SIAS

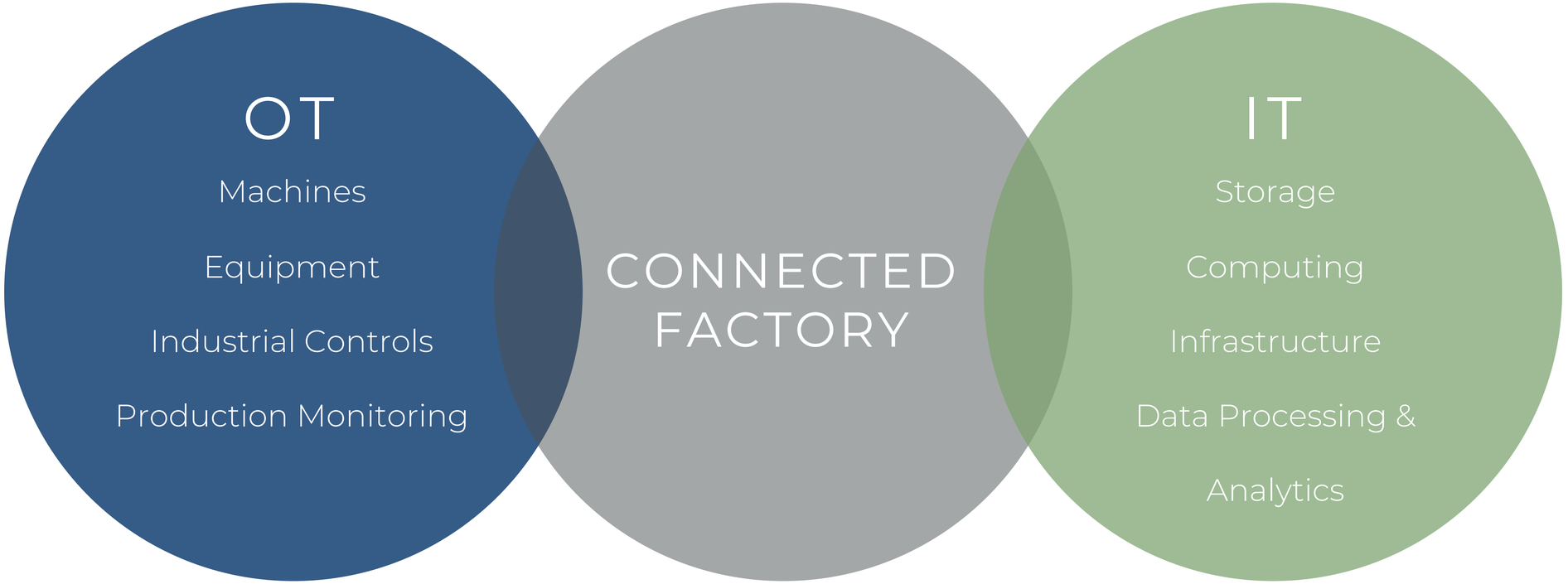
Secured Industrial Analytics Solution

Powered by Sightline. Secured by Unisys.

UNISYS | Securing Your Tomorrow™

SIGHTLINE SYSTEMS

SMART FACTORY BRING IT AND PLANT OPERATIONS TOGETHER



SMART FACTORY HELPS IMPROVE PLANT OPERATIONS

Benefits from smart factory initiatives are many and sizeable

Impact to the key manufacturing metrics over the past three years

+12%

Change in labor productivity

+11%

Change in factory capacity utilization

+10%

Change in total production output

Source: Deloitte analysis of the 2019 Deloitte and MAPI Smart Factory Study data.

Deloitte Insights | deloitte.com/insights

A SMART FACTORY INTRODUCES NEW CHALLENGES

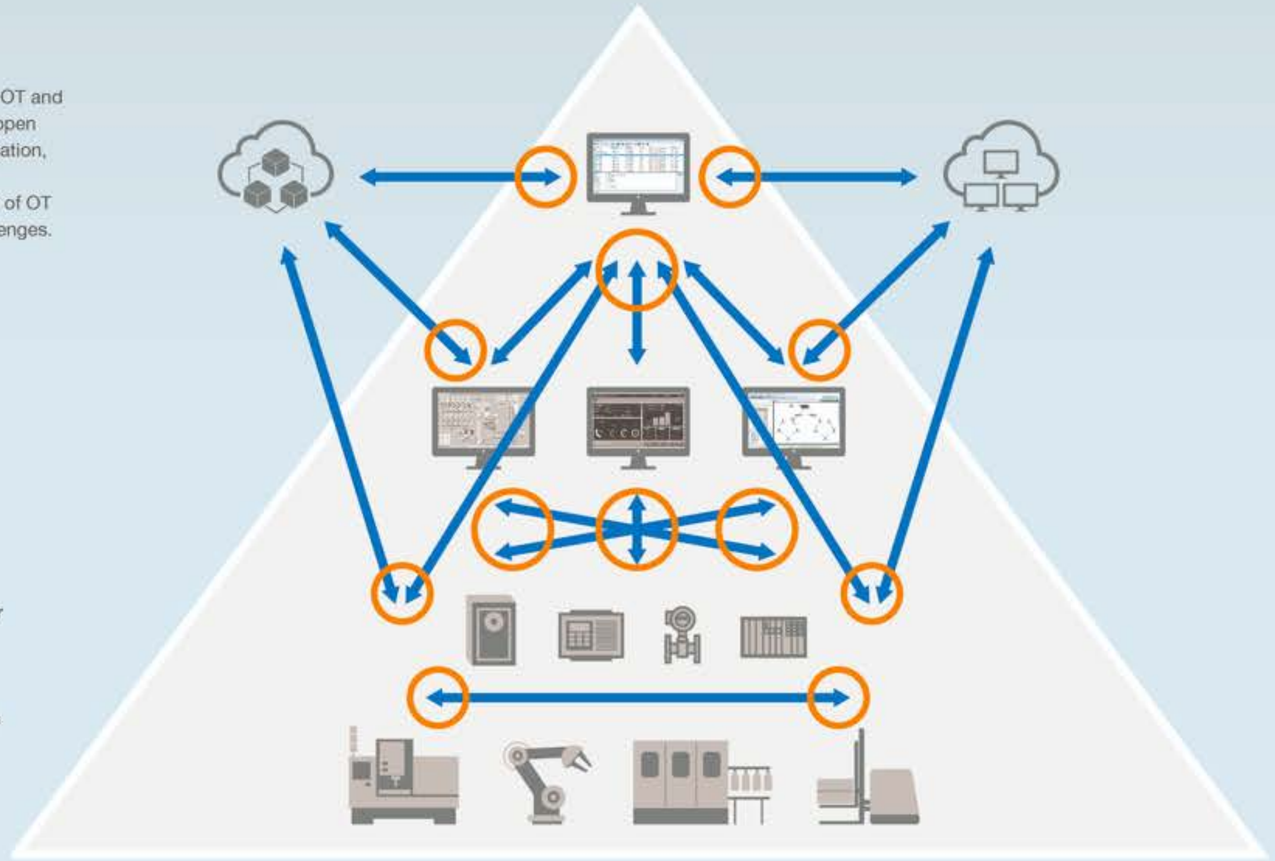
Various Protocols

Multiple communication protocols abound in OT and IT realms, such as fieldbus, proprietary, and open protocols for machine-to-machine communication, and RESTful API and MQTT for IT and cloud applications. The IIoT requires the integration of OT and IT—hence, the protocol conversion challenges.

Azure · Alibaba Cloud · MQTT · RESTful API · SNMP · OPC UA · PROFINET · EtherNet/IP · Modbus

Various Interfaces

A variety of wired interface conversions occur in OT and IT, including serial-to-serial, serial-to-fiber, fieldbus-to-fiber, Ethernet-to-fiber. With the IIoT requiring hyper-agility, an increase in wired-to-wireless conversions only complicates operations.



Various Vulnerabilities

In the past, ICS networks were physically isolated and almost immune to cyberattacks. However, the IIoT has opened up OT silos to the IT world to expand system and network integration, making IT/OT convergence unfortunately vulnerable to internal interferences and external threats.

Firewall · VPN · WiFi a b g n ac · IEEE 8023 · lte

Various Networks

Various networks already exist in the worlds of OT and IT, including local area network (LAN), wireless local area network (WLAN), and wide-area network (WAN). As the IIoT requires more device-to-cloud and sensor-to-cloud integration, adopting new communication technologies to achieve interconnectivity will actually complicate network integration.

A SMART FACTORY INTRODUCES NEW RISKS AND THREATS

RISKS	THREATS
Business and operation disruption	Malware
Financial fraud	Ransomware
Privilege abuse attempts/escalation	Advance persistent threats (APT)
Platform hacking	Spear phishing
Data leakage, tampering, manipulation	Bots
Configuration change	Distributed Denial of Service
Vulnerabilities	Password attacks
Software update and patch	Rogue software
Device tamper, impersonation, disruption	Malvertising
Device hacking or snooping	Internal Threats
Comprised firmware update	
API interface manipulation	

HOW DO WE HELP?

SEAMLESS MONITORING

- Collect data from virtually any source
- Automate monitoring activities
- Custom dashboards to show status

Making Data Smart
Securing Your Tomorrow

BETTER DECISIONS

- Make quantitative decisions based on real time data
- Improve service while reducing costs
- Forecast future behavior easily with web-based reports

SECURE ENVIRONMENT

- Encrypt all data
- Dynamically isolate threats
- Protection from cyber attacks

FASTER RESPONSES

- Correlate data in seconds
- Visualize data in real time
- Find cause of issues more quickly

UNISYS | Securing Your Tomorrow™ SIGHTLINE SYSTEMS

WHAT IS SIAS?

SECURE INDUSTRIAL ANALYTICS SOLUTION

COLLECT DATA FROM SYSTEMS & ICS DEVICES

ALERT POTENTIAL ISSUES & REAL-TIME REPORTING

EASY TO USE VISUALIZATION & ANALYTICS TOOLS

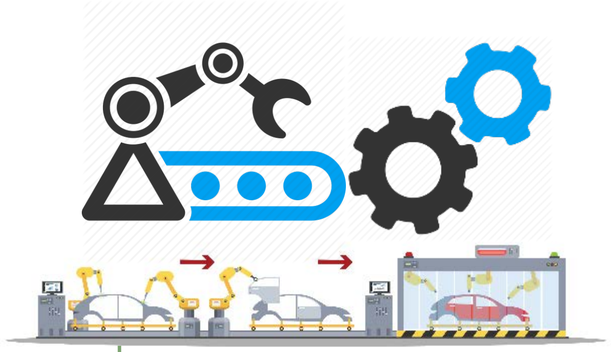
CRYPTOGRAPHIC ZONING & DATA ENCRYPTION

ENDPOINTS ARE CLOAKED

DYNAMIC ISOLATION

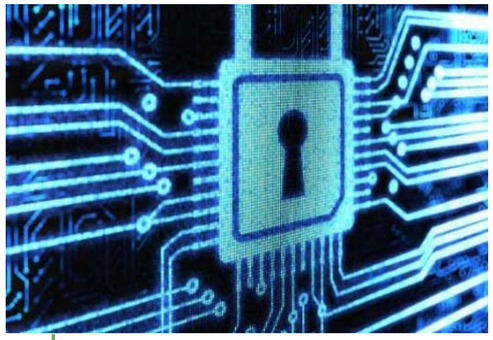
UNISYS | Securing Your Tomorrow™ SIGHTLINE SYSTEMS

HOW DOES IT WORK?



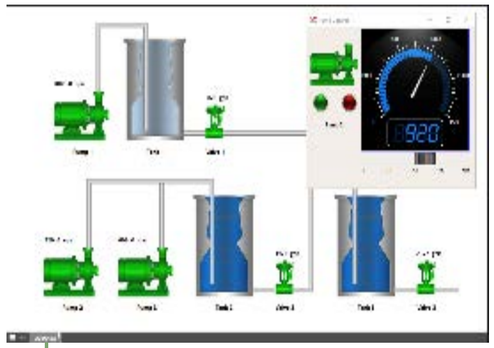
Equipment produces data

Devices are cloaked on network



Data is transmitted over Network

Data is encrypted



Users control machines, plc's, etc

Data is collected & stored

Users monitor status of systems

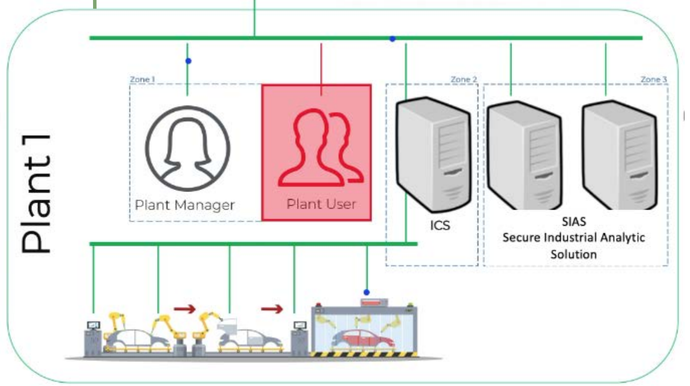
Real-time dashboards and reports

Data is analyzed

Alerts, trends, & forecasts produced

Systems begin behaving abnormally

Threats isolated immediately



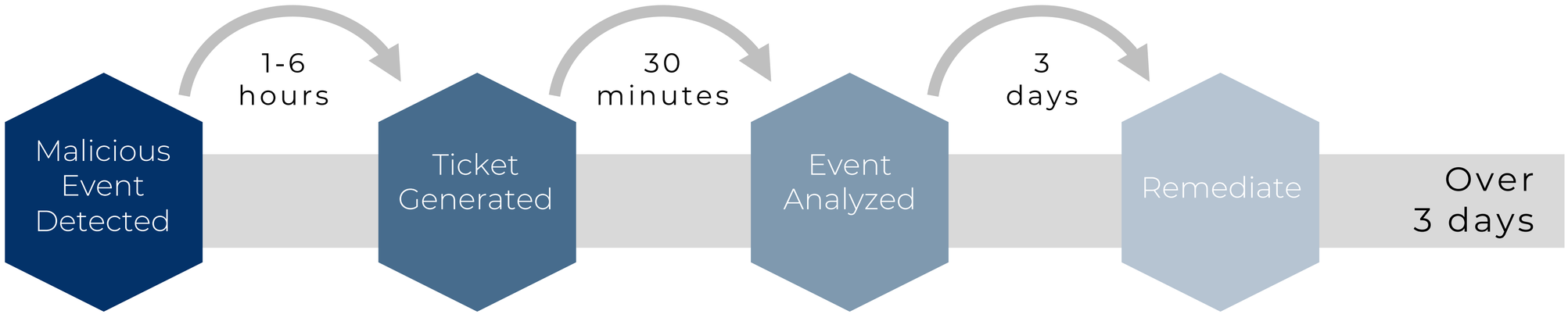
UNISYS | Securing Your Tomorrow™

SIGHTLINE SYSTEMS

SIAS DYNAMIC ISOLATION

TRADITIONAL **IT** SIEM TECHNOLOGIES

*NOT TYPICALLY IN THE **OT** ENVIRONMENT*



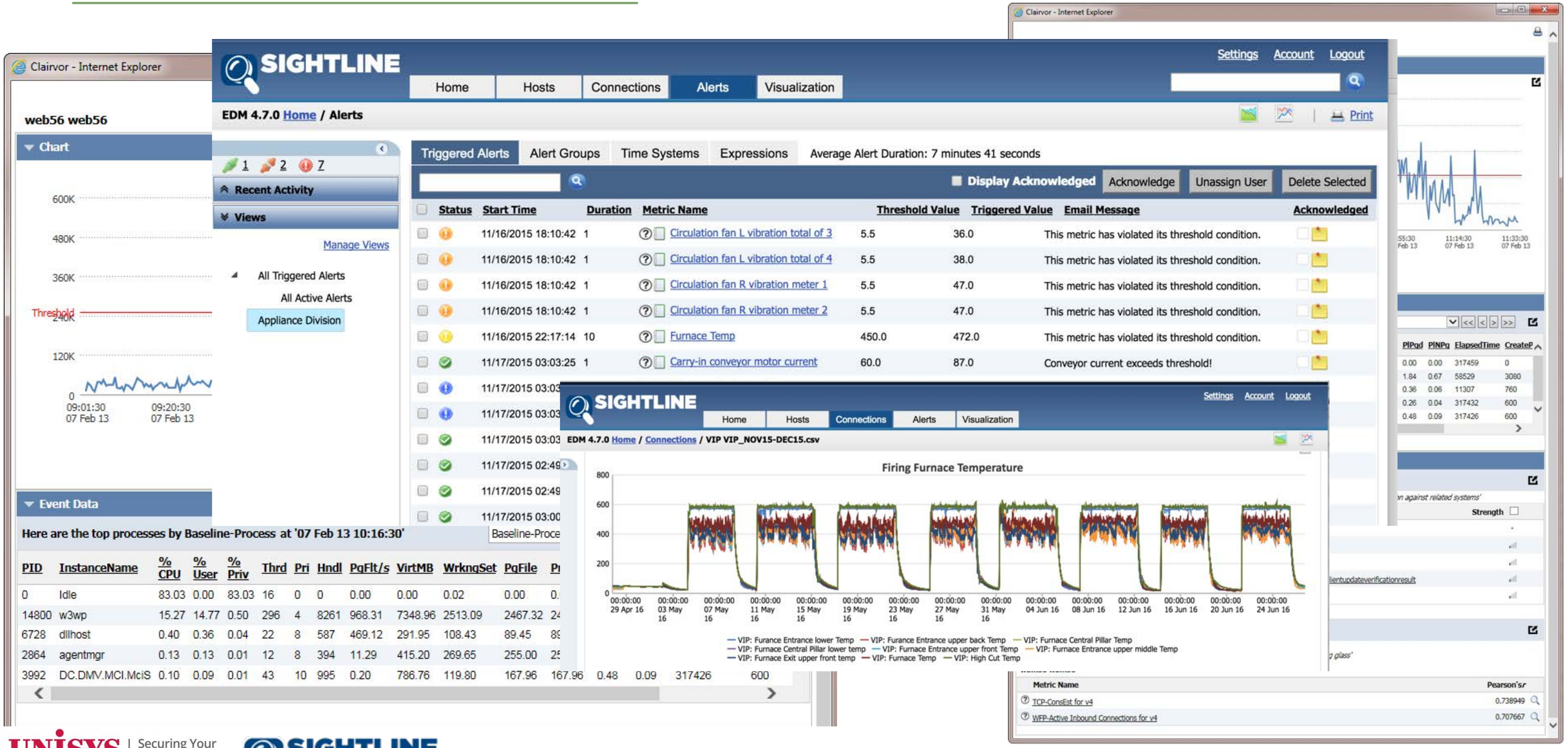
SIAS DYNAMIC ISOLATION

*SECURITY FOR BOTH **IT AND OT** ENVIRONMENTS*

UNISYS | Securing Your Tomorrow™ SIGHTLINE SYSTEMS

EASILY BUILD REPORTS, DASHBOARDS & FORECAST FUTURE BEHAVIOR

ALERTING & ADVANCED ANALYTICS SOLVE ISSUES FASTER



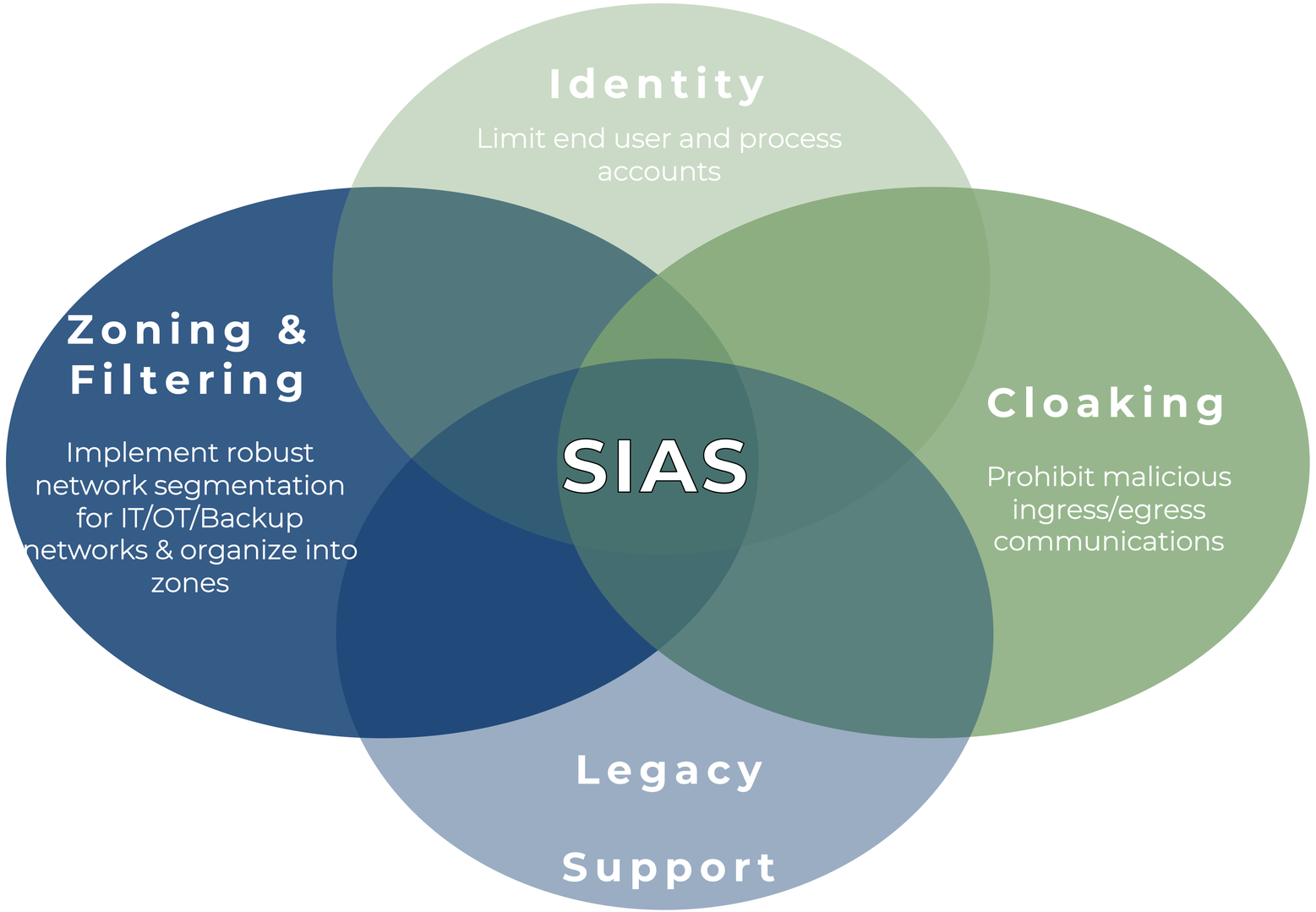
RANSOMWARE IMPACTS US PIPELINE OPERATIONS

In February 2020 a US Natural Gas Pipeline Operator suffered Ransomware attack

- A spearphishing email initially gained access to the IT network, then pivoting to OT network
- Commodity ransomware was deployed, encrypting the data on both IT and OT networks
- This prevented human operators from accessing HMI's, data historians and polling sensors
- Operations were halted for two days while attack was resolved

ADDRESSING REAL WORLD SCENARIO'S

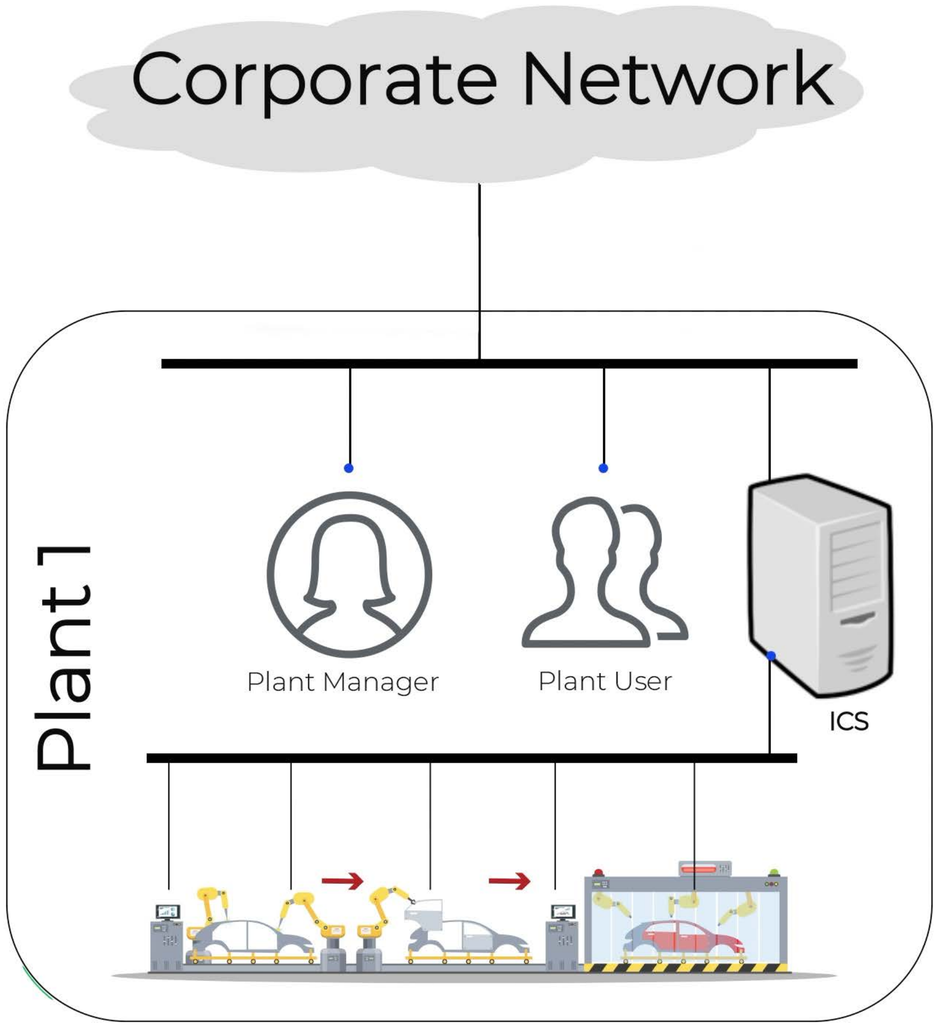
https://www.us-cert.gov/ncas/alerts/aa20-049a



CISA Recommendations

- Implement and ensure robust Network Segmentation
- Organize OT assets into logical zones by taking into account criticality
- Implement regular Data Backup procedures
- Ensure user and process accounts are limited
- Filter Network Traffic to prohibit ingress and egress communications
- Update Software including operating systems
- Limit Access to Resources over Network

TYPICAL CONFIGURATION



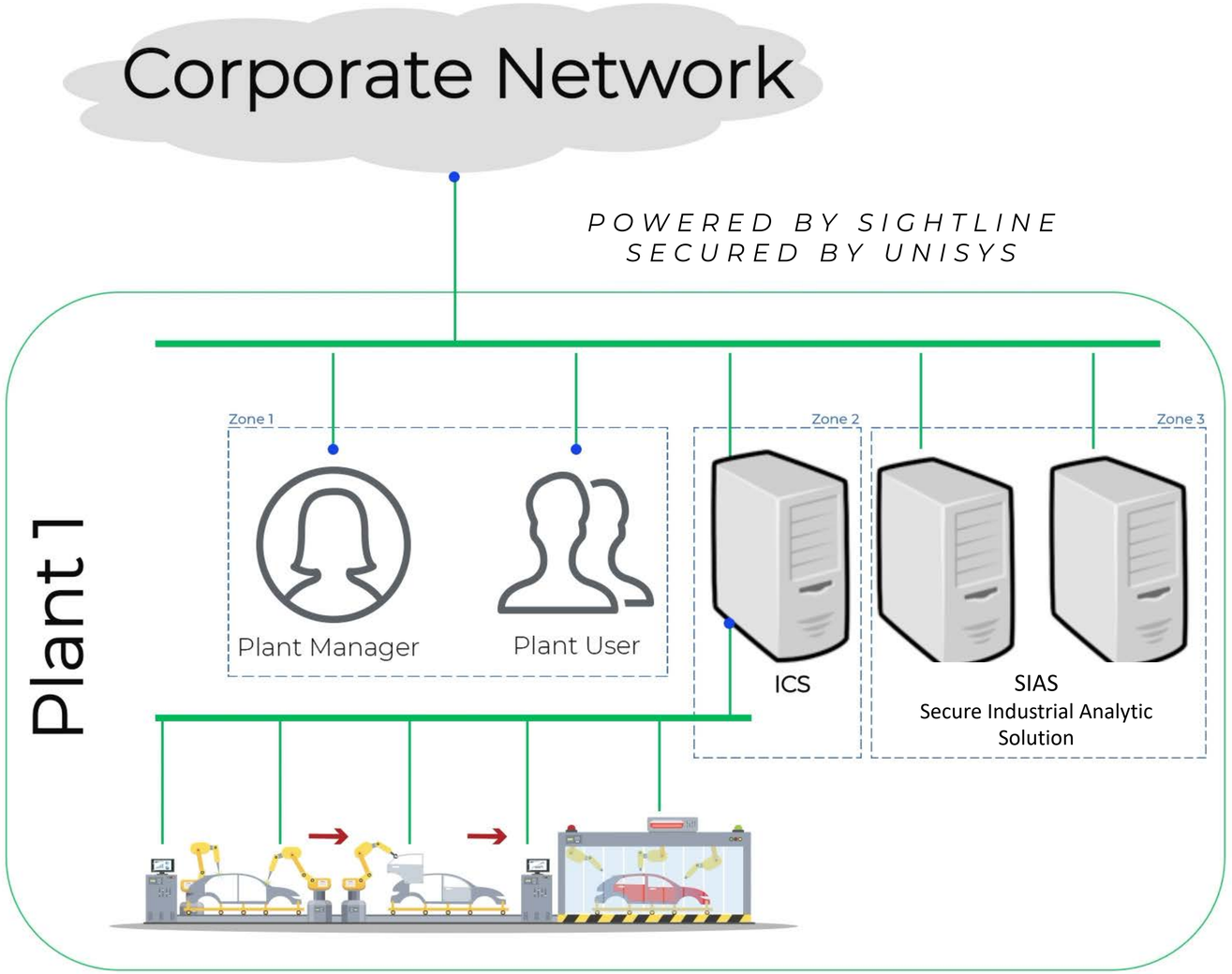
SCENARIO

- 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

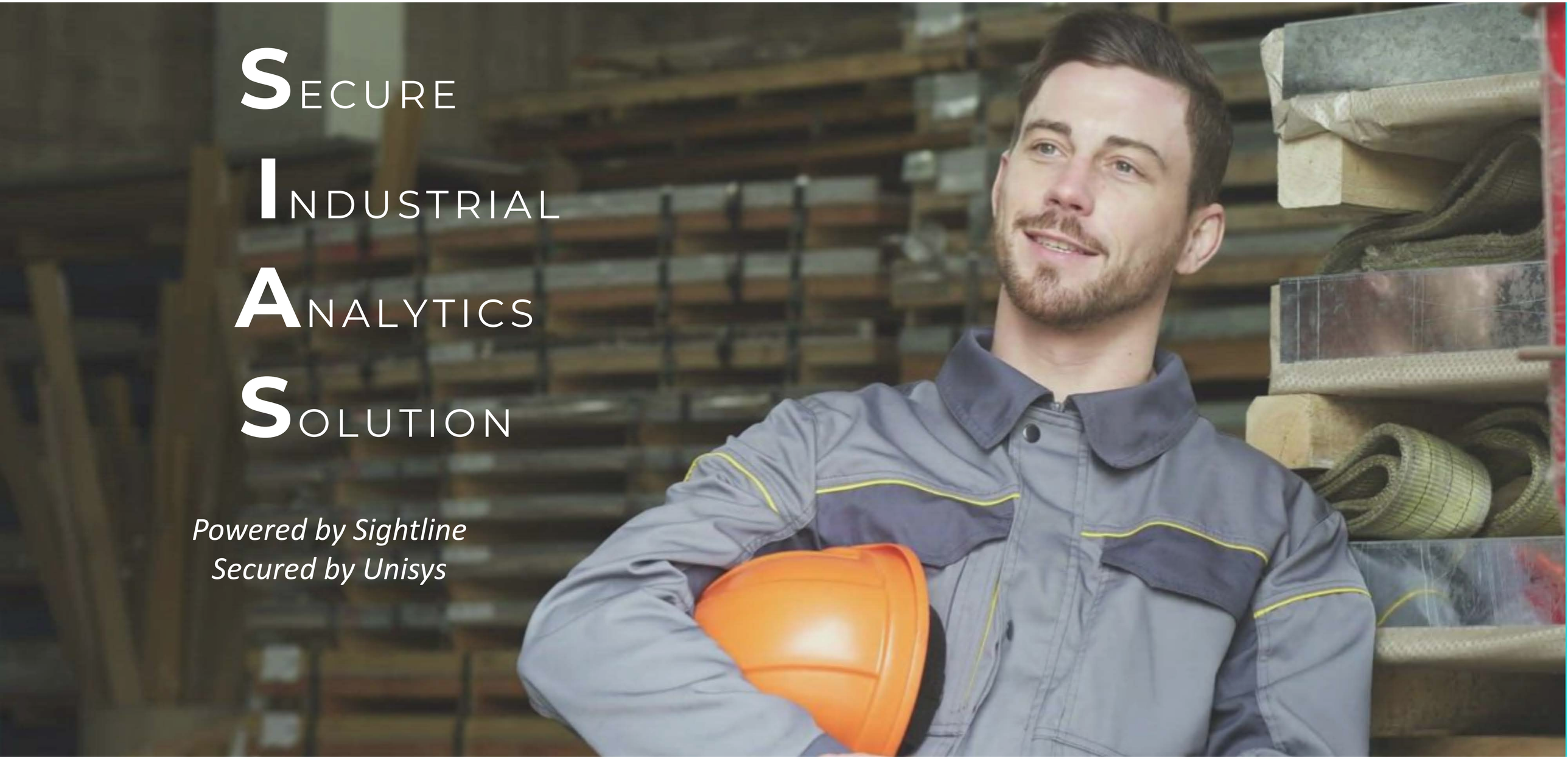
- Data is not encrypted on internal networks
- Ransomware / virus can infect plant network likely disrupting operations

SIAS IN ACTION



FOR EXAMPLE: DYNAMIC ISOLATION IN ACTION

- SIAS collects IOT data from ICS & monitors production servers
- Plant User makes malicious 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