DRAGOS AVEVA

WEBINAR

Operational Technology (OT) Cybersecurity Best Practices for Digital Transformation in Manufacturing

Dr. Michael Powell
Cybersecurity Engineer, NCCoE, NIST

John Hoyt
Lead Cybersecurity Engineer, MITRE

Josh Carlson
Director, Business Development, Dragos

Dan Lopez
Staff Pre-Sales Engineer, AVEVA

Agenda

- Cybersecurity Challenges and Best Practice Overview
- NCCOE Test Bed Architecture
- Dragos Technology Overview
- AVEVA Technology Overview
- Use Case Scenarios 1 - 4
- Summary
- Next steps

Who We Are

It takes a village – together, providing process data + cyber data with scalable best of breed integrated solutions, to solve today's cybersecurity challenges.

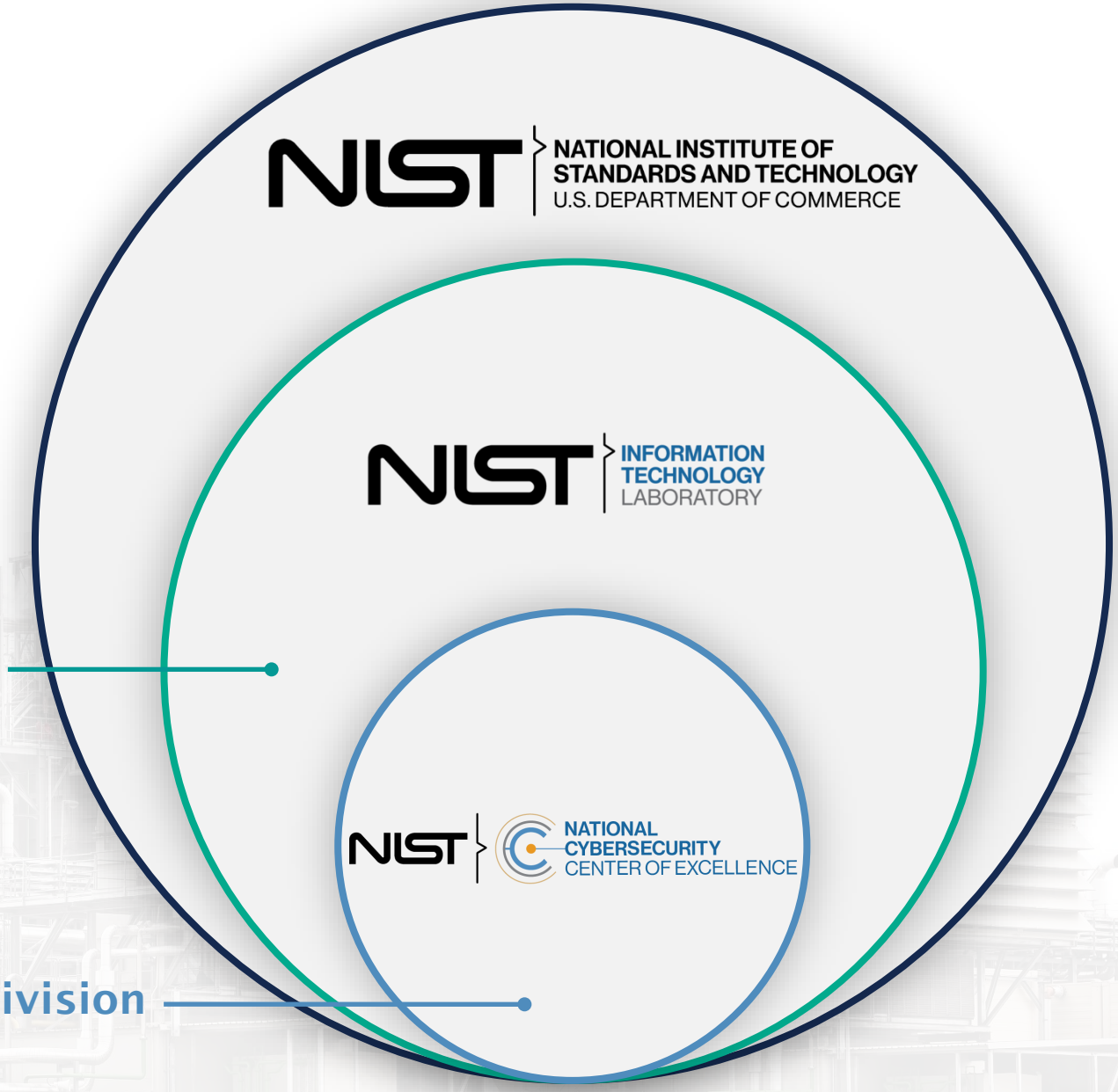
Dragos is an industrial (ICS/OT/IIoT) cybersecurity company on a mission to safeguard civilization.

AVEVA empowers operators to deliver safer, more reliable, resilient, sustainable, and efficient services to their customers while minimizing risk and lowering total cost to operate.

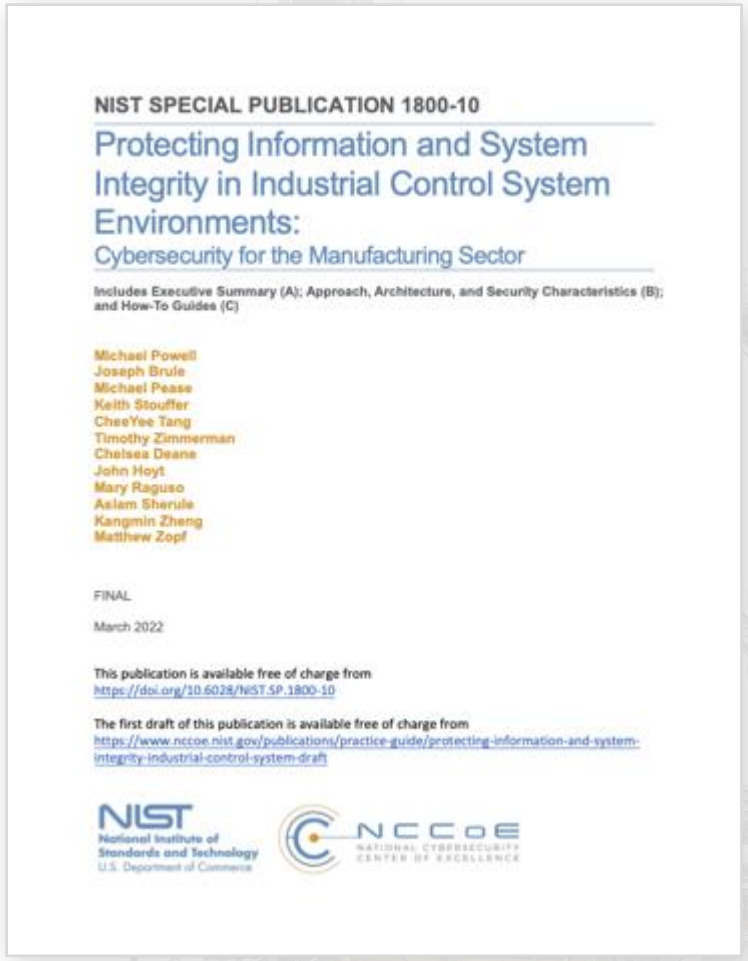
NCCoE is a solution-driven, collaborative hub addressing complex cybersecurity problems.

NCCoE

As part of the NIST family, the NCCoE has access to a foundation of expertise, resources, relationships, and experience.



Cybersecurity Best Practice Guide



NIST SPECIAL PUBLICATION 1800-10

Protecting Information and System Integrity in Industrial Control System Environments:

Cybersecurity for the Manufacturing Sector

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Michael Powell
Joseph Brule
Michael Pease
Keith Stouffer
CheeYee Tang
Timothy Zimmerman
Chelsea Deane
John Hoyt
Mary Raguso
Aslam Sherule
Kangmin Zheng
Matthew Zopf

FINAL

March 2022

This publication is available free of charge from
https://doi.org/10.6028/NIST.SP.1800-10

The first draft of this publication is available free of charge from
https://www.nccoe.nist.gov/publications/practice-guide/protecting-information-and-system-integrity-industrial-control-system-draft

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE National Cybersecurity Center of Excellence

NIST SPECIAL PUBLICATION 1800-10

Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector

- Provide an approach to help manufacturers prevent, mitigate, and detect threats from cyberattacks or insider threats within an ICS environment
- Demonstrate how commercially available technologies deployed in this build can provide cybersecurity capabilities that manufacturing organizations can use to secure their operational technology (OT) systems

Cybersecurity Best Practice Scenarios

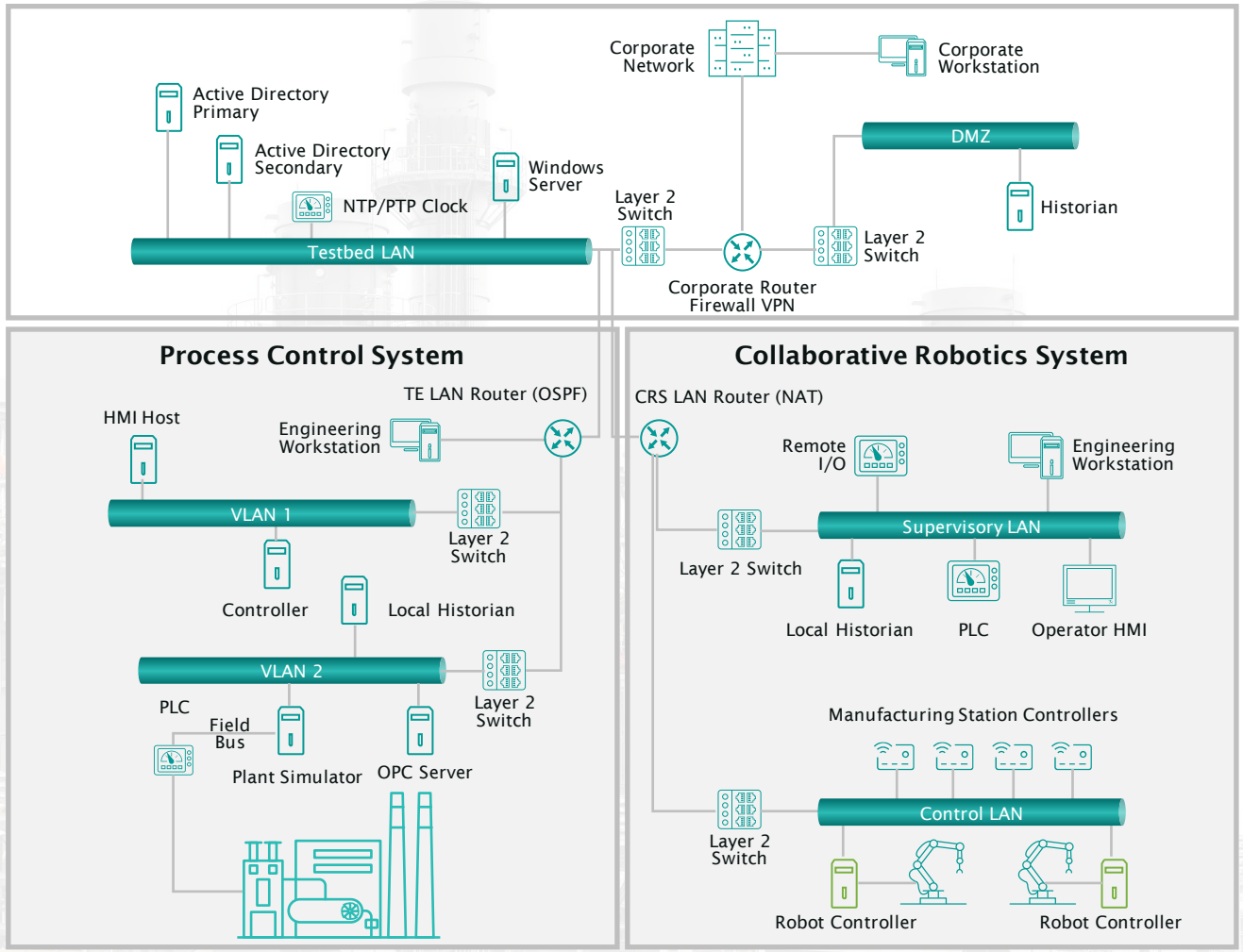
Challenge:

ICS are vulnerable to disruption and security risks because they are no longer isolated from the outside world leaving them exposed to cyberattacks, as well as authorized users who accidentally or intentionally compromise information and system integrity.

Scenario 1	Detect Unauthorized Device-to-Device Communications
Scenario 2	Detect Sensor Data Manipulation
Scenario 3	Detect Unauthorized Modification of PLC Logic
Scenario 4	Detect Unauthorized Firmware Modification

NIST Engineering Laboratory Testbed

Common Components



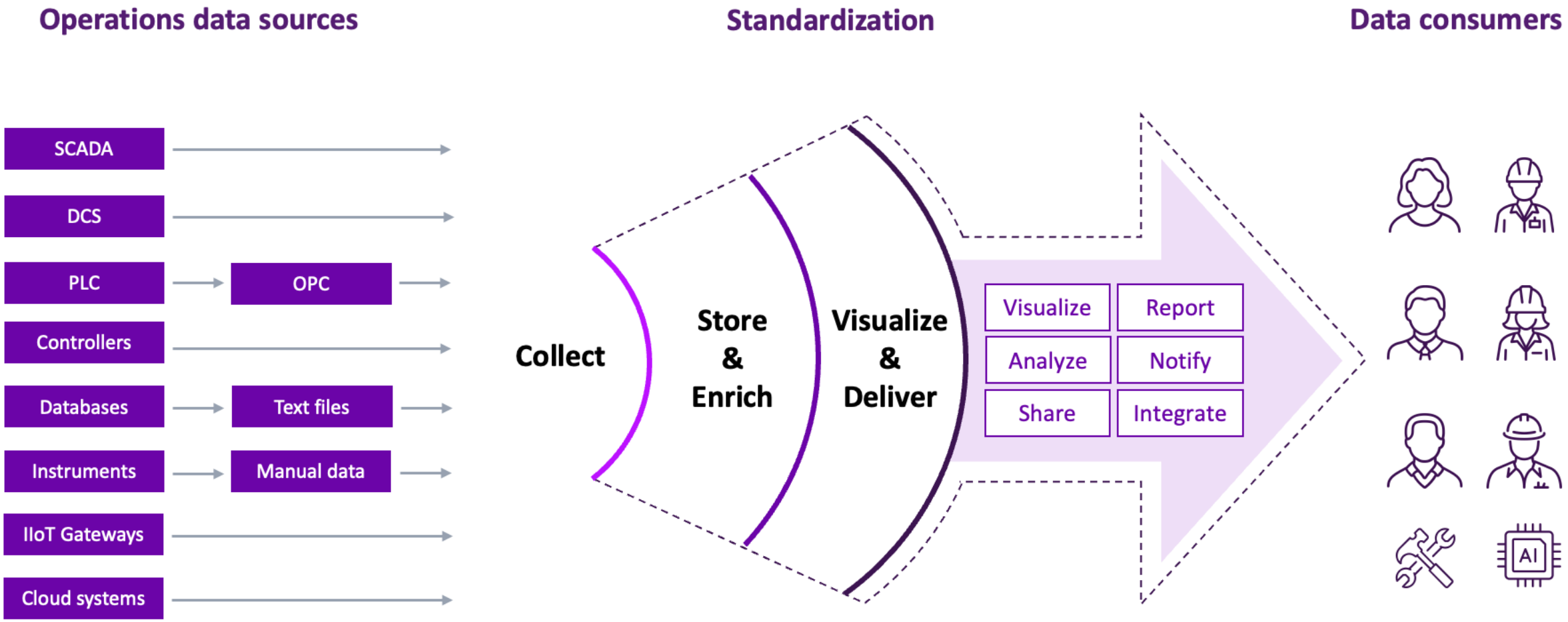
1. Process Control System (PCS)

2. Collaborative Robotics System (CRS)

NISTIR 8089: *An Industrial Control System Cybersecurity Performance Testbed*, http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf

The Dragos Platform

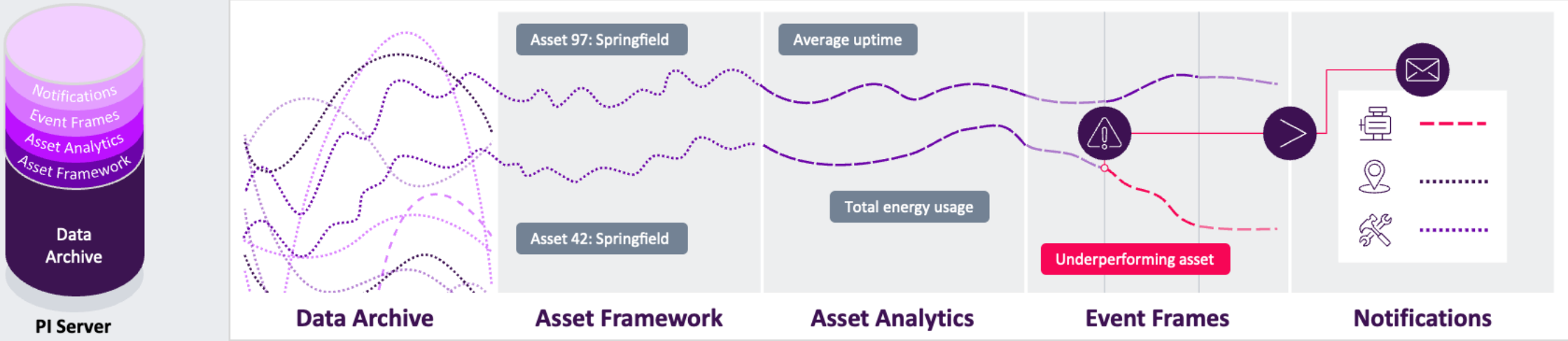
AVEVA PI Server Provides Underlying Data Infrastructure



PI Server's Enrichment Features Turn Data Into Decision-ready Information

Add structure and meaningful context to operations data

Automatically **pinpoint important events** in operations



Optimized storage & access to massive volumes of operational data

Transform raw data into actionable KPIs using streaming calculations

Send automatic alerts to the right people with the right information

Scenario 1: Detect Unauthorized Device-to-Device Communications

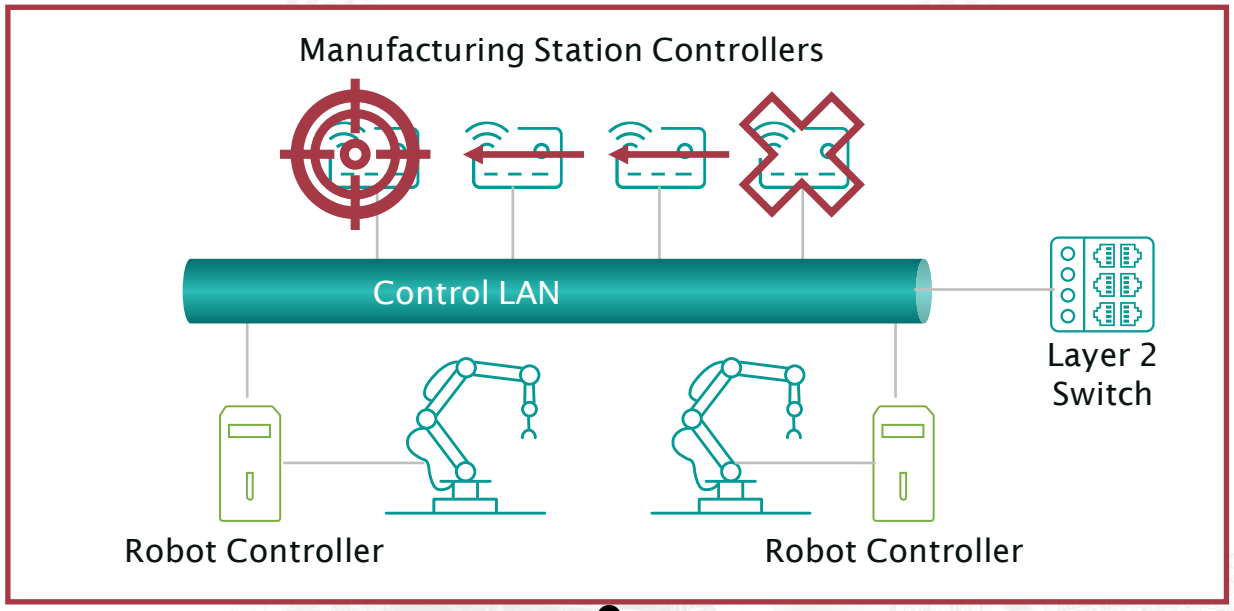
A device authorized to be on the network attempts to establish an unapproved connection.

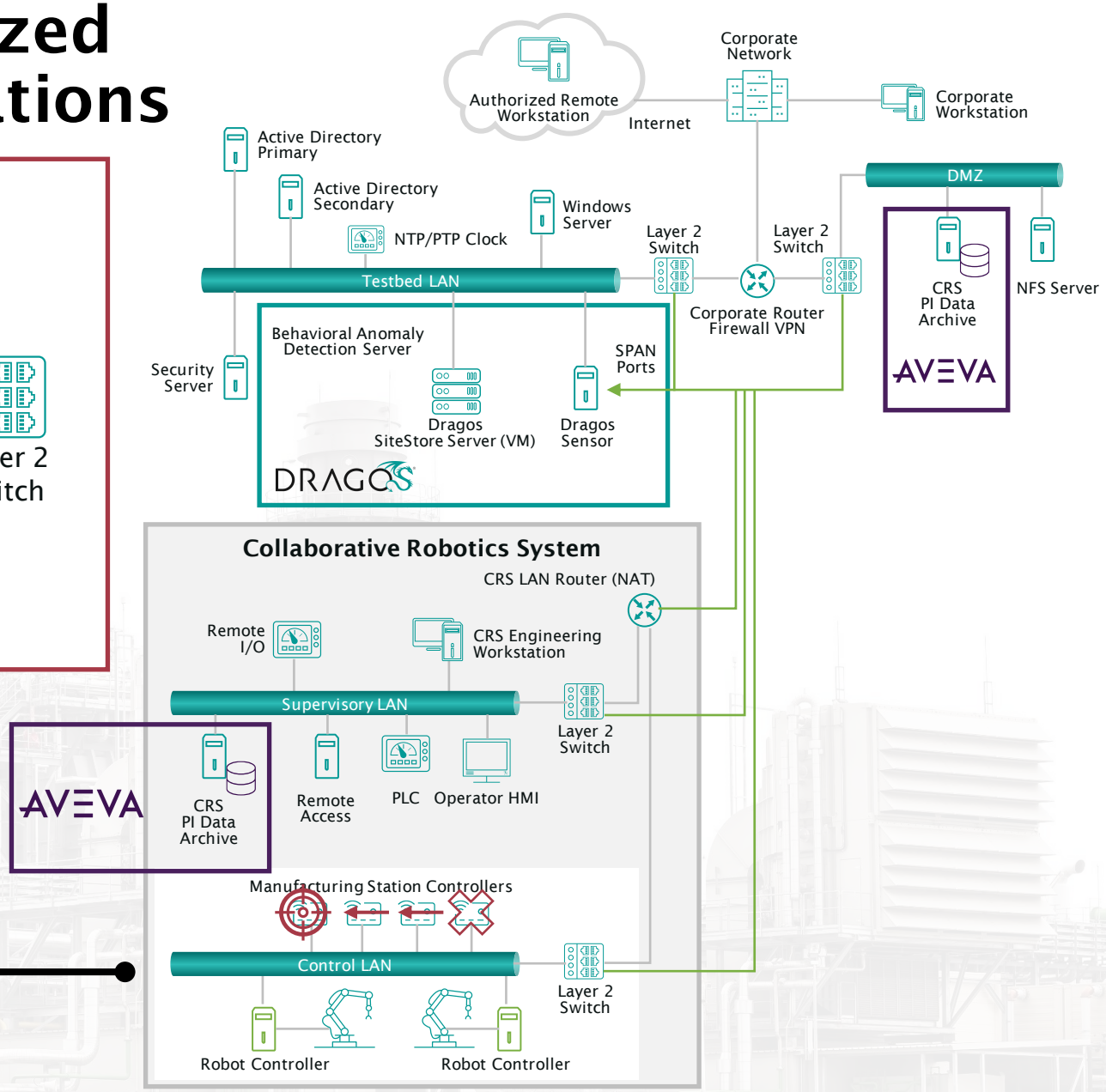
Objective: Demonstrate the detection of unauthorized communications between devices.

Test: The device attempts to establish an unapproved connection.

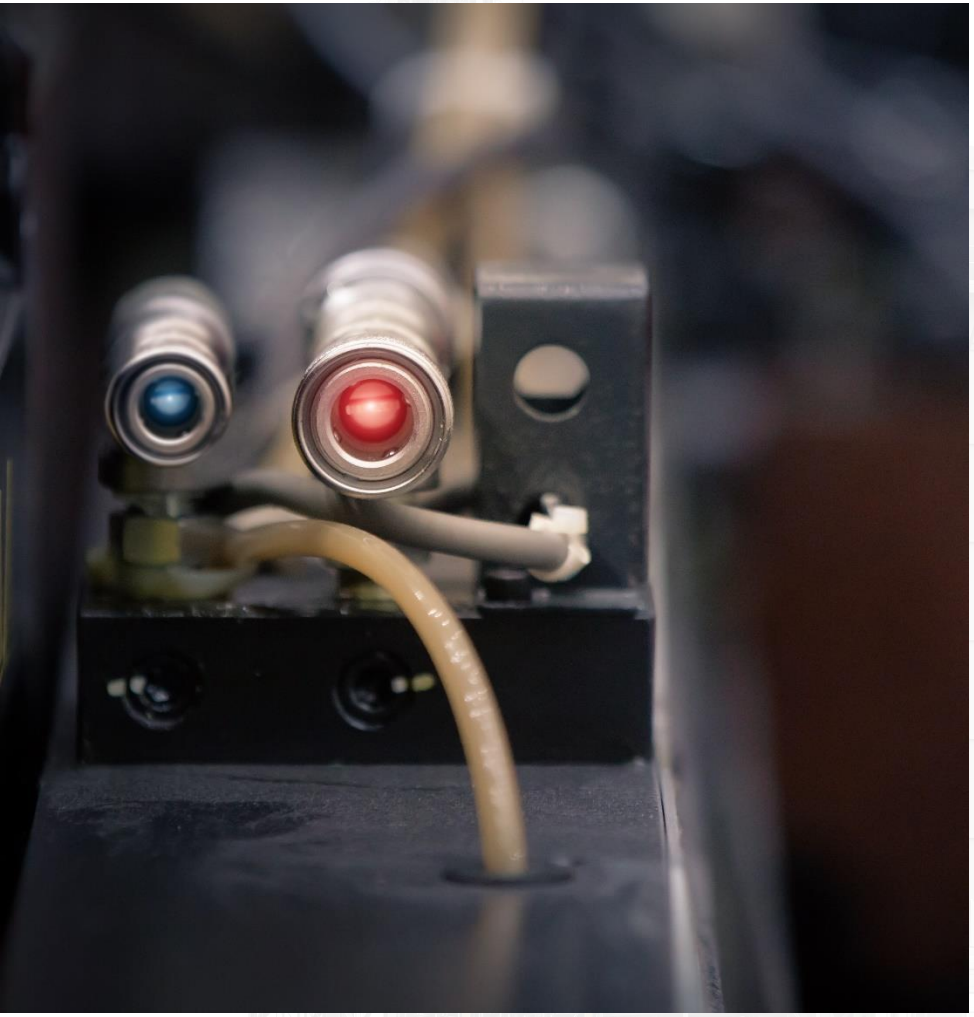
Results: Capture the suspicious traffic and generate an alert.

Scenario 1: Detect Unauthorized Device-to-Device Communications





Scenario 2: Detect Sensor Data Manipulation (PI)



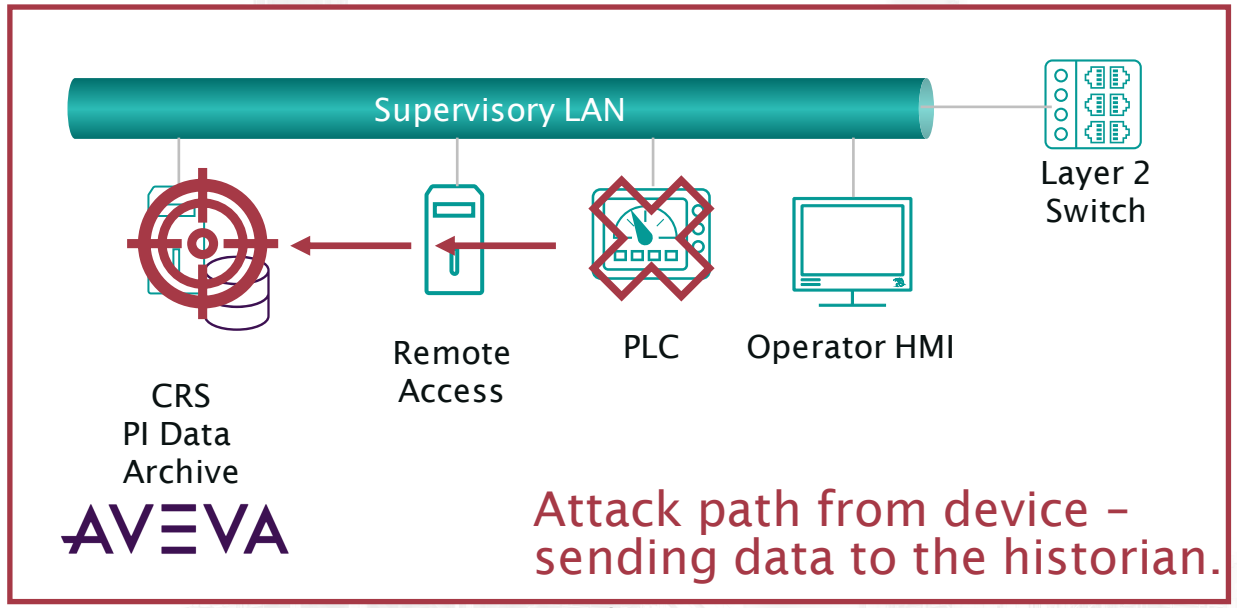
A sensor in the manufacturing system begins sending atypical data values to the historian.

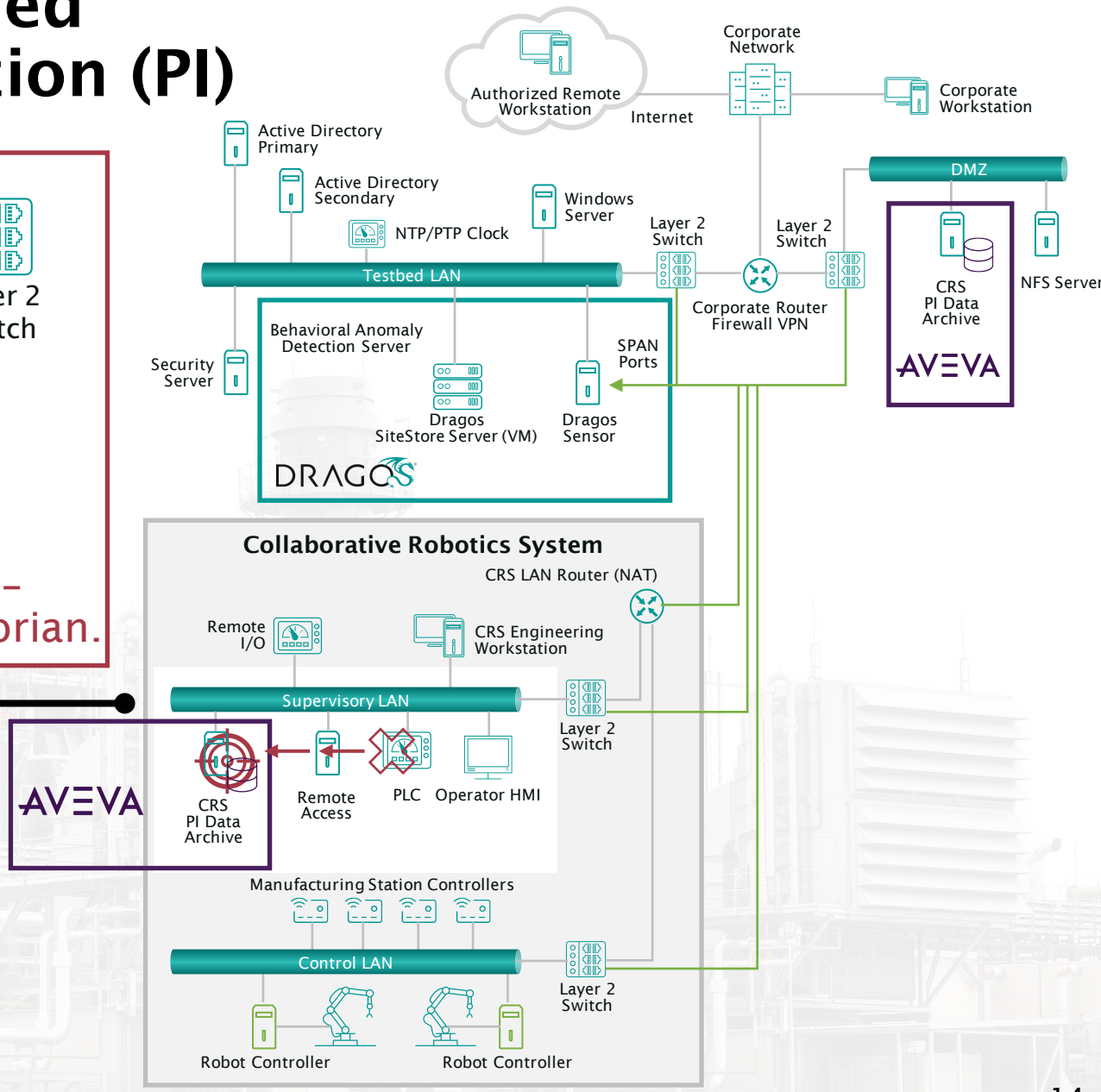
Objective: Demonstrate the detection of atypical data reported to the historian.

Test: A sensor sends invalid data to the historian.

Results: Ability to detect atypical data and create an event frame.

Scenario 2: Detect Unauthorized Detect Sensor Data Manipulation (PI)





Scenario 3: Detect Unauthorized Modification of PLC Logic

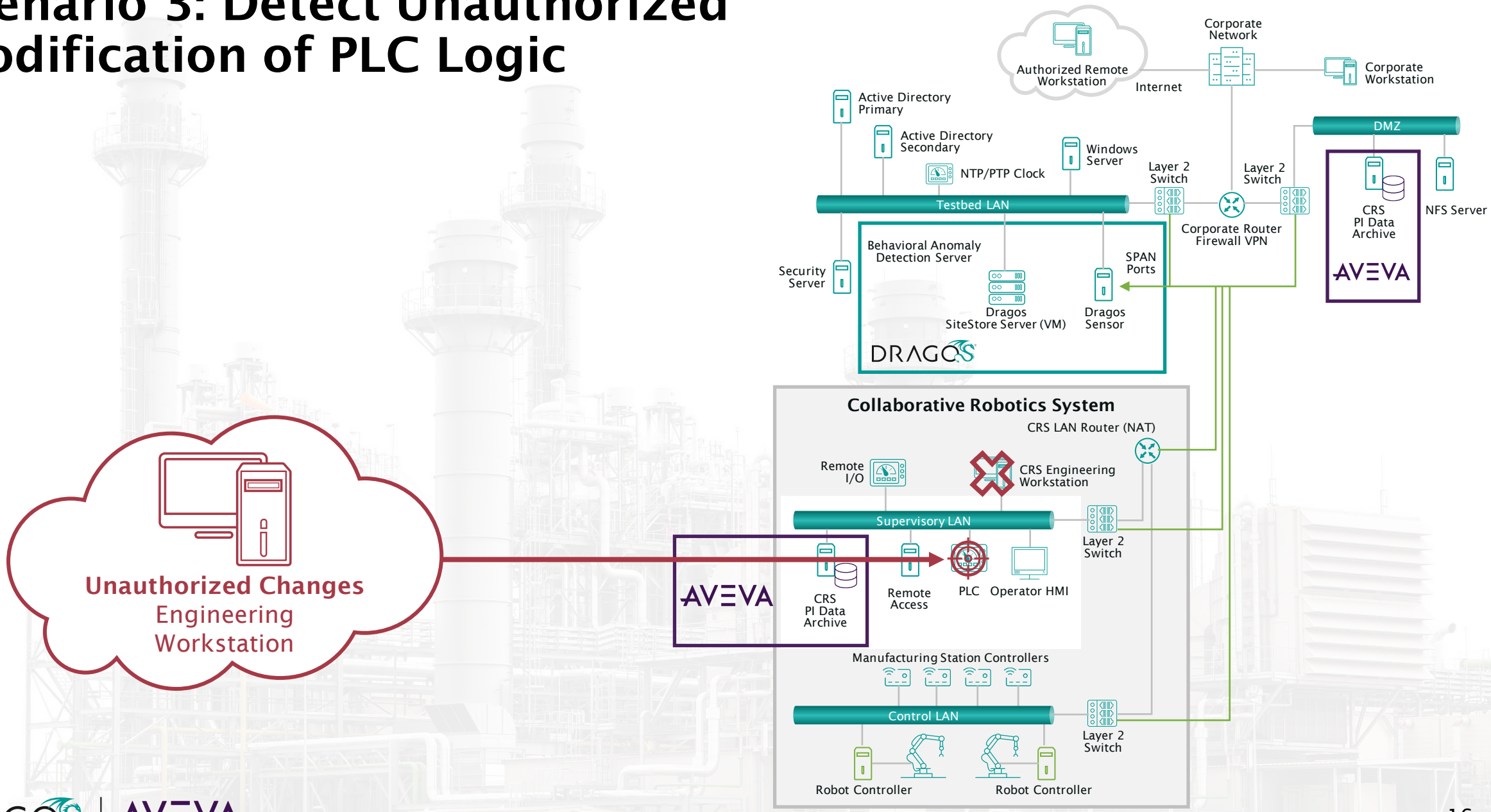
An authorized user performs an unapproved or unauthorized modification of the PLC logic from an engineering workstation.

Objective: Demonstrate the detection of PLC logic modification.

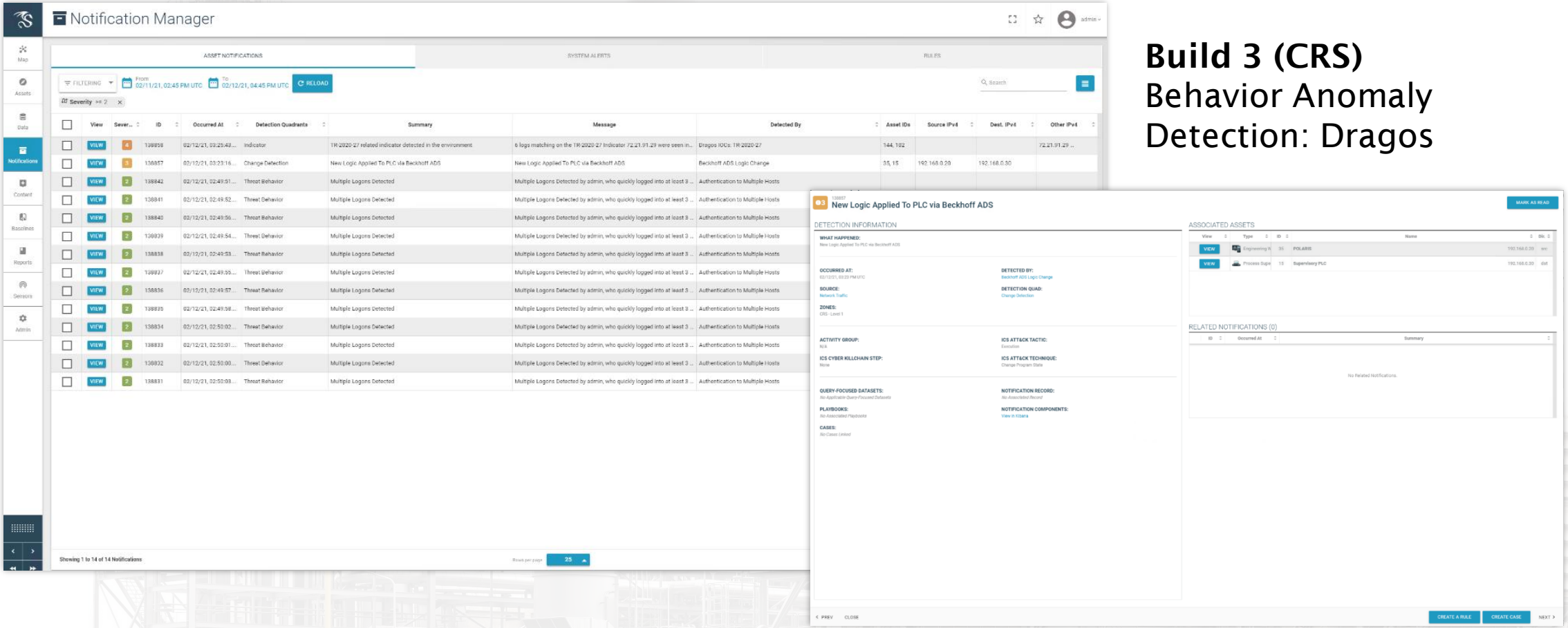
Test: The authorized user remotely connects to a manufacturing environment, modifies and downloads a logic file to the PLC.

Results: Ability to detect and alert on activity accessing the PLC.

Scenario 3: Detect Unauthorized Modification of PLC Logic

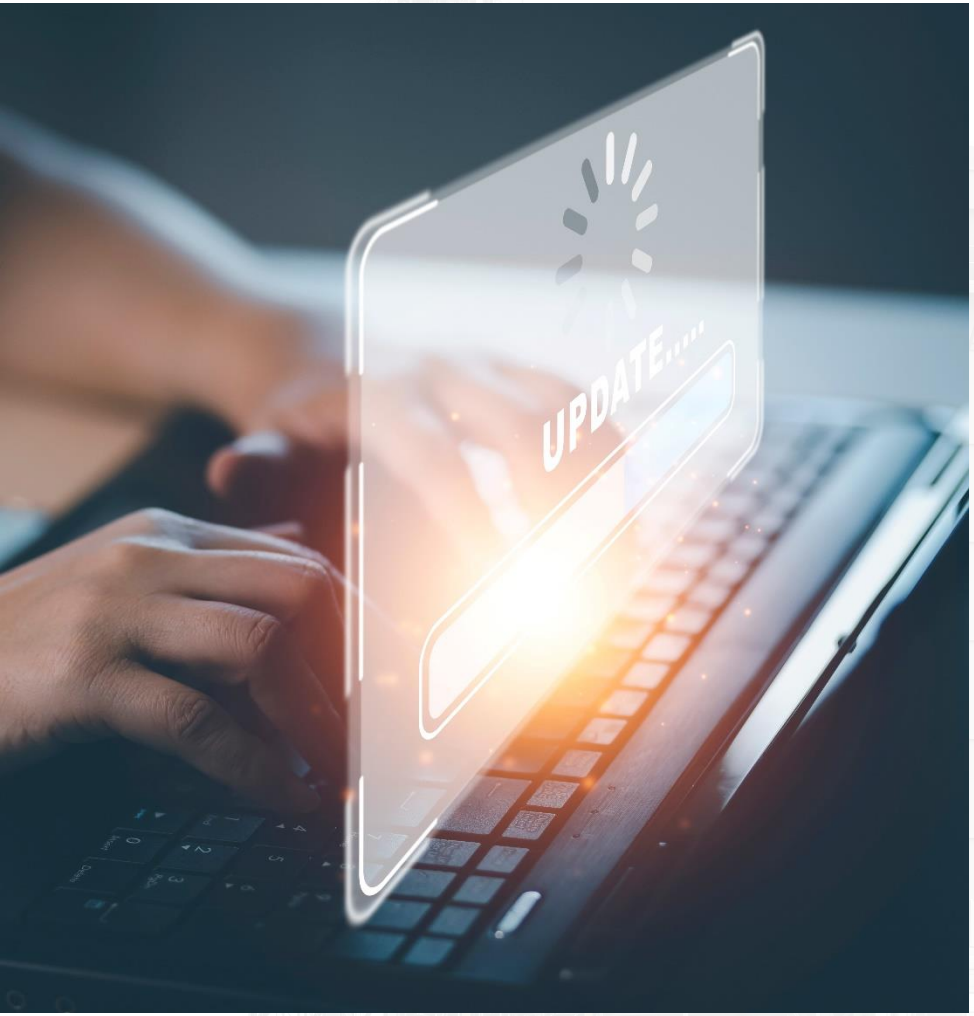


Behavior Anomaly Detection, CRS



Build 3 (CRS)
Behavior Anomaly Detection: Dragos

Scenario 4: Detect Unauthorized Firmware Modification



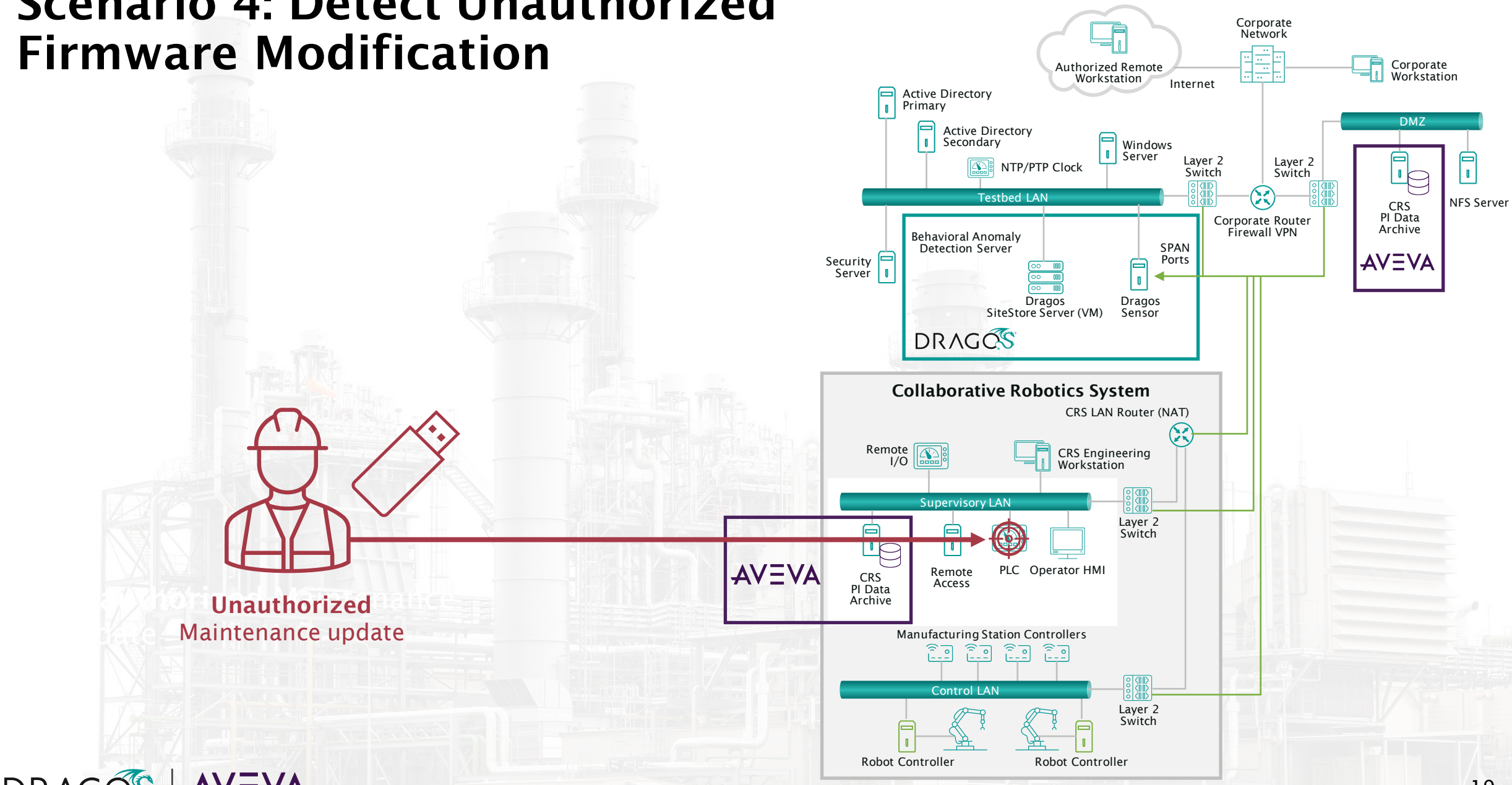
An authorized user performs a change of the firmware on a PLC.

Objective: Demonstrate the detection of device firmware modification.

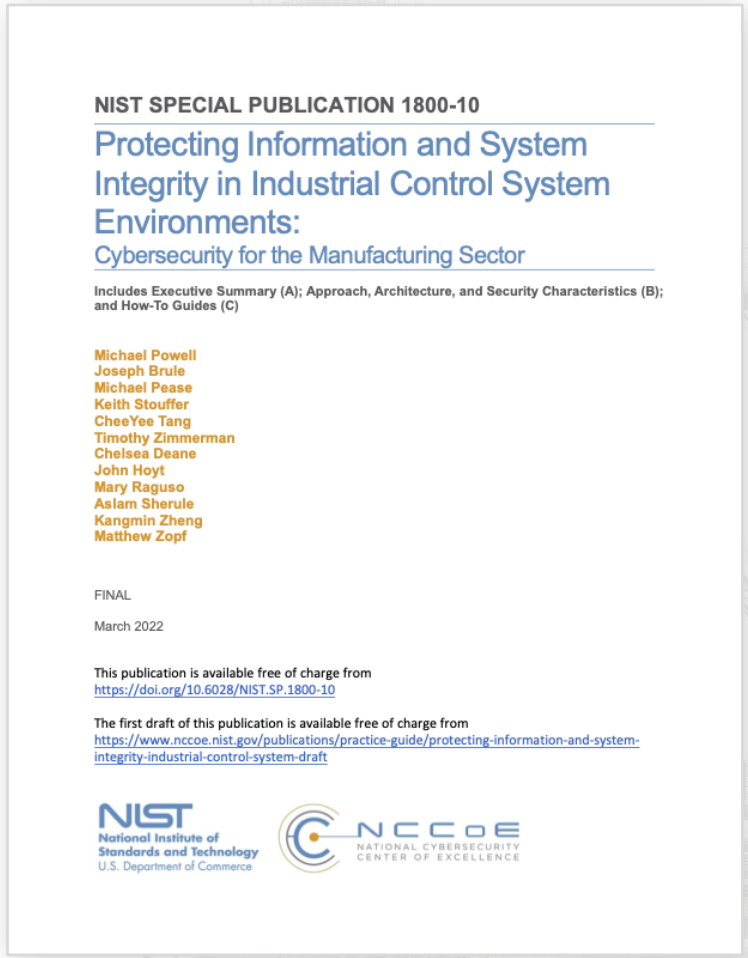
Test: An authorized user with local access to the PLC replaces the memory card containing the PLC Firmware with a memory card containing new firmware.

Results: Ability to detect behavioral anomalies and generate alerts for updates to PLC component firmware.

Scenario 4: Detect Unauthorized Firmware Modification



Summary – It Takes a Village Working Together



NIST SPECIAL PUBLICATION 1800-10

Protecting Information and System Integrity in Industrial Control System Environments:

Cybersecurity for the Manufacturing Sector

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Michael Powell
Joseph Brule
Michael Pease
Keith Stouffer
CheeYee Tang
Timothy Zimmerman
Chelsea Deane
John Hoyt
Mary Raguso
Aslam Sherule
Kangmin Zheng
Matthew Zopf

FINAL

March 2022

This publication is available free of charge from
https://doi.org/10.6028/NIST.SP.1800-10

The first draft of this publication is available free of charge from
https://www.nccoe.nist.gov/publications/practice-guide/protecting-information-and-system-integrity-industrial-control-system-draft

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Download NIST SPECIAL PUBLICATION 1800-10

- Technical solutions for maintaining system and information integrity
- Solutions mapped to NIST Cybersecurity Framework
- Example of the solutions that can be used in manufacturing environments

Available as a Complete Guide, Executive Summary and How-To Guides:

https://www.nccoe.nist.gov/manufacturing/protecting-information-and-system-integrity-industrial-control-system-environments

Next steps – Q&A

It takes a village – together, providing process data + cyber data with scalable best of breed integrated solution, to solve today's cybersecurity challenges.

New Project: Responding to and Recovering from a Cyber Attack

https://www.nccoe.nist.gov/manufacturing/responding-and-recovering-cyber-attack

https://www.aveva.com/

Using Bow Tie Risk Modeling for Industrial Cybersecurity: https://www.dragos.com/resource/using-bow-tie-risk-modeling-for-industrial-cybersecurity

5 Critical Controls for World-Class OT Cybersecurity: https://hub.dragos.com/guide/5-critical-controls

Thank you