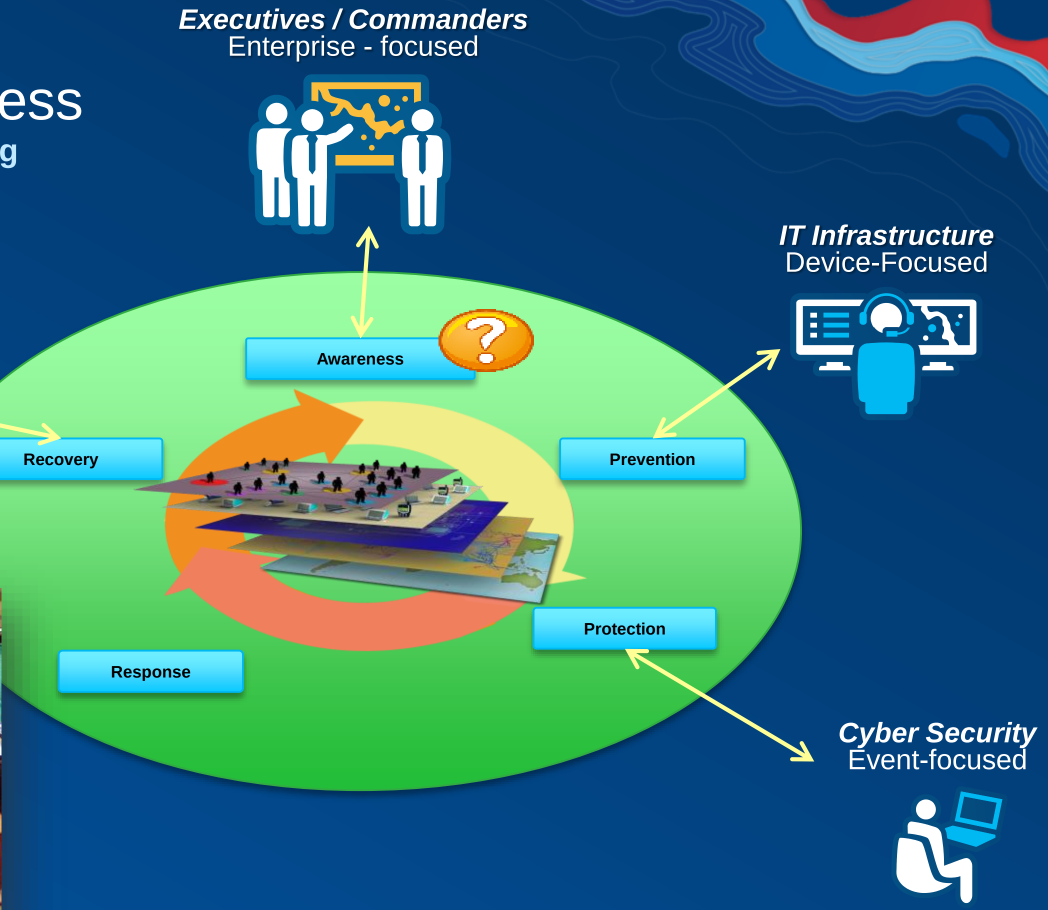
Server w/GeoEvent Extension

Server

Intrusion Data

Share Situational Awareness

Integrating to improve information sharing



ArcGIS Integration with Cyber Security Tools

Executives

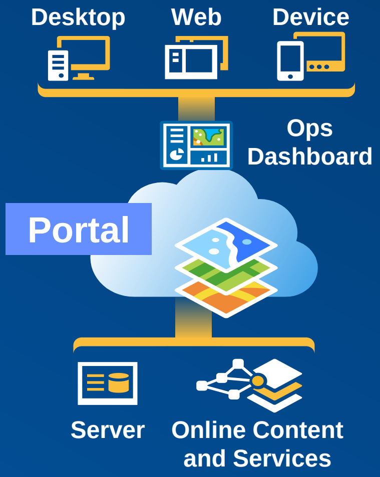
Executive Dashboards -
Status Reports, Trends,
Brand Sentiment, Financials

Operations

Ops Data -
Mission Activity, Status Reports,
Real-time monitoring

Human Resources

HR Database -
Personnel, Orgs,
Locations, Travel



Desktop

Web

Device

Ops Dashboard

Portal

Server

Online Content and Services

Cyber Security

Cyber Tools & Data-
IDS/IPS, HBSS, Virus Scanning,
Patch Monitoring

IT Operations

IT Tools & Databases -
IT Inventory, Device Locations,
Health and Status Monitoring

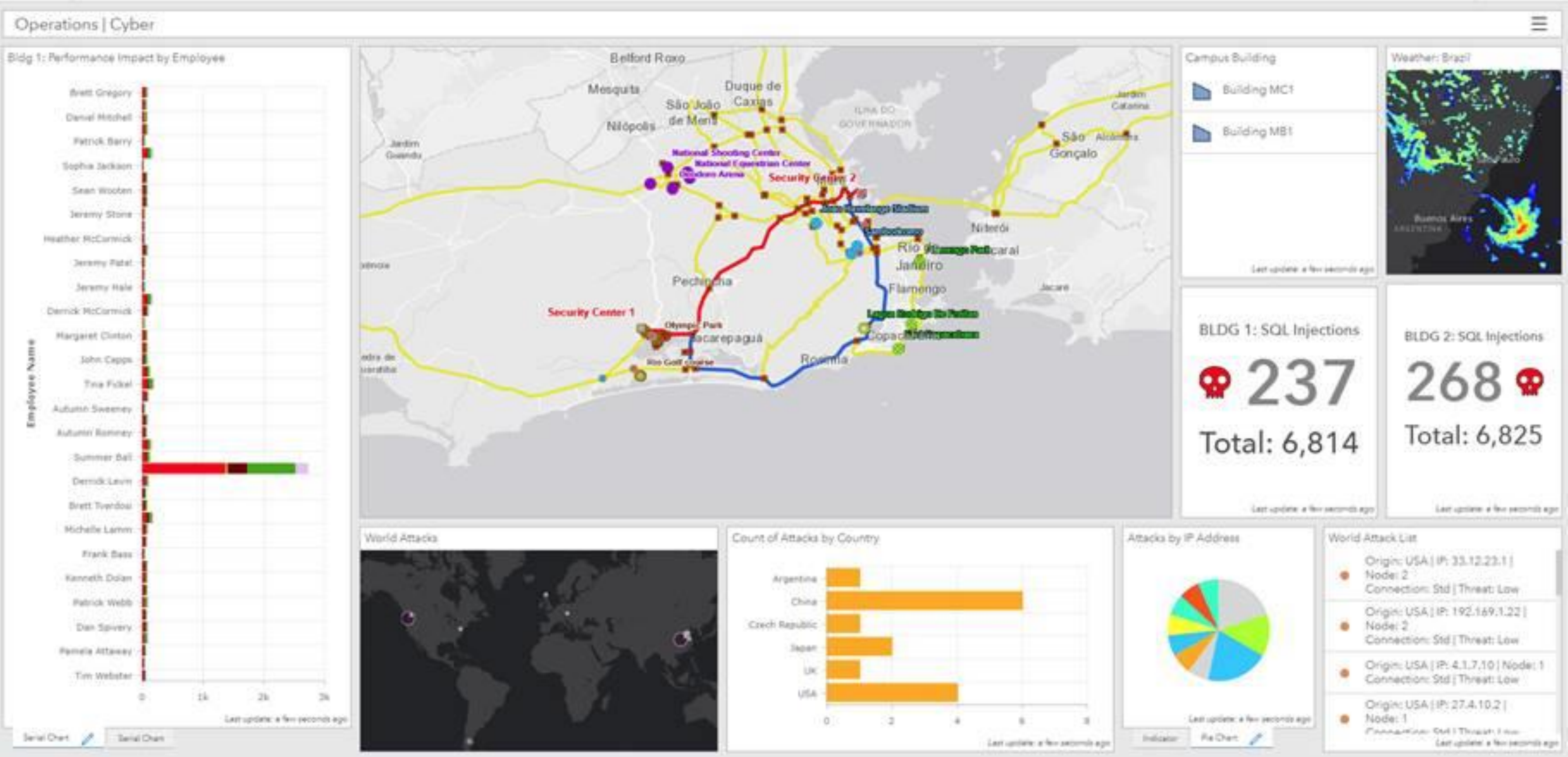
Facilities

Facilities Data -
CAD & GIS of
Buildings and Campuses,
Electric, Water, HVAC, Facilities
Monitoring, Physical Security

Rio Olympics Demo

Ken Mitchell

Operations Dashboard for Cyber Security



Operations | Cyber

BLDG 1: SQL Injections

237

Total: 6,814

BLDG 2: SQL Injections

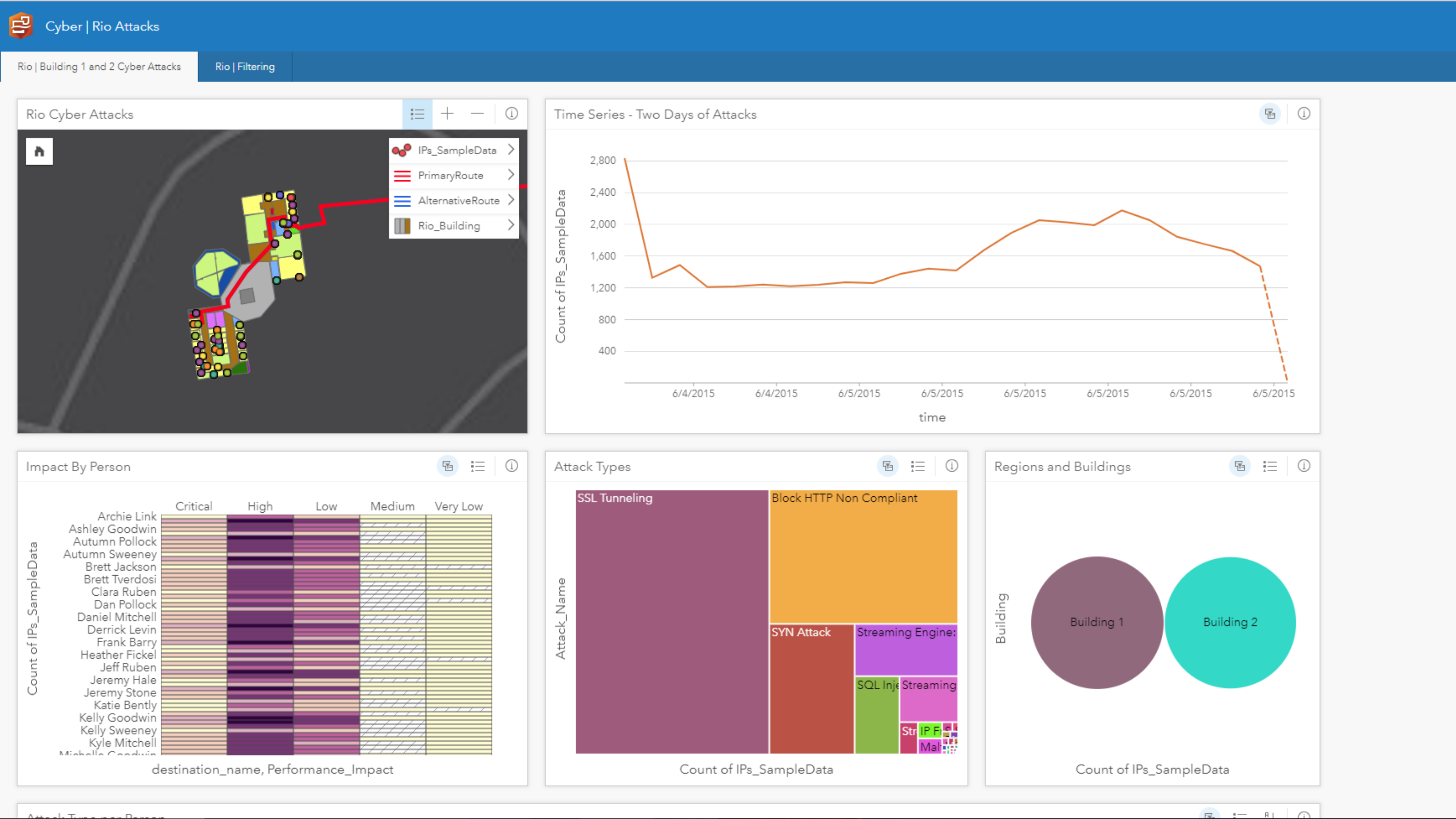
268

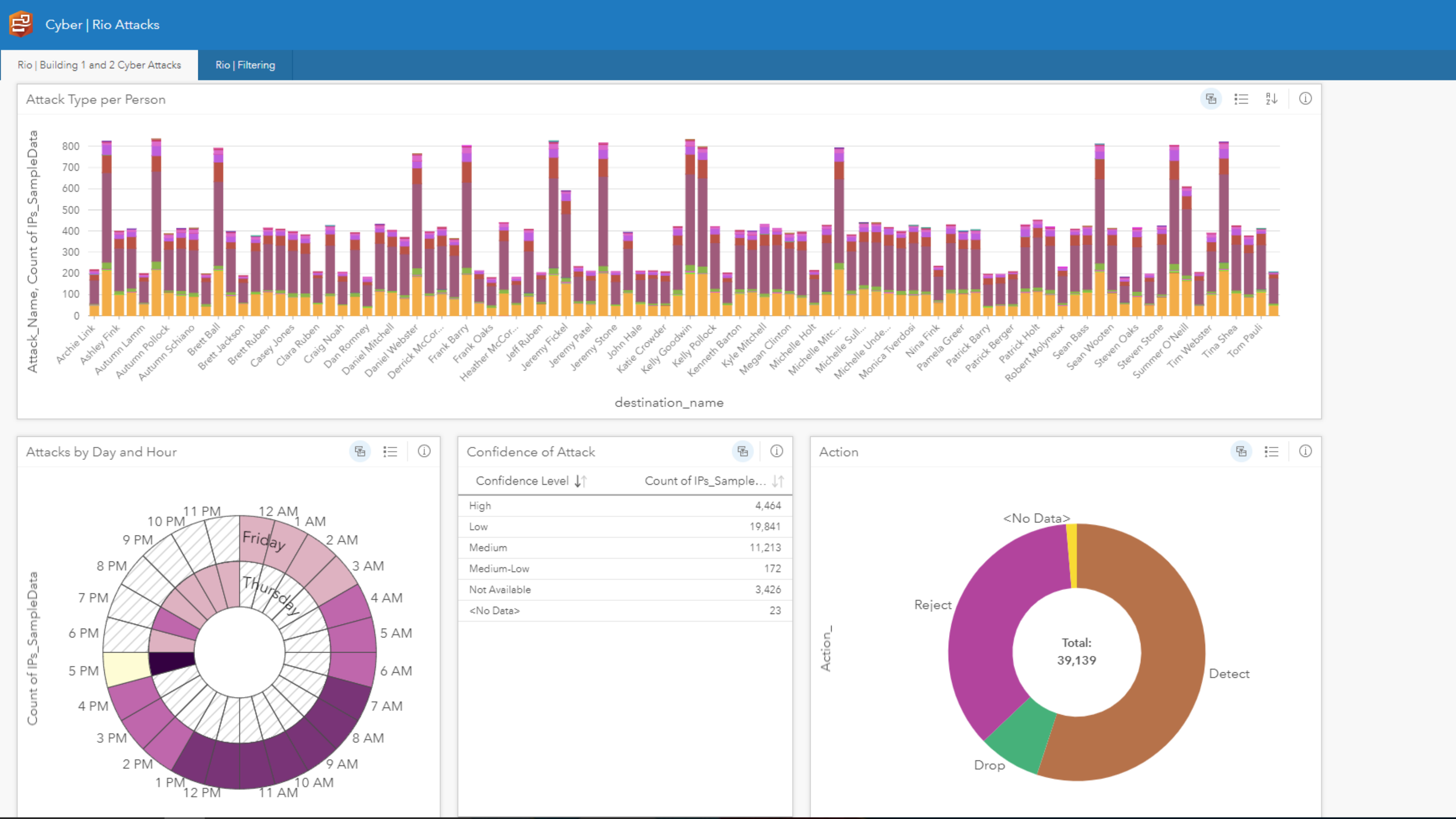
Total: 6,825

World Attack List

- Origin: USA | IP: 33.12.23.1 | Node: 2 Connection: Std | Threat: Low
- Origin: USA | IP: 192.169.1.22 | Node: 2 Connection: Std | Threat: Low
- Origin: USA | IP: 4.1.7.10 | Node: 1 Connection: Std | Threat: Low
- Origin: USA | IP: 27.4.10.2 | Node: 1 Connection: Std | Threat: Low

Last update: a few seconds ago


Cyber | Rio Attacks
Rio | Building 1 and 2 Cyber Attacks
Rio | Filtering
Rio Cyber Attacks
IPs_SampleData
PrimaryRoute
AlternativeRoute
Rio_Building
Time Series - Two Days of Attacks
2,800
2,400
2,000
1,600
1,200
800
400
Count of IPs_SampleData
6/4/2015
6/4/2015
6/5/2015
6/5/2015
6/5/2015
6/5/2015
6/5/2015
6/5/2015
time
Impact By Person
Critical
High
Low
Medium
Very Low
Archie Link
Ashley Goodwin
Autumn Pollock
Autumn Sweeney
Brett Jackson
Brett Tverdosi
Clara Ruben
Dan Pollock
Daniel Mitchell
Derrick Levin
Frank Barry
Heather Fickel
Jeff Ruben
Jeremy Hale
Jeremy Stone
Katie Bently
Kelly Goodwin
Kelly Sweeney
Kyle Mitchell
Michelle Goodwin
Count of IPs_SampleData
destination_name, Performance_Impact
Attack Types
SSL Tunneling
Block HTTP Non Compliant
SYN Attack
Streaming Engine:
SQL Inje
Streaming
Str
IP Fi
Mal
Attack_Name
Count of IPs_SampleData
Regions and Buildings
Building 1
Building 2
Building
Count of IPs_SampleData
Attack Type per Person



Cyber | Rio Attacks

Rio | Building 1 and 2 Cyber Attacks

Rio | Filtering

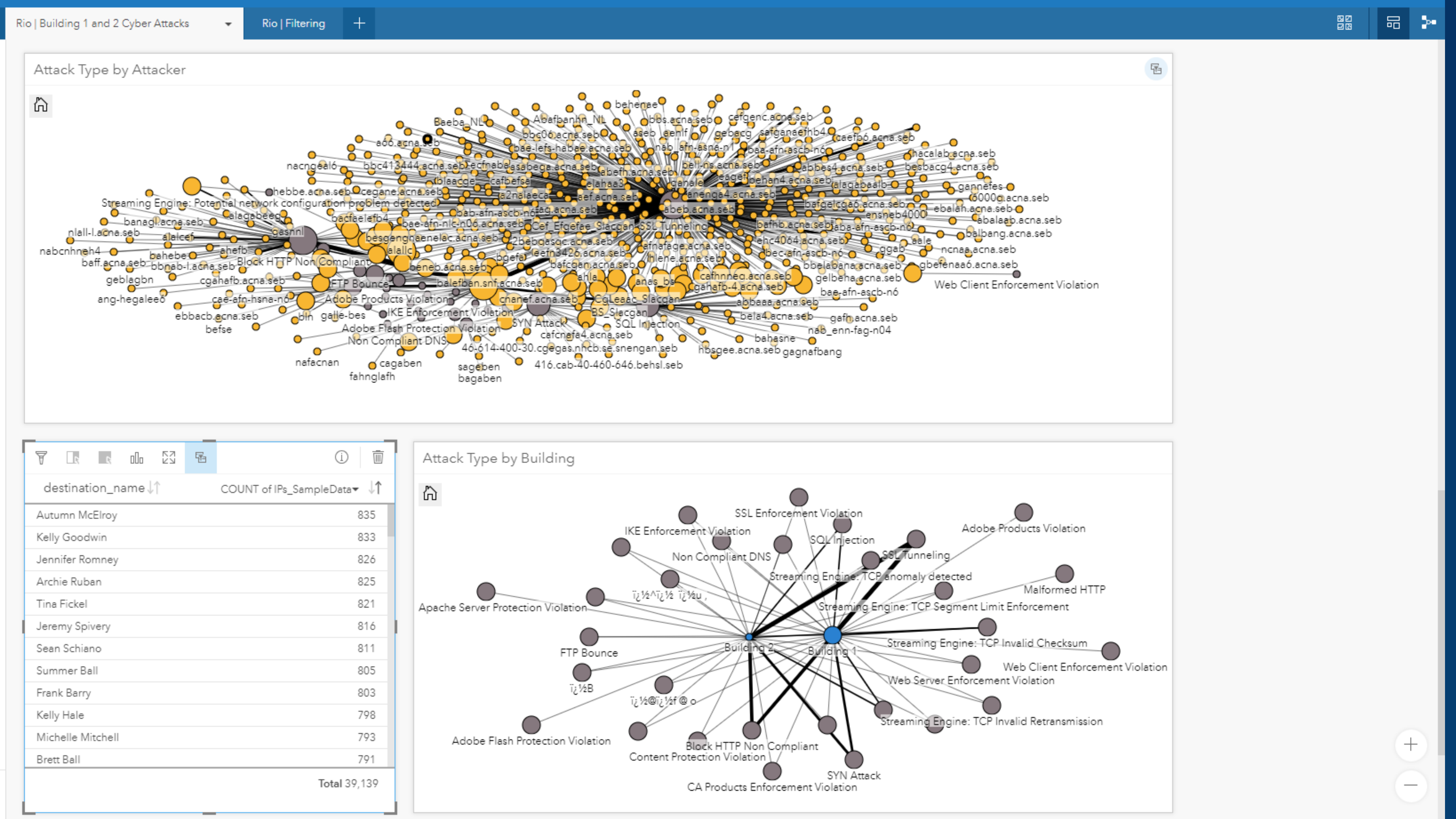
Attack Type per Person

Attacks by Day and Hour

Confidence of Attack

Confidence Level	Count of IPs_Sample...
High	4,464
Low	19,841
Medium	11,213
Medium-Low	172
Not Available	3,426
<No Data>	23

Action

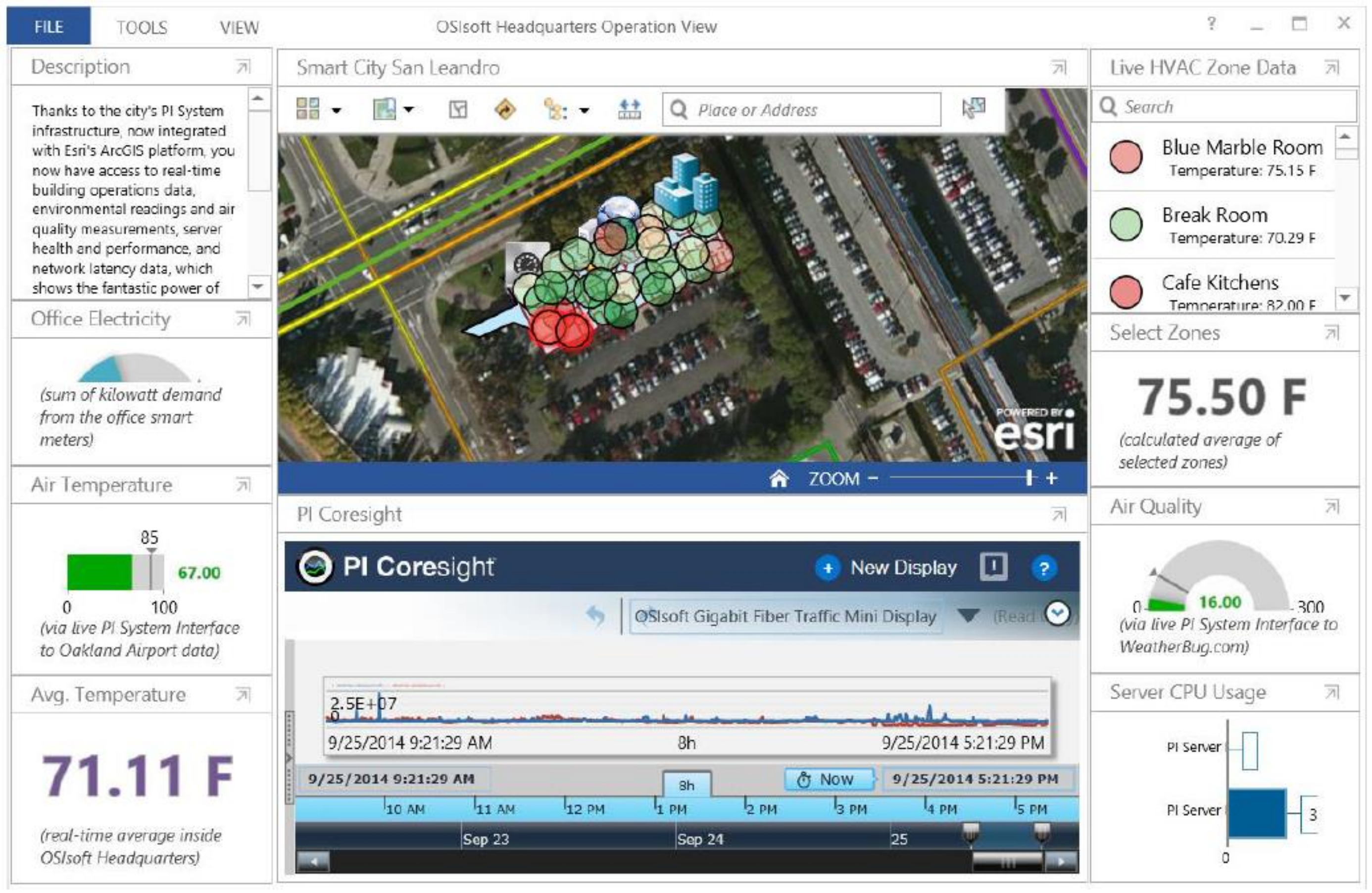


destination_name	COUNT of IPs_SampleData
Autumn McElroy	835
Kelly Goodwin	833
Jennifer Romney	826
Archie Ruban	825
Tina Fickel	821
Jeremy Spivery	816
Sean Schiano	811
Summer Ball	805
Frank Barry	803
Kelly Hale	798
Michelle Mitchell	793
Brett Ball	791

Total 39,139

Operations Dashboard integration with OSIsoft

Integrating data and information for situational awareness



OSIsoft Headquarters Operation View

Description

Thanks to the city's PI System infrastructure, now integrated with Esri's ArcGIS platform, you now have access to real-time building operations data, environmental readings and air quality measurements, server health and performance, and network latency data, which shows the fantastic power of

Office Electricity

(sum of kilowatt demand from the office smart meters)

Air Temperature

67.00

(via live PI System Interface to Oakland Airport data)

Avg. Temperature

71.11 F

(real-time average inside OSIsoft Headquarters)

Smart City San Leandro

PI Coresight

OSIsoft Gigabit Fiber Traffic Mini Display

Live HVAC Zone Data

Blue Marble Room
Temperature: 75.15 F

Break Room
Temperature: 70.29 F

Cafe Kitchens
Temperature: 82.00 F

Select Zones

75.50 F

(calculated average of selected zones)

Air Quality

16.00

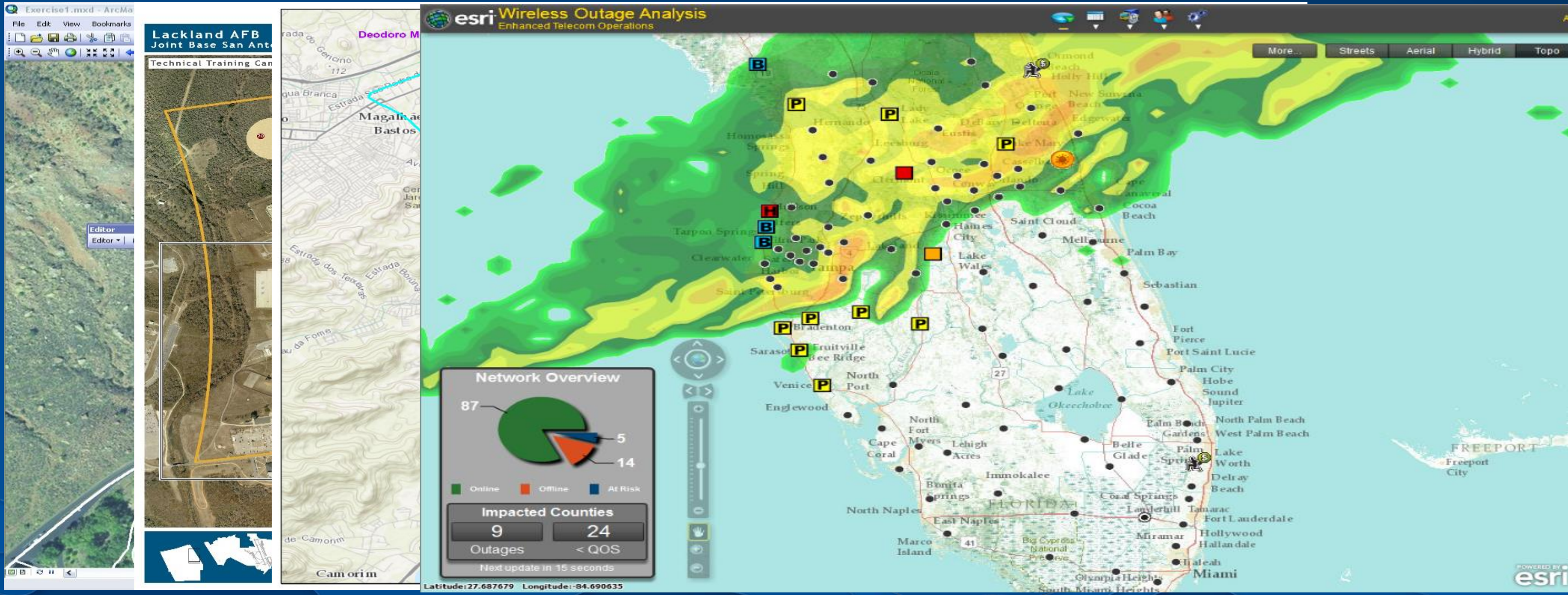
(via live PI System Interface to WeatherBug.com)

Server CPU Usage

Data Linkages

Missions / Operations	to	Critical Systems / Infrastructure
Critical Systems	to	Components
Components	to	Their location
Components	to	Their logical network connection
Logical Network	to	Physical Network
Logical / Physical Network	to	Network Devices
Cyber Threats	to	Components
IT Health and Status	to	Components
Impacted Components	to	Impacted Mission

Cyber Summary



Network Overview

87 · 5 · 14

🟩 Online 🟥 Offline 🟦 At Risk

Impacted Counties

9	24
Outages	< QOS

Next update in 15 seconds

esri

THE
SCIENCE
OF
WHERE

Contact Information

Brian Biesecker

bbiesecker@esri.com

Technical Director IC

Esri

Thank You

OSIsoft®