Possibilities

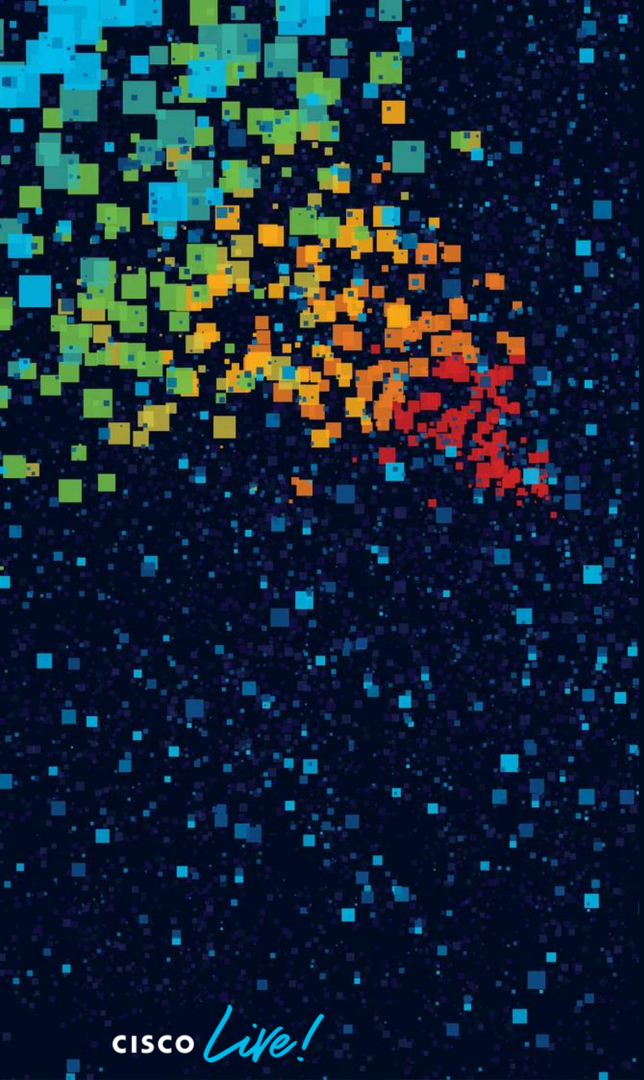
#CiscoLive

Water Cybersecurity: A Critical Foundation

Sielen Namdar, PE – Global Water Lead, Cisco
Rocky Smith – Global Lead Architect, Cisco
Adi Karisik – Global Technology Lead, Jacobs

DGTL-PSOIND-1011

June 2-3, 2020 | ciscolive.com/us



Agenda

- Industry Trends and Regulations
- IT/OT Cybersecurity
- Case Studies
- Cybersecurity in Water
- Resources

Industry Trends and Regulations

Why now? The water landscape is changing

$114B

To get clean water and working toilets to everyone on the planet by 2030

30%

Potable water lost to leakage and theft

$40B

Annual cost of flood damage worldwide

40%

Gap in freshwater needed to support the global economy by 2030

21%

US SCADA systems that can support remote operations

The value of smart water

SCADA systems

- Extend asset life
- Improve efficiencies
- Increase security

Quality monitoring

- Assure ecosystem/ public health
- Identify risk zones
- Automate systems

Asset management

- Automate systems
- Proactive maintenance
- Extend asset life

Equitable access and continuity

- Right to water
- Right to sanitation

Energy optimization

- Prioritize infrastructure spending
- Increase capacity without overextending resources

Water leak & theft detection

- Conserve water
- More efficient billing
- Improve response times

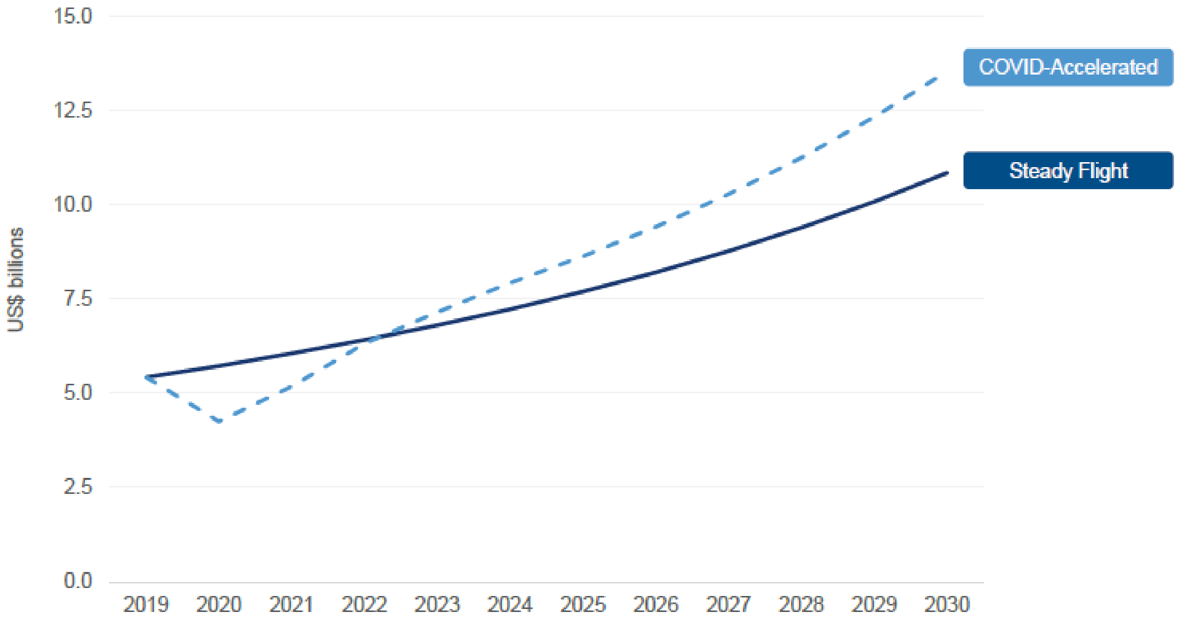
Emergency response

- Improve response times
- Proactively identify risk zones
- Protect public health and safety
- Remote operations

System security

- Secure critical infrastructure
- Understand & establish risk management framework
- Build resiliency

Smart water growth (North America)



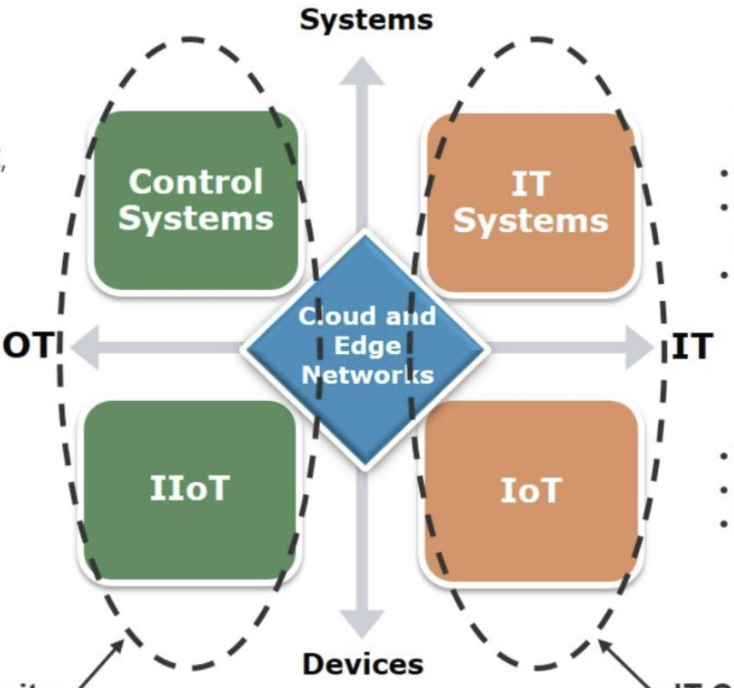
Source: Bluefield Research

America's Water Infrastructure Act (2018)

Population Served	Risk Assessment	Emergency Response Plan
>100K	March 31, 2020	September 30, 2020
50-100K	December 31, 2020	June 30, 2021
<50K	June 30, 2021	December 30, 2021

IT/OT Cybersecurity

IT/OT integrated cybersecurity approach



Manage Physical Processes

- Industrial Controllers (PLC, DCS, SCADA) & I/O
- Hardened PCs & Servers
- Industrial Networks

- Sensors (Temp, Pres, etc.)
- Cameras, Scanners, etc.
- Embedded Systems (Robots, Analyzers, etc.)

OT Cybersecurity

Manage Information

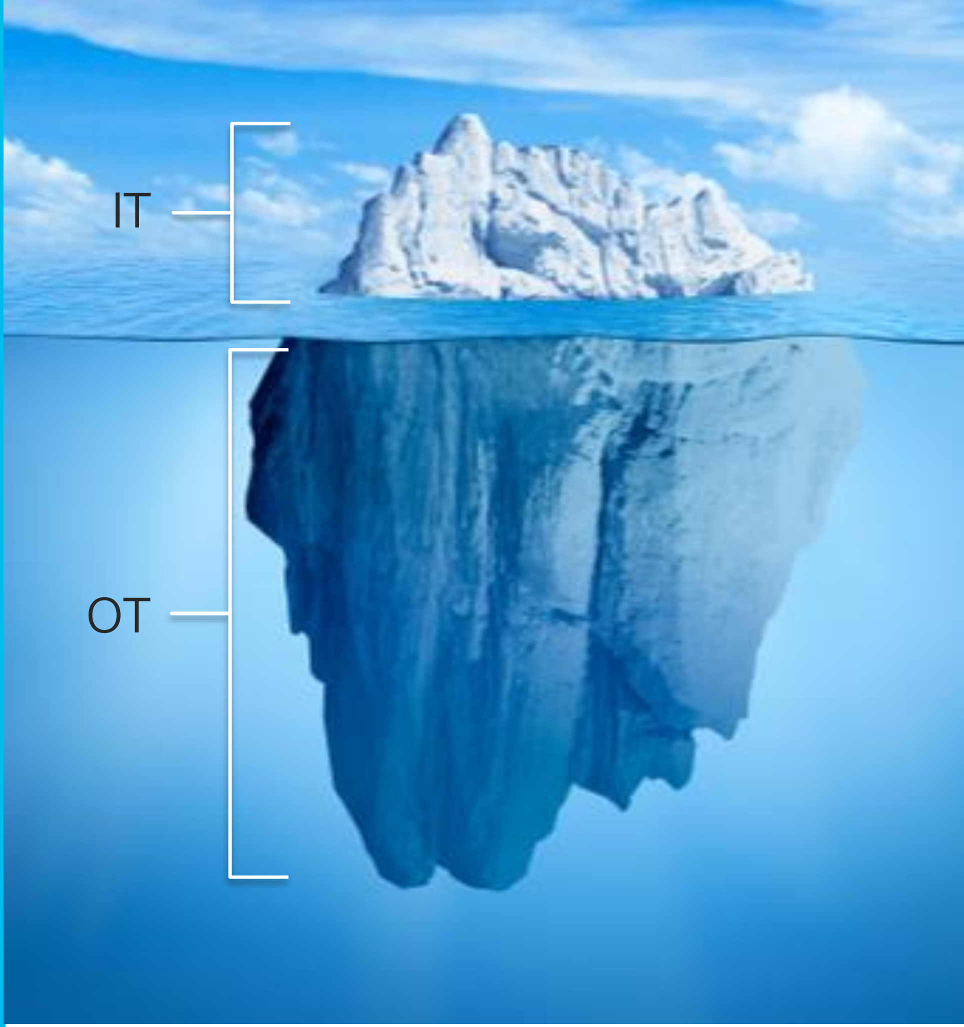
- Office PCs, Printers
- Web/App/Data/Email Servers
- TCP Networks

- Tablets
- Smart Phones
- Etc.

IT Cybersecurity

Attack surface

- Ability to control physical devices remotely
- Addition of IT-style services
  - Big data
  - Machine learning
  - M2M communication
  - Sensors (IoT/IIoT)
  - Remote Diagnostics
  - Predictive maintenance
  - Digital Twin
- Traditionally older systems
- Large attack surface



Case Studies

Super Bowl 2020, North Miami Beach

Jacobs cisco

SUPER BOWL LIV
MIAMI
EARLY ACCESS
LOOK INSIDE WITH SCOTT HANSON
G-EAZY
TBD GUEST
INSIDE THE LOCKER ROOM WITH SCOTT HANSON
13
DOLPHINS

Oklahoma City Water Utilities Trust

Customer story

Utility Operations and Management
Oklahoma City, Oklahoma

Oklahoma City Water retained Jacobs to increase resiliency and cybersecurity of the SCADA system according to their SCADA Masterplan. Jacobs partnered with Cisco on the cybersecurity solution.

Challenge

Vulnerability assessment highlighted multiple cyber risks, aged infrastructure, no forward-looking OT plan

Solution

- Enterprise-wide Secure SCADA Architecture (WAN, LAN, Systems, DMZ)
- Reviewed architecture and performed verification/validation
- Features: cybersecurity policies and procedures, ICS Security Awareness Training, Multi-Factor Authentication

Impact

- Secure and resilient enterprise-wide SCADA system
- Redundant architecture with multiple datacenters and EOC
- Increased system awareness and better access to data for management
- IT/OT convergence with SLA's and improved communications

Rio Rancho Water Utility

Customer story

Utility Operations and Management
City of Rio Rancho, New Mexico

Jacobs partnered with Cisco to improve network and cybersecurity posture of Rio Rancho's SCADA system based on their SCADA Masterplan.

Challenge

Utility-wide infrastructure deficiencies contributed to poor cybersecurity posture, unsecure communications network, and lack of commercial grade server and network infrastructure

Solution

- Comprehensive cybersecurity and network improvements
- Encrypted communications and network implementation
- 3rd party vulnerability assessment at the conclusion of the project

Impact

- Greatly improved the cybersecurity posture
- Continuous improvements to keep up with cybersecurity threats
- Secure communications network

Roseville Water Utility

Environmental Utilities
City of Roseville, California

Jacobs collaborated with Roseville Water to improve their SCADA system cybersecurity posture.

Jacobs

cisco Live!

Customer story

Challenge

Aging water and wastewater SCADA infrastructure facilities, increased cybersecurity risk

Solution

- Detailed defense design and cybersecurity improvements
- US Department of Homeland Security (DHS) Design Architecture Review
- Close collaboration on integration and testing
- DHS network architecture verification and validation

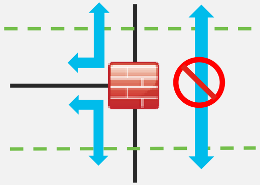
Impact

- Commendation from DHS on design and network security performance
- Continuous cybersecurity improvements and heightened cybersecurity awareness
- ICS cybersecurity program improvements

Cybersecurity in Water

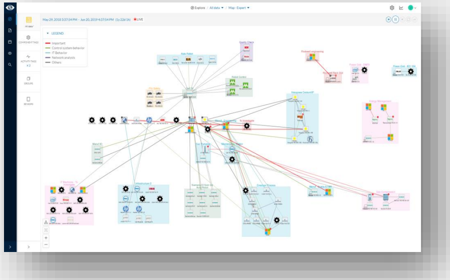
Cisco cybersecurity for water

Architectural Approach



Architectures built for industry requirements with security as a foundational element

Operational Asset Visibility



Asset visibility updated in real-time to assist in both secure design and threat response in addition to providing operational insight

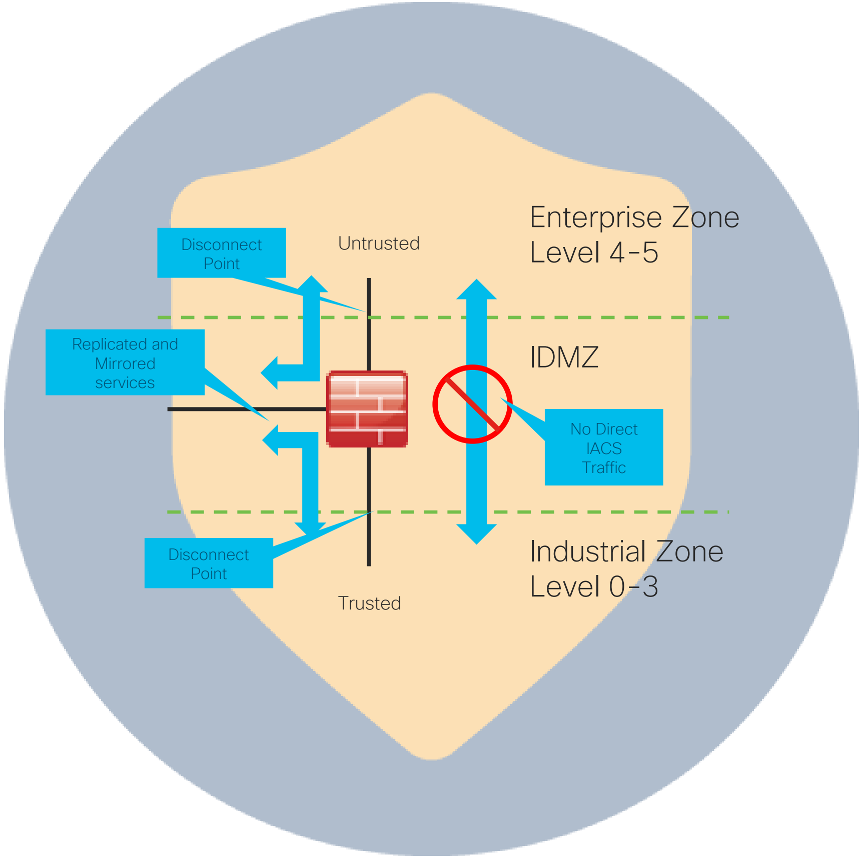
Industry Focus

Applying secure solutions to meet the specific challenges of the water industry

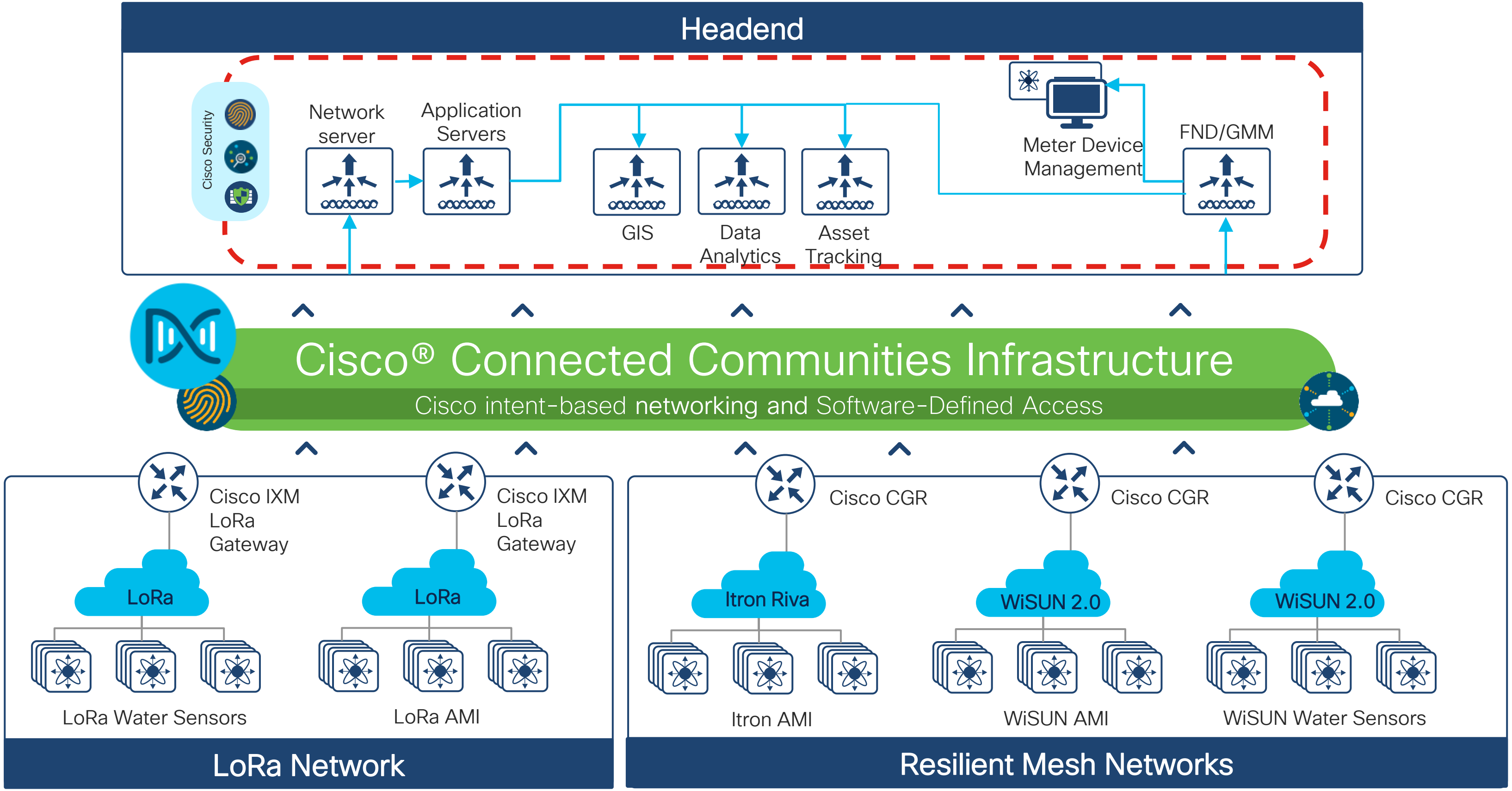
Cisco Industrial Cybersecurity

Cybersecurity in Water

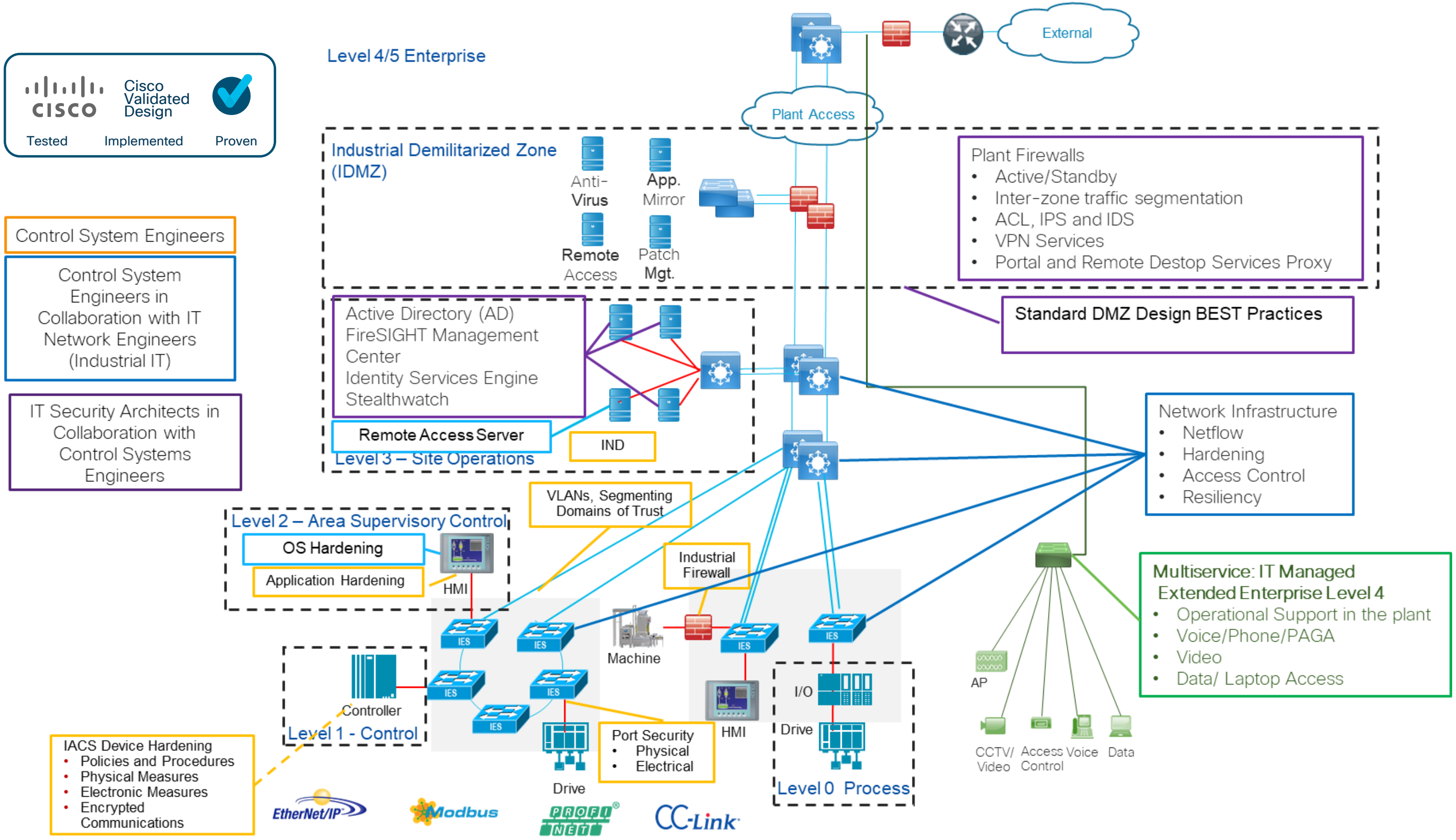
Architectural Approach


Disconnect Point
Untrusted
Enterprise Zone Level 4-5
Replicated and Mirrored services
IDMZ
No Direct IACS Traffic
Disconnect Point
Trusted
Industrial Zone Level 0-3

Distributed secondary water networks



Water SCADA modernization – defense in depth



Cisco Validated Design

Tested Implemented Proven

Control System Engineers

Control System Engineers in Collaboration with IT Network Engineers (Industrial IT)

IT Security Architects in Collaboration with Control Systems Engineers

Plant Firewalls
- Active/Standby
- Inter-zone traffic segmentation
- ACL, IPS and IDS
- VPN Services
- Portal and Remote Destop Services Proxy

Standard DMZ Design BEST Practices

Active Directory (AD)
FireSIGHT Management Center
Identity Services Engine
Stealthwatch

Remote Access Server

IND

Network Infrastructure
- Netflow
- Hardening
- Access Control
- Resiliency

VLANs, Segmenting Domains of Trust

OS Hardening

Application Hardening

Industrial Firewall

Multiservice: IT Managed Extended Enterprise Level 4
- Operational Support in the plant
- Voice/Phone/PAGA
- Video
- Data/ Laptop Access

Port Security
- Physical
- Electrical

IACS Device Hardening
- Policies and Procedures
- Physical Measures
- Electronic Measures
- Encrypted Communications

Cybersecurity in Water

cisco Live!

Operational Asset Visibility

You cannot secure what you don’t know

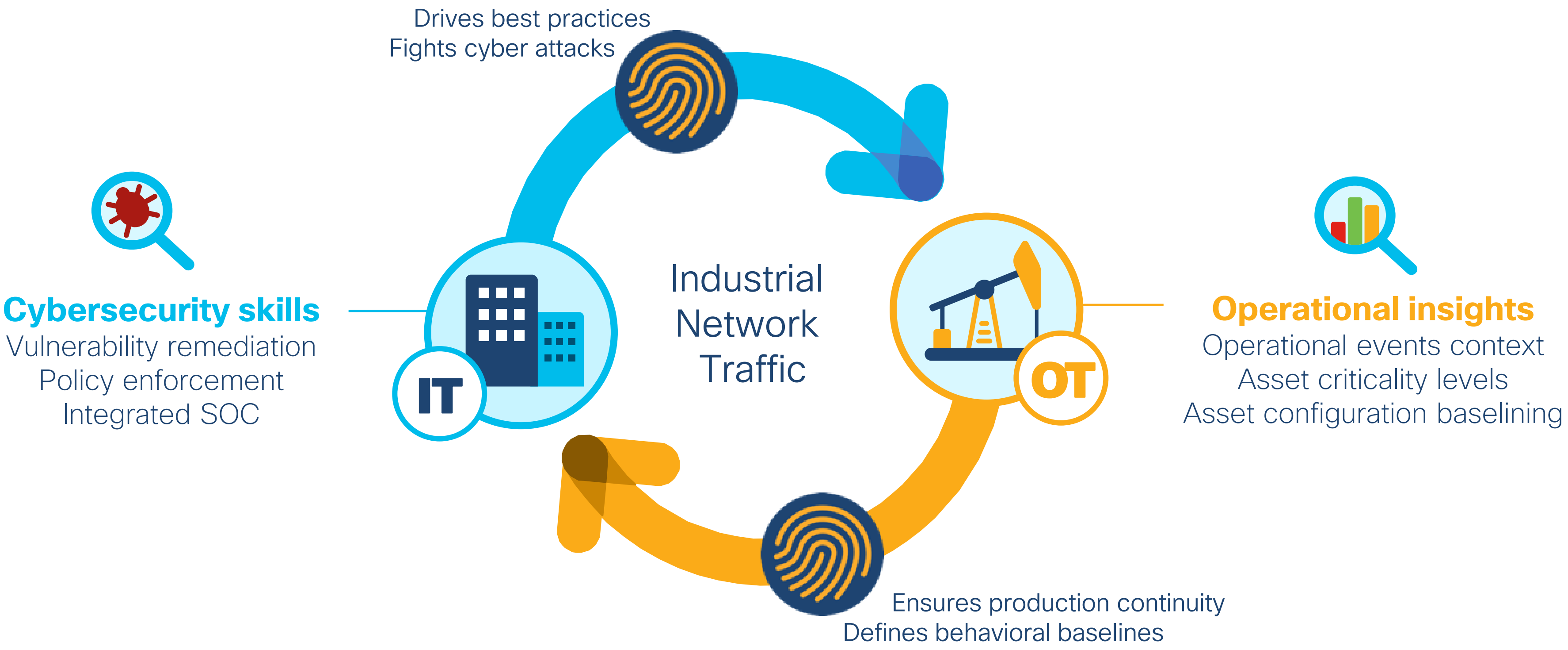
Most customers don’t have accurate asset inventory

55% have no or low confidence that they know all devices in their network

Blind to what their assets are communicating with

ICS equipment deployed over the years without strict security policies

Cyber Vision **IT-OT Collaboration**

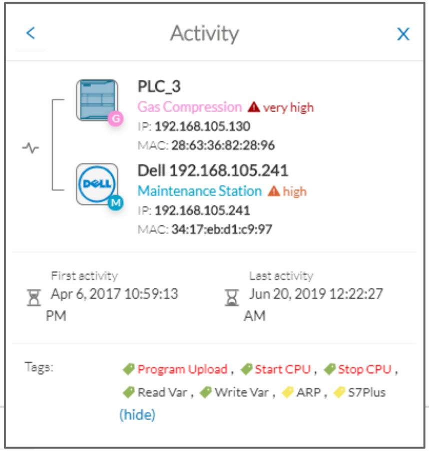

Drives best practices
Fights cyber attacks
IT
Industrial Network Traffic
OT
Ensures production continuity
Defines behavioral baselines

Cybersecurity skills
Vulnerability remediation
Policy enforcement
Integrated SOC

Operational insights
Operational events context
Asset criticality levels
Asset configuration baselining

Cyber Vision **Operational Insights**

- Passive asset and communication discovery
- Asset tags and groups
  - Process-based views
  - Prioritize maintenance
- Baselines and deviations
- Vulnerabilities



Activity

PLC_3
Gas Compression very high
IP: 192.168.105.130
MAC: 28:63:36:82:28:96

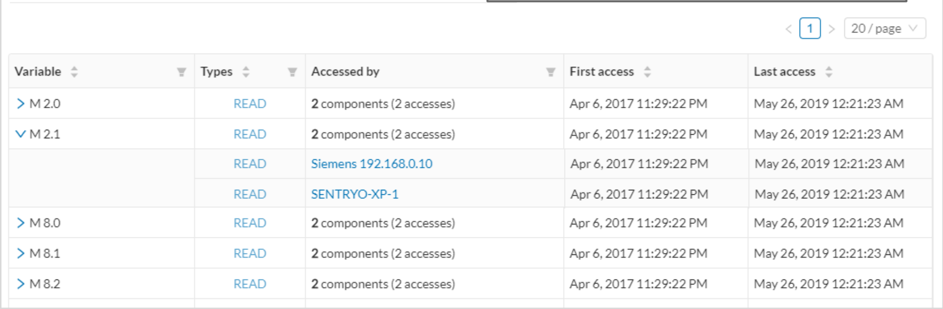
Dell 192.168.105.241
Maintenance Station high
IP: 192.168.105.241
MAC: 34:17:eb:d1:c9:97

First activity
Apr 6, 2017 10:59:13 PM

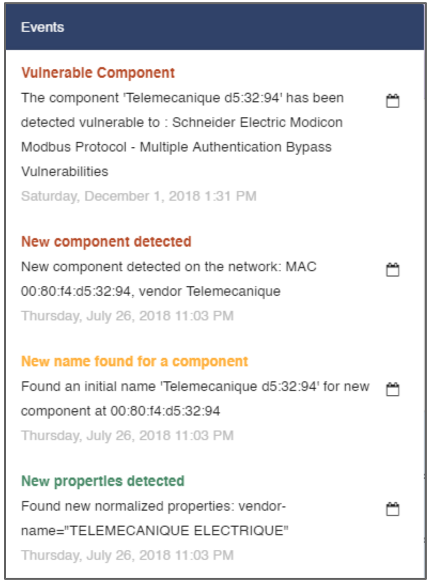
Last activity
Jun 20, 2019 12:22:27 AM

Tags: Program Upload , Start CPU , Stop CPU , Read Var , Write Var , ARP , S7Plus
(hide)

Variables accesses



Variable	Types	Accessed by	First access	Last access
> M 2.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
∨ M 2.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
	READ	Siemens 192.168.0.10	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
	READ	SENTRYO-XP-1	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M 8.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M 8.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M 8.2	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM



Events

Vulnerable Component
The component 'Telemecanique d5:32:94' has been detected vulnerable to : Schneider Electric Modicon Modbus Protocol - Multiple Authentication Bypass Vulnerabilities
Saturday, December 1, 2018 1:31 PM

New component detected
New component detected on the network: MAC 00:80:f4:d5:32:94, vendor Telemecanique
Thursday, July 26, 2018 11:03 PM

New name found for a component
Found an initial name 'Telemecanique d5:32:94' for new component at 00:80:f4:d5:32:94
Thursday, July 26, 2018 11:03 PM

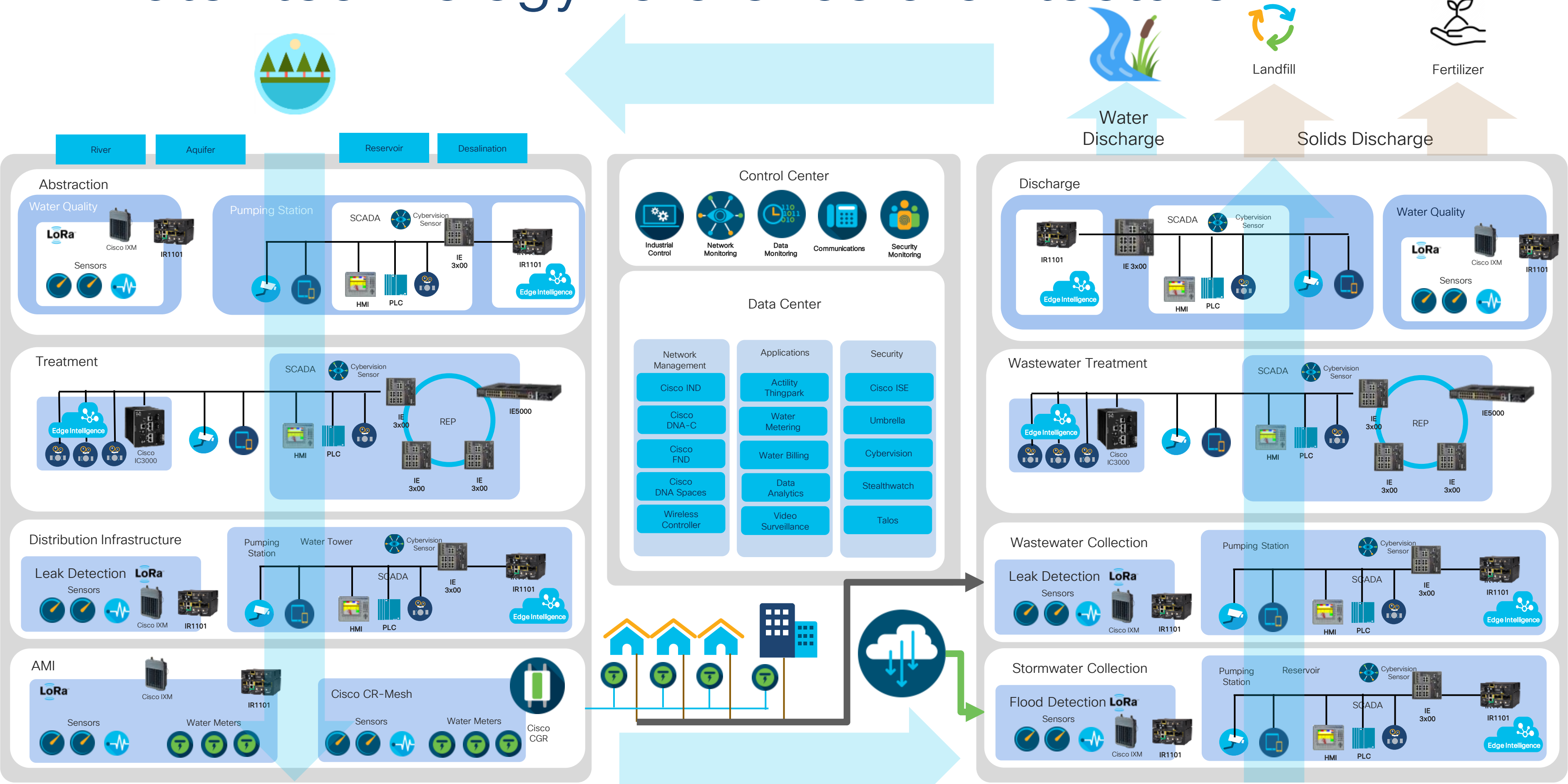
New properties detected
Found new normalized properties: vendor-name="TELEMECANIQUE ELECTRIQUE"
Thursday, July 26, 2018 11:03 PM

Cybersecurity in Water

Industry Focus

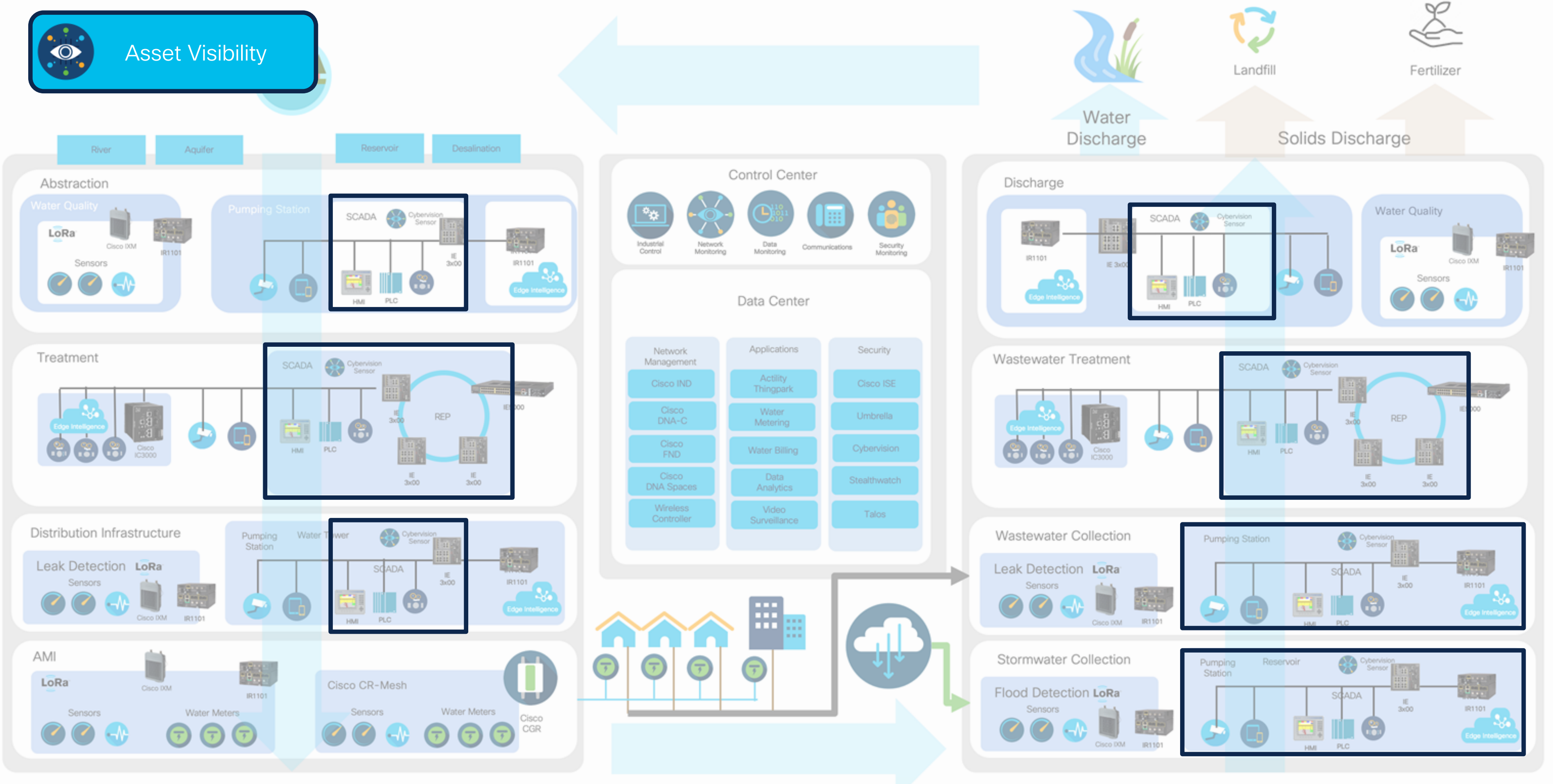
cisco Live!

Water technology reference architecture

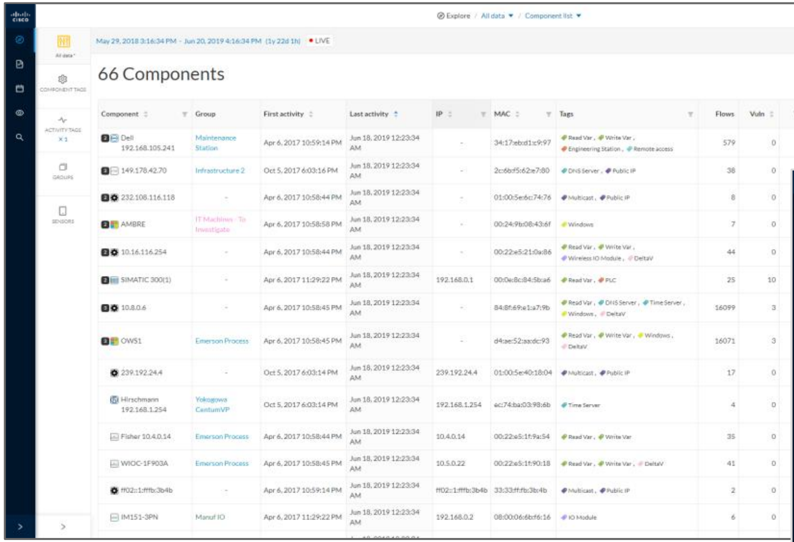


Water technology reference architecture

Asset Visibility



Cisco Cyber Vision **Asset Visibility**

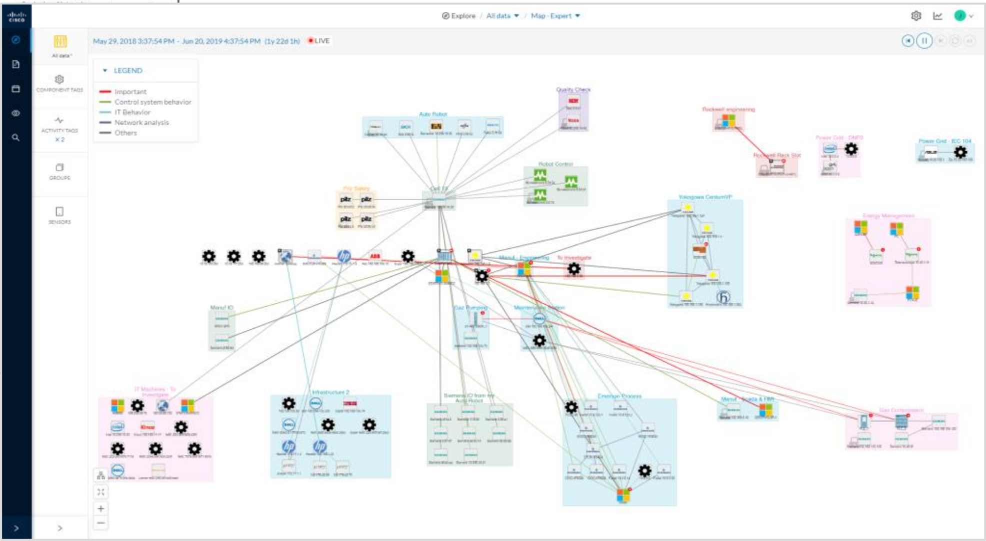

Explore / All data ▾ / Component list ▾
May 29, 2018 3:16:34 PM - Jun 20, 2019 4:16:34 PM (1y 22d 1h) ● LIVE
All data*
COMPONENT TAGS
ACTIVITY TAGS
× 1
GROUPS
SENSORS
< 1 2 3 4 > 20 / page

66 Components

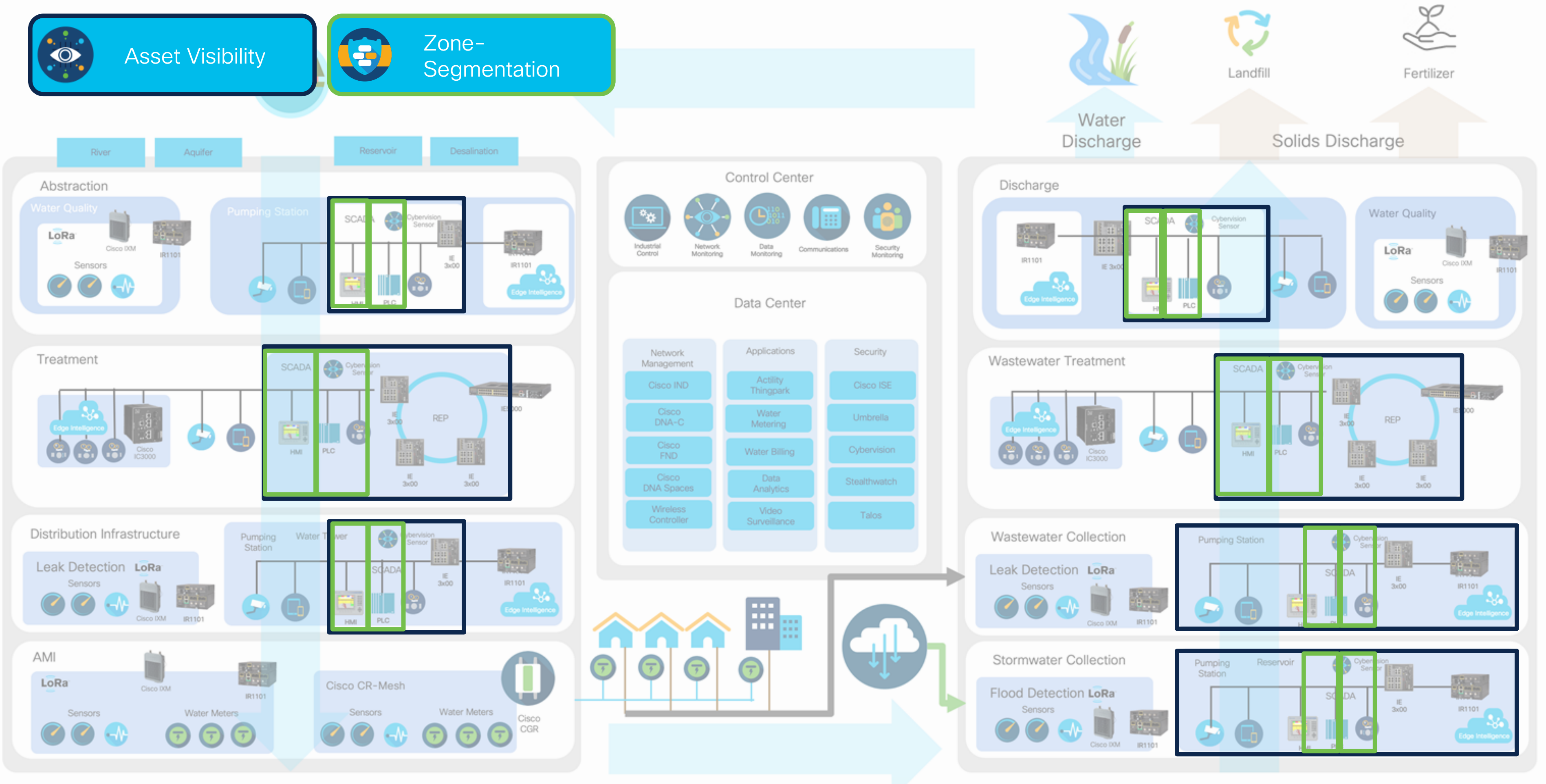
Component	Group	First activity	Last activity	IP	MAC	Tags	Flows	Vuln	Var	Vendor	OS
Dell 192.168.105.241	Maintenance Station	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	-	34:17:eb:d1:c9:97	Read Var , Write Var , Engineering Station , Remote access	579	0	0	Dell Inc.	-
149.178.42.70	Infrastructure 2	Oct 5, 2017 6:03:16 PM	Jun 18, 2019 12:23:34 AM	-	2c:6b:f5:62:e7:80	DNS Server , Public IP	38	0			
232.108.116.118	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	01:00:5e:6c:74:76	Multicast , Public IP	8	0			
AMBRE	IT Machines - To Investigate	Apr 6, 2017 10:58:58 PM	Jun 18, 2019 12:23:34 AM	-	00:24:9b:08:43:6f	Windows	7	0			
10.16.116.254	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	00:22:e5:21:0a:86	Read Var , Write Var , Wireless IO Module , DeltaV	44	0			
SIMATIC 300(1)	-	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.1	00:0e:8c:84:5b:a6	Read Var , PLC	25	10			
10.8.0.6	-	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	84:8f:69:e1:a7:9b	Read Var , DNS Server , Time Server , Windows , DeltaV	16099	3			
OWS1	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	d4:ae:52:aa:dc:93	Read Var , Write Var , Windows , DeltaV	16071	3			
239.192.24.4	-	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	239.192.24.4	01:00:5e:40:18:04	Multicast , Public IP	17	0			
Hirschmann 192.168.1.254	Yokogowa CentumVP	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	192.168.1.254	ec:74:ba:03:98:6b	Time Server	4	0			
Fisher 10.4.0.14	Emerson Process	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	10.4.0.14	00:22:e5:1f:9a:54	Read Var , Write Var	35	0			
WIOC-1F903A	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	10.5.0.22	00:22:e5:1f:90:18	Read Var , Write Var , DeltaV	41	0			
ff02::1:fffb:3b4b	-	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	ff02::1:fffb:3b4b	33:33:ff:fb:3b:4b	Multicast , Public IP	2	0			
IM151-3PN	Manuf IO	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.2	08:00:06:6b:f6:16	IO Module	6	0			

Comprehensive Asset Inventory

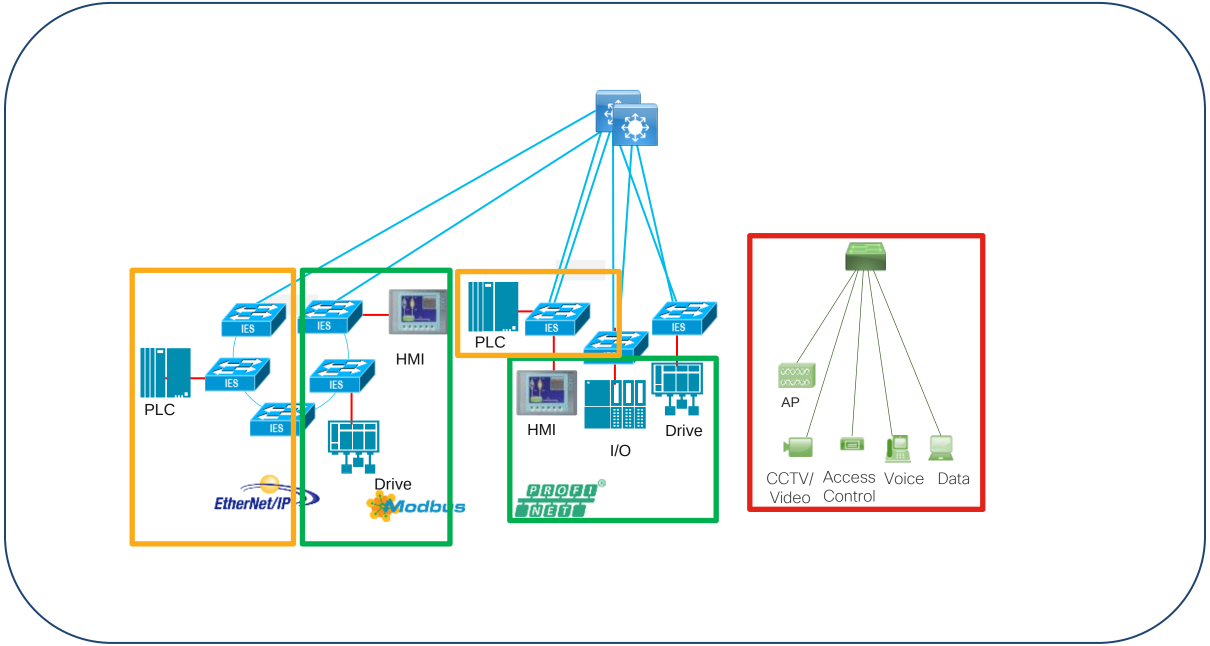
Dynamic Communication Map



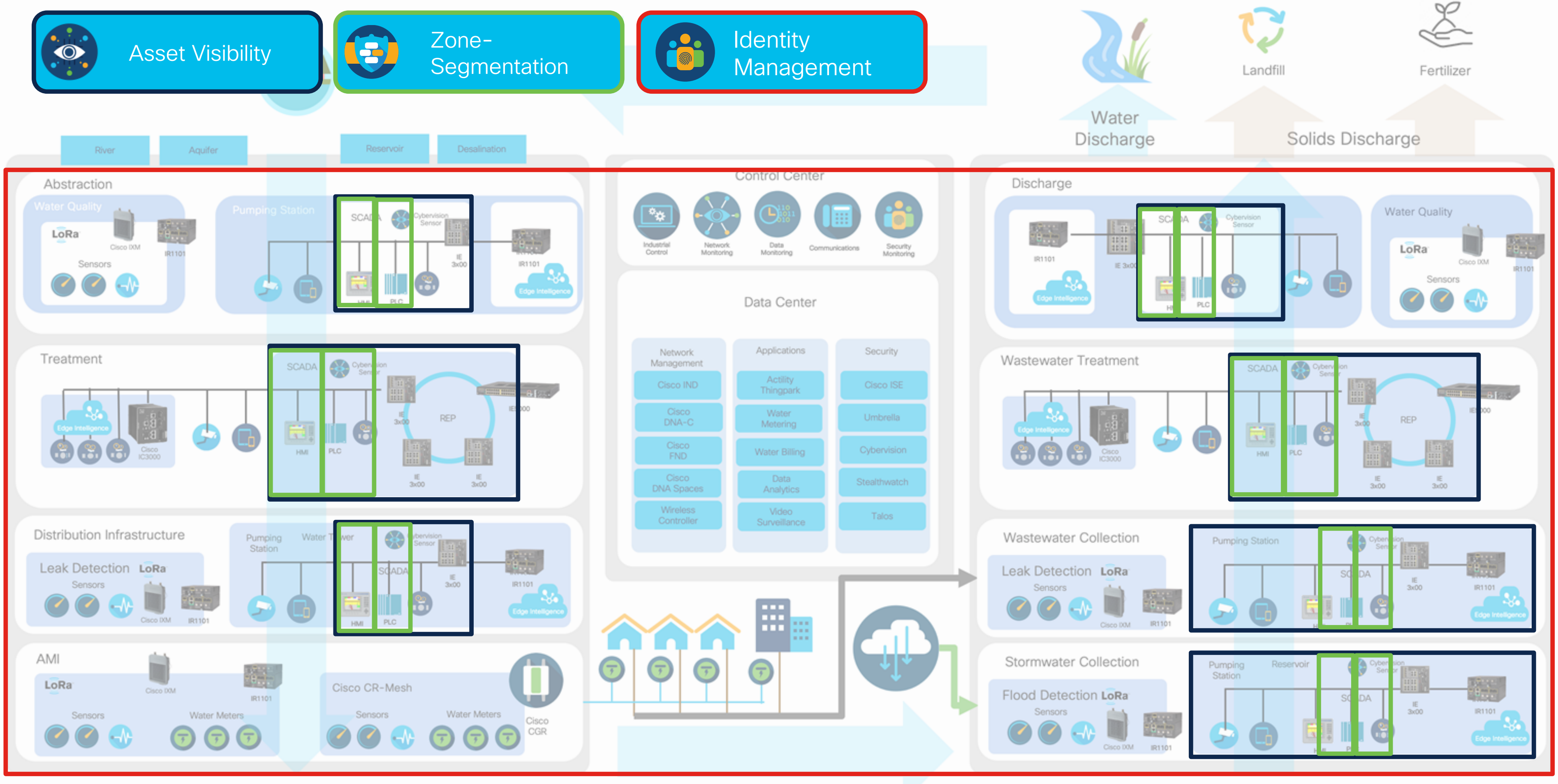
Water technology reference architecture



Cisco SDA – Network **Zone Segmentation**



Water technology reference architecture

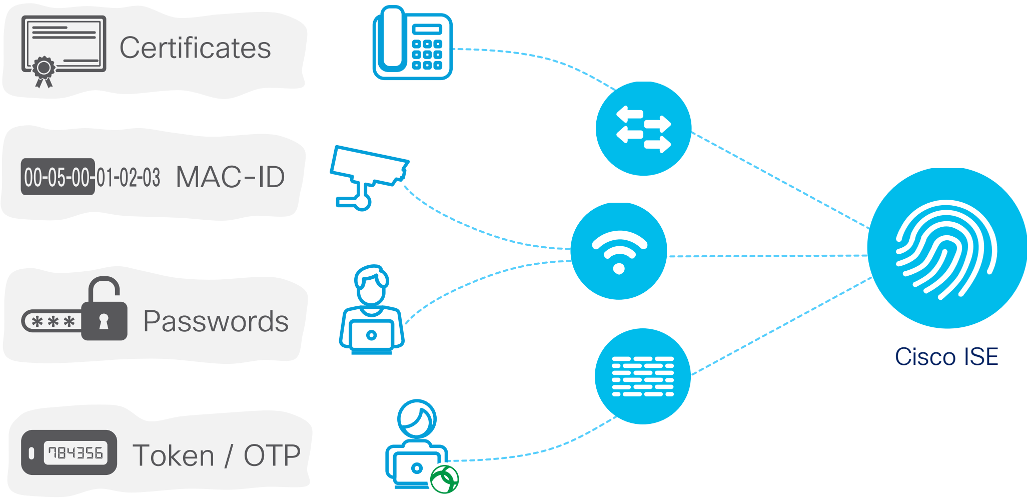


Asset Visibility

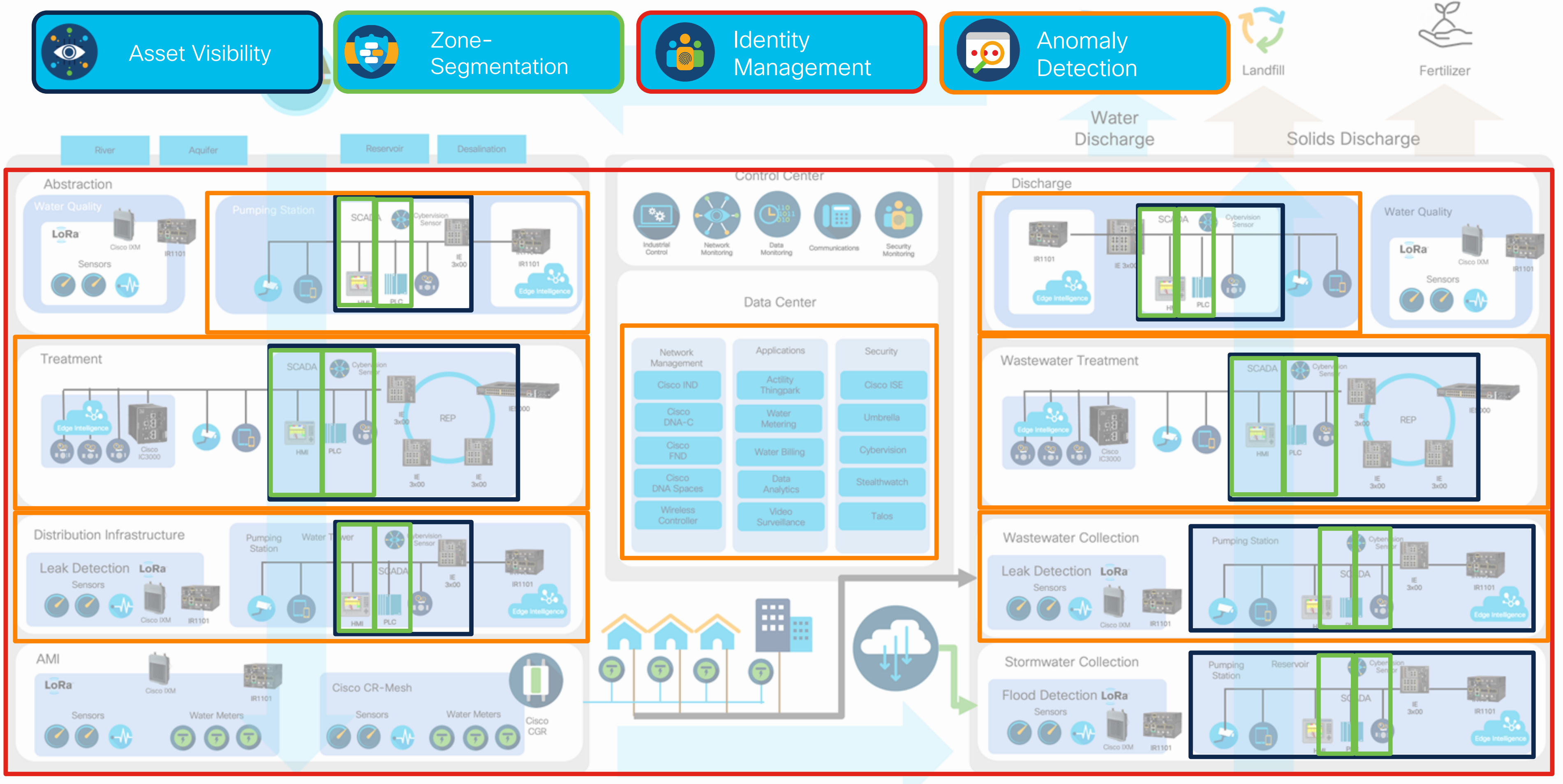
Zone-Segmentation

Identity Management

Cisco ISE **Identity Management**



Water technology reference architecture



Asset Visibility

Zone-Segmentation

Identity Management

Anomaly Detection

Cisco Stealthwatch **Anomaly Detection**

- Detect malicious behavior
- No endpoint agents
- Segmentation

Water technology reference architecture

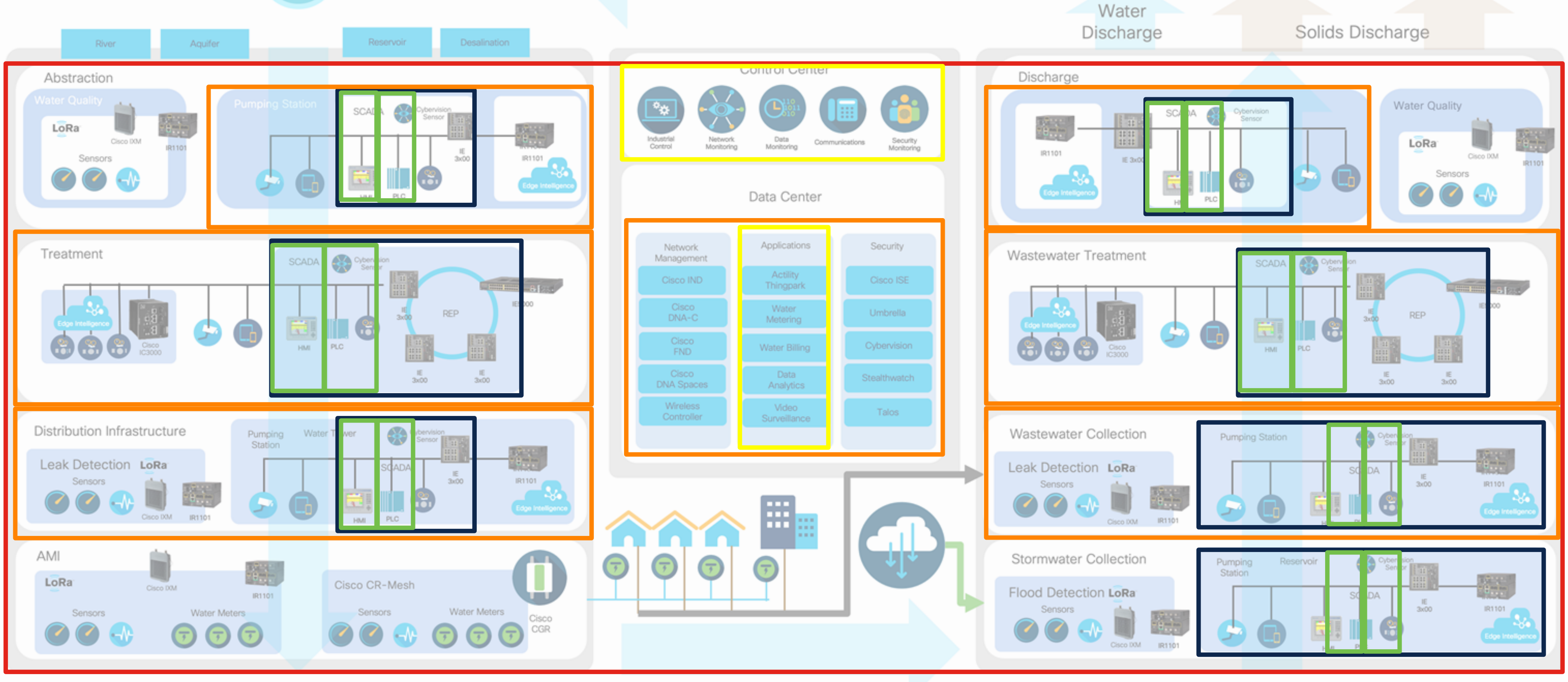
Asset Visibility

Zone-Segmentation

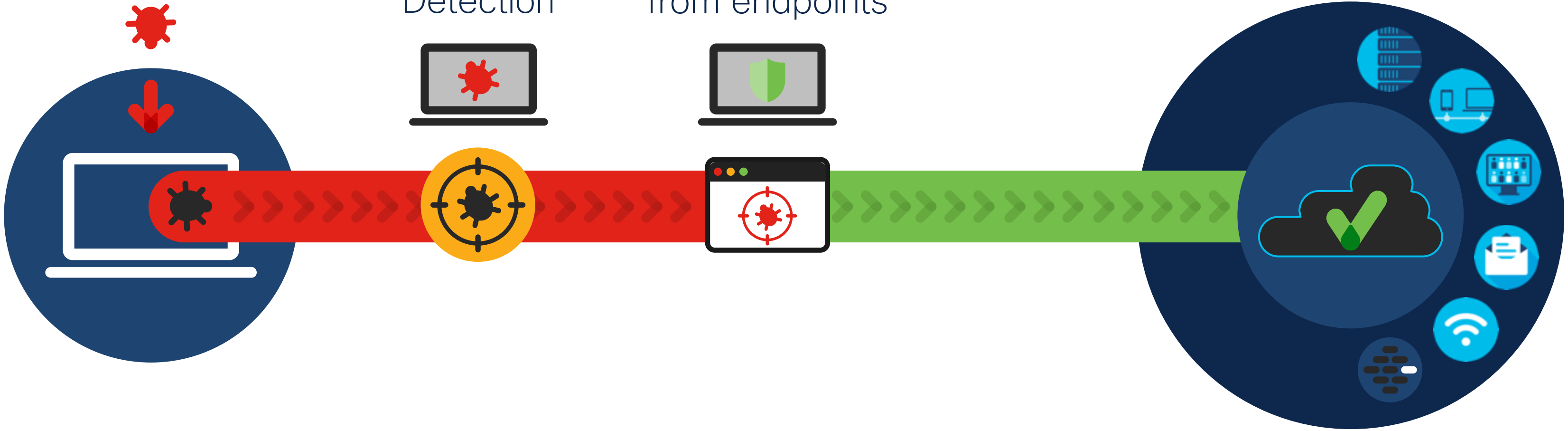
Identity Management

Anomaly Detection

Advanced Malware Protection



Cisco AMP - **Malware Protection**



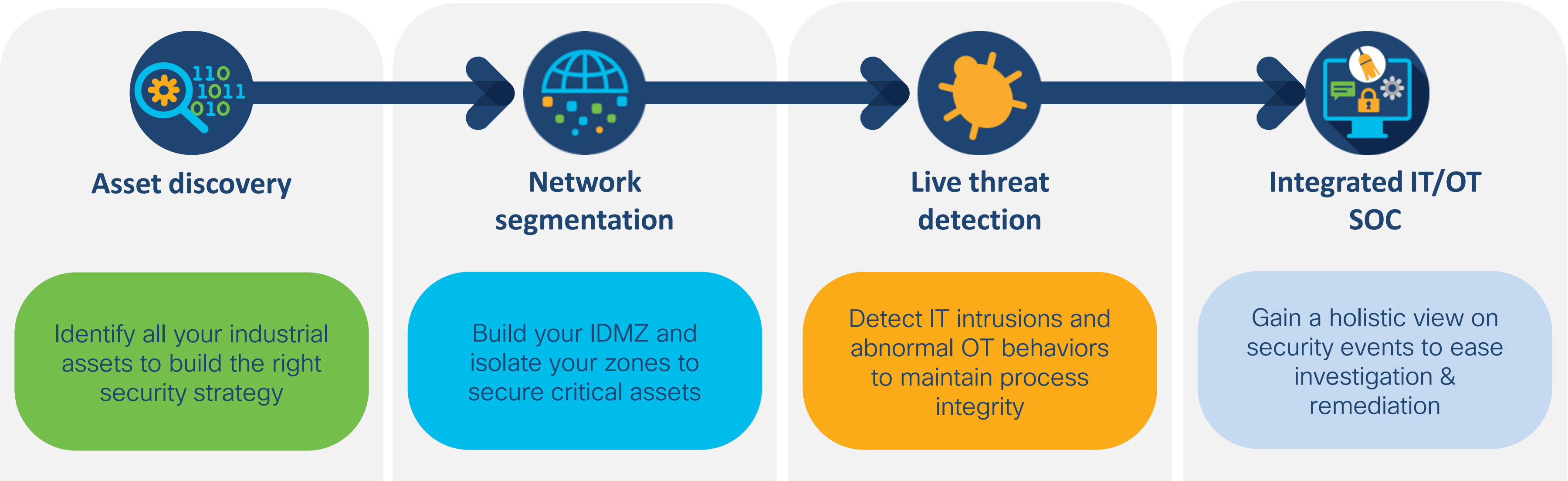
If malware gets in

Immediate Detection

Removed automatically from endpoints

Blocked across network, endpoints, email and cloud

The 4-step journey to secure water networks



Asset discovery

Identify all your industrial assets to build the right security strategy

Network segmentation

Build your IDMZ and isolate your zones to secure critical assets

Live threat detection

Detect IT intrusions and abnormal OT behaviors to maintain process integrity

Integrated IT/OT SOC

Gain a holistic view on security events to ease investigation & remediation

Gain visibility on your OT to build and enforce the right security policies

Resources

Cisco Cyber Vision

https://www.cisco.com/c/en/us/products/security/cyber-vision/index.html

Cisco Smart Water

cisco.com/go/smartwater

Jacobs Solutions

jacobs.com/capabilities

Connect with us

Sielen Namdar, PE, sienamda@cisco.com

Rocky Smith, rocsmith@cisco.com

Adi Karisik, Adi.Karisik@jacobs.com

Thank you

Possibilities

#CiscoLive