Protecting your Operations Against Cyber Attacks

SIAS Webinar Series

Brandon Witte, President Sightline Systems
Lance Vaughn, VP Global Security & Alliances

Powered by Sightline Systems
Secured by Unisys

UNISYS | Securing Your Tomorrow™

SIGHTLINE SYSTEMS

Protecting your Operations Against Cyber Attacks

OUR AGENDA

- Attack Profile – Florida Water Treatment
    - Overview of attack
    - Vulnerabilities leading to attack
    - Recommendations to prevent
- SIAS – How Unisys & Sightline can help
- Q&A

Making Data Smart
Securing Your Tomorrow

Oldsmar Water Treatment Facility Hack

Timeline: February 5, 2021. A currently unknown threat actor(s) took control of SCADA based water treatment systems on 2 separate occasions approximately 5 hours apart.

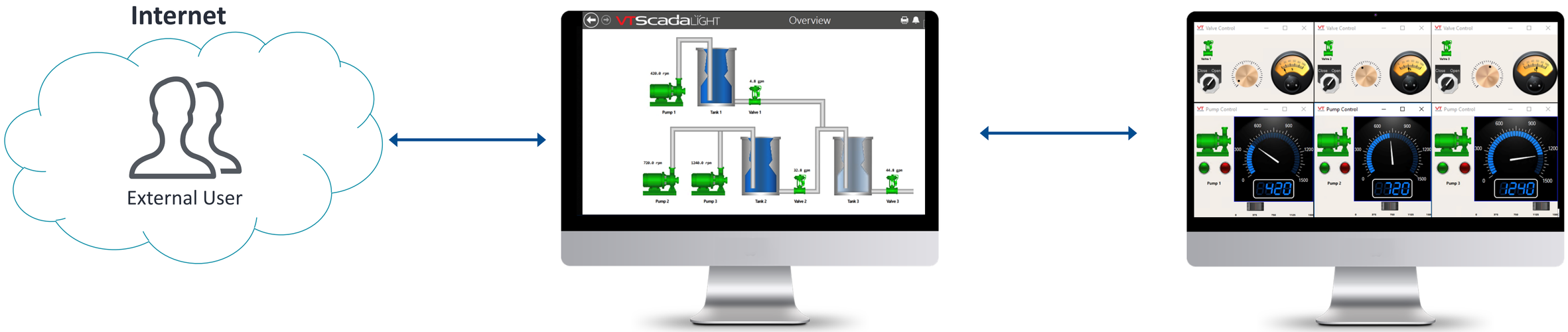
- Access gained via screen sharing exploit
- Ratio of Lye changed from 100ppm to 11,100ppm
- Unusual value noticed by operator & corrected

Report available at
https://www.mass.gov/doc/joint-fbi-cisa-cybersecurity-advisory-on-compromise-of-water-treatment-facility/download

UNISYS | Securing Your Tomorrow™

SIGHTLINE SYSTEMS

Facility Vulnerabilities



- Minimize External Access points

- Windows 7 System
- Allows Remote Access
- Common Password

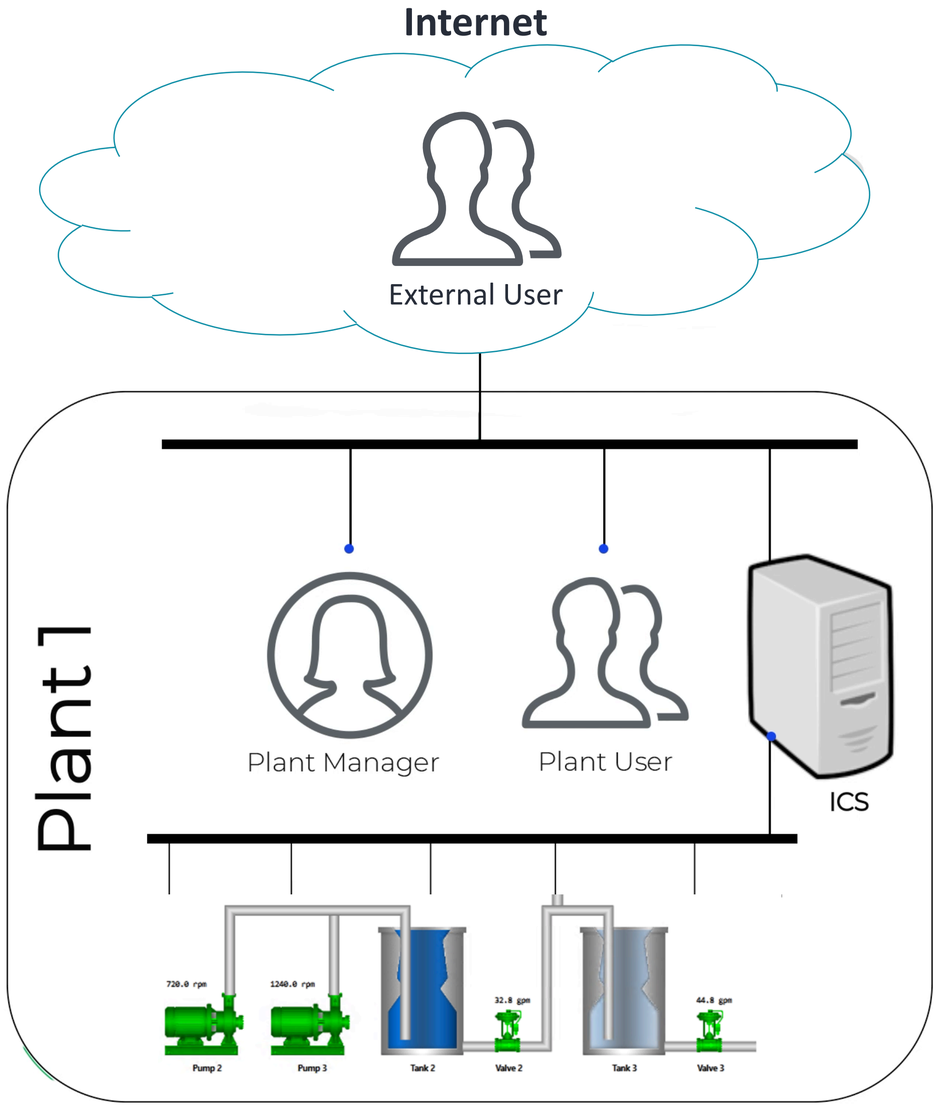
- Minimal process automation / monitoring

"The FBI, the Cybersecurity and Infrastructure Security Agency (CISA), the Environmental Protection Agency (EPA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) **have observed cyber criminals targeting and exploiting desktop sharing software and computer networks running operating systems with end-of-life status to gain unauthorized access to systems**. "

Source: Joint cybersecurity Advisory, Product ID: A21-042A, co authored by FBI, CISA, EPA, Multi-state ISAC. February 11, 2021

UNISYS | Securing Your Tomorrow™ SIGHTLINE SYSTEMS

Typical ICS Configuration



SCENARIO

- The manufacturing machines and sensors are connected to the Industrial Control System (ICS)
- Plant Manager and Plant User access the ICS to monitor status of operations and make any adjustments necessary
- Corporate network is connected to Plant network providing the plant employees access to various corporate systems

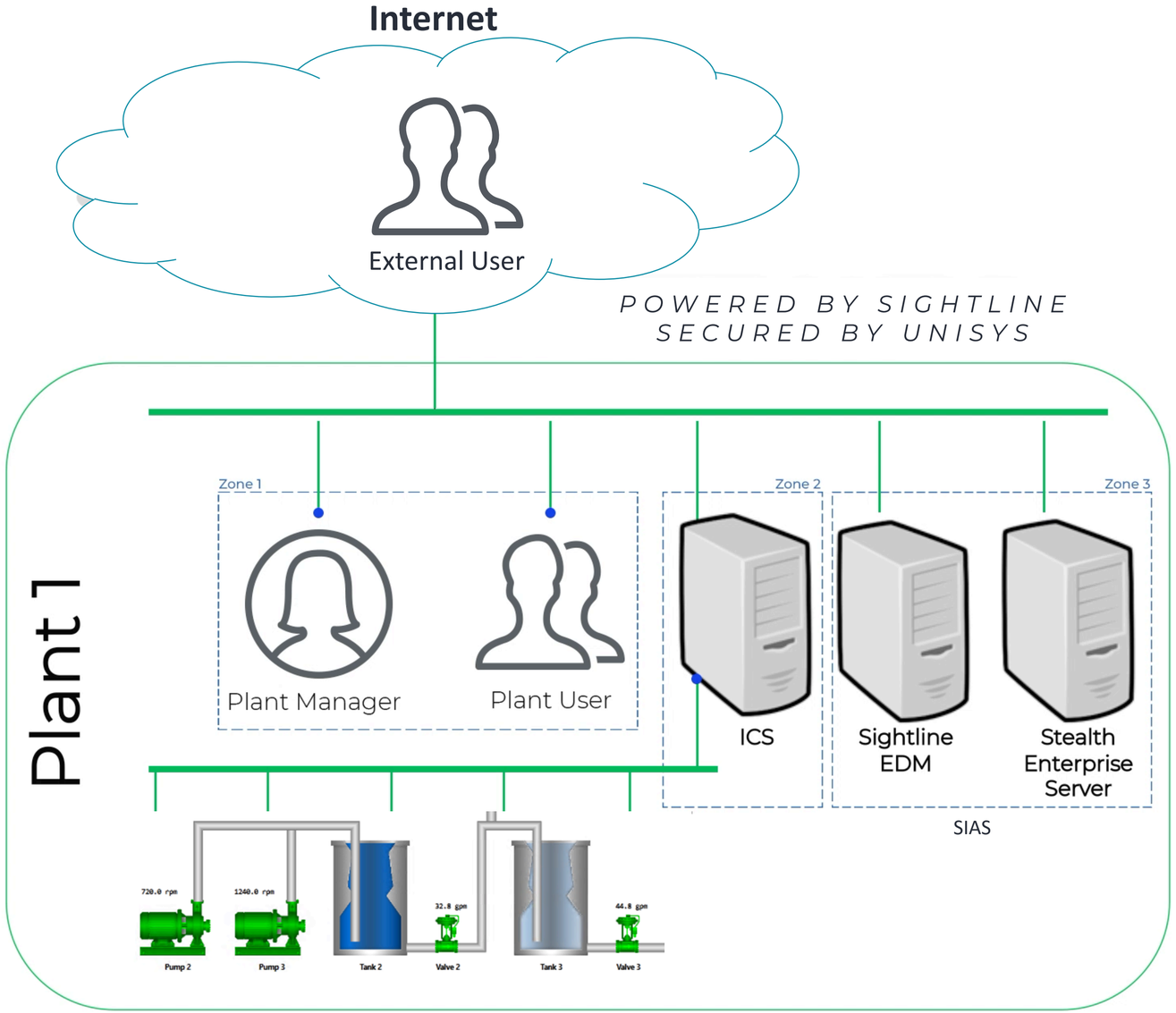
RISKS

- Data is not encrypted on internal networks
- Ransomware / virus can infect plant network likely disrupting operations

UNISYS | Securing Your Tomorrow™

SIGHTLINE SYSTEMS

Recommendations



- Update to the latest version of the operating system (e.g. Windows 10).
- Use multiple-factor authentication.
- Use strong passwords to protect Remote Desktop Protocol (RDP) credentials.
- Ensure anti-virus, spam filters, and firewalls are up to date, properly configured and secure.
- Audit network configurations and isolate computer systems that cannot be updated.
- Audit your network for systems using RDP, closing unused RDP ports, applying multiple-factor authentication wherever possible, and logging RDP login attempts.
- Audit logs for all remote connection protocols.
- Train users to identify and report attempts at social engineering.
- Identify and suspend access of users exhibiting unusual activity.

UNISYS | Securing Your Tomorrow™

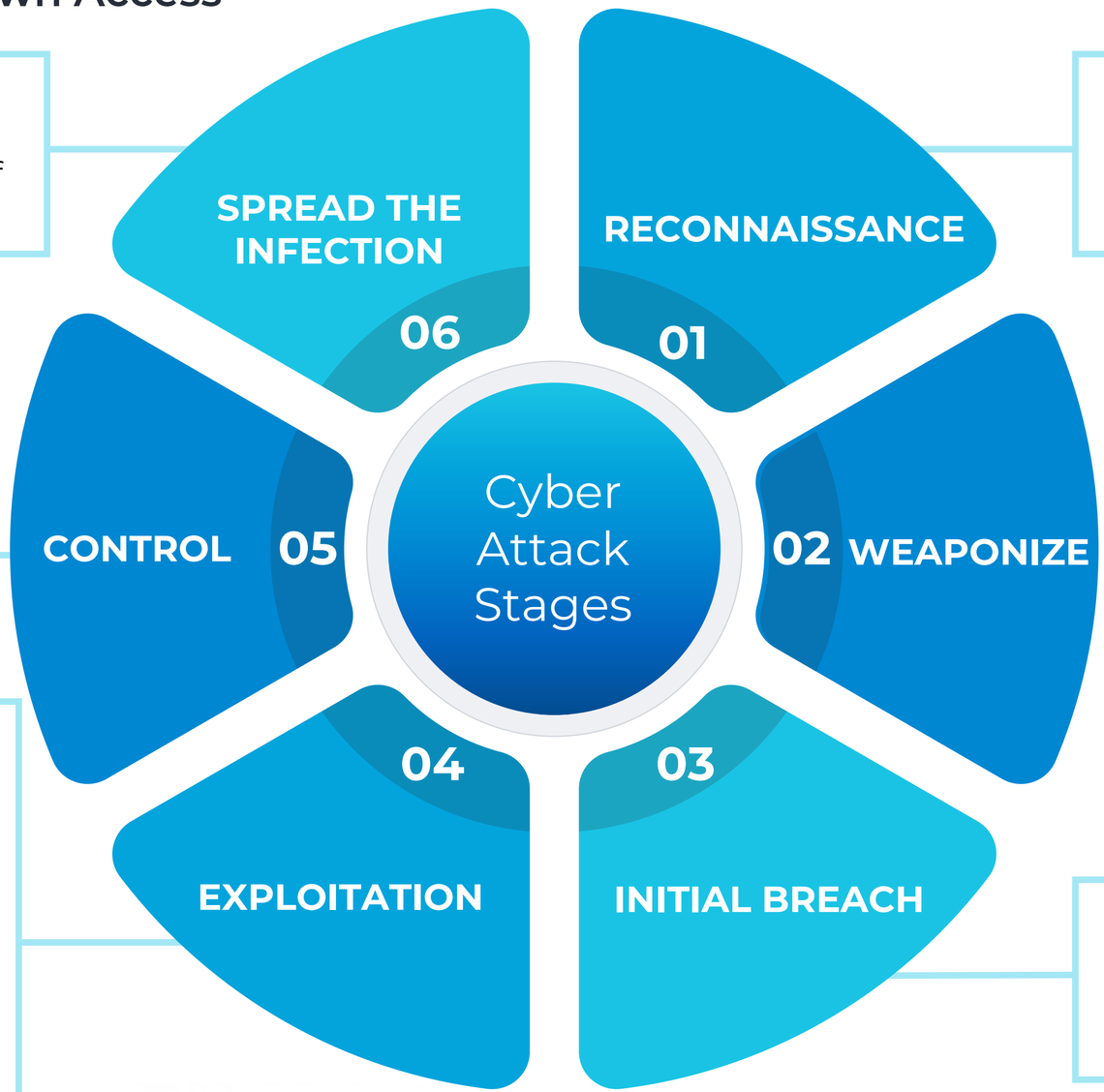
SIGHTLINE SYSTEMS

Defending a Cyber Attack

SIAS Engages to Shut Down Access

SIAS Zoning – Secure IT and OT with cryptographic zones
SIAS Cloaking – Endpoints outside of secure zone not visible

SIAS Cloaking – Protected endpoints not visible outside secure zones
SIAS Aware – Scan your own network to understand existing information flows



SIAS Zoning – Block Internet access by default

SIAS Zoning – Secure zones compliant to IEC62443
SIAS Filtering – Block unused ports
SIAS Encryption – Secure data in transit compliant to NIAP and Common Criteria
SIAS Endpoint Monitoring – Identify unusual behaviour: file encryption, processes stopped, malicious DLLs
SIAS Dynamic Isolation – Automatically isolate endpoints under attack

SIAS Identity – Security profile based on individual user
SIAS Cloaking – Access only available to endpoints within zones

UNISYS | Securing Your Tomorrow™

SIGHTLINE SYSTEMS

What is SIAS?

ANALYSIS

Real Time, Seamless Data Collection & Monitoring

Easy to Use Smart Analytics & Custom Anomaly Alerts

Predictive Forecasting & Root Cause Analysis

SECURITY

Cloaking: Cloaking Of All Endpoints & Sensitive Data

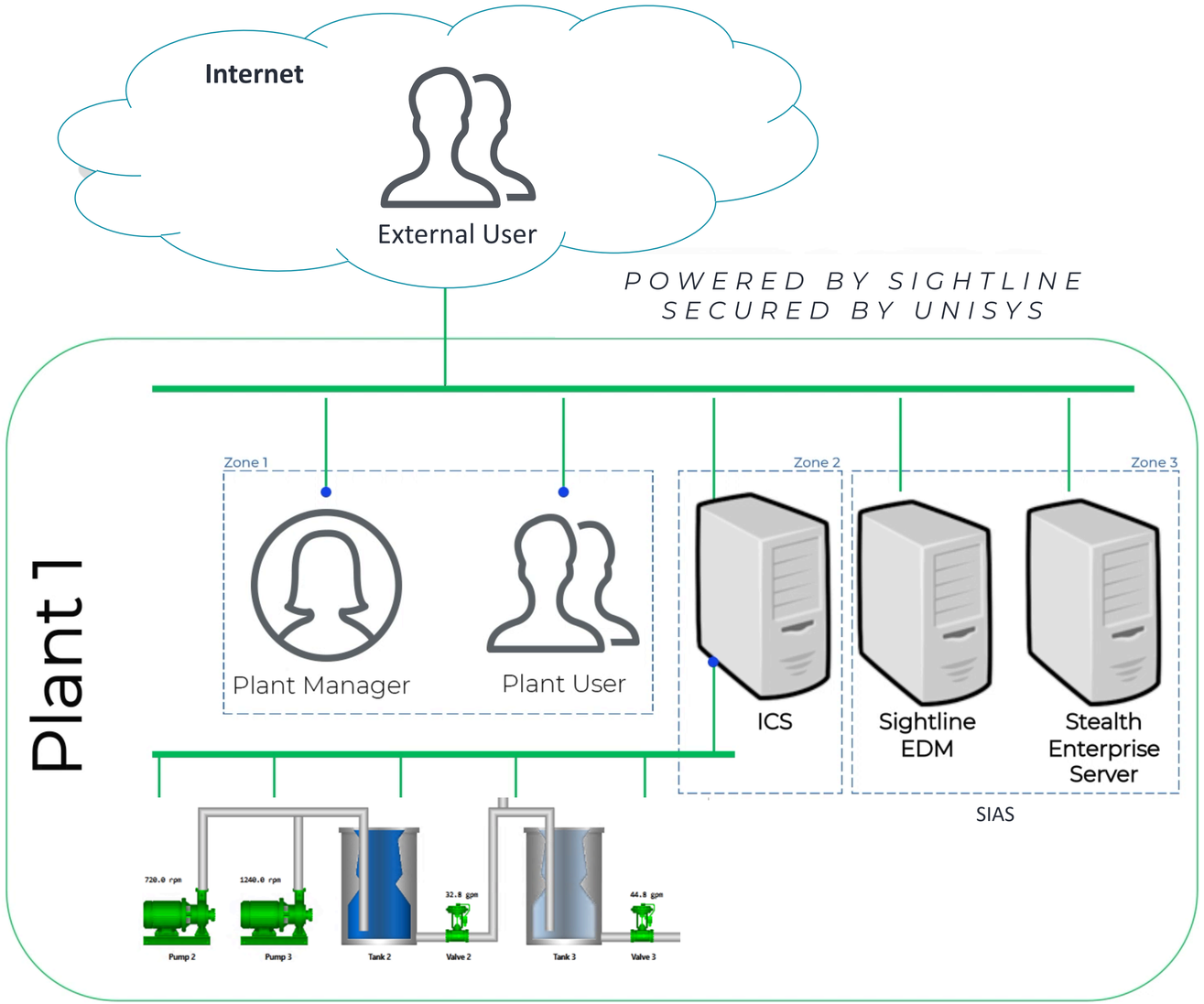
Isolation: Dynamic Isolation Of Potential Threats

Zoning: Cryptographic Zoning & Data Encryption

UNISYS | Securing Your Tomorrow™

SIGHTLINE SYSTEMS

SIAS in Action



EXAMPLE: DYNAMIC ISOLATION IN ACTION

- SIAS collects IOT data from ICS & monitors production servers
- Plant User makes change to IOT setting on production system
- SIAS detects change in data from an IOT sensor triggering alert
- SIAS protects network via dynamic isolation, isolating the “Plant User” from the rest of network

UNISYS | Securing Your Tomorrow™

SIGHTLINE SYSTEMS

Thank You!

Learn More: www.sightline.com/security

Secure Industrial Analytics Solution (SIAS) : Powered by Sightline Systems | Secured by Unisys

UNISYS | Securing Your Tomorrow™

SIGHTLINE SYSTEMS