



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/IloT) 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

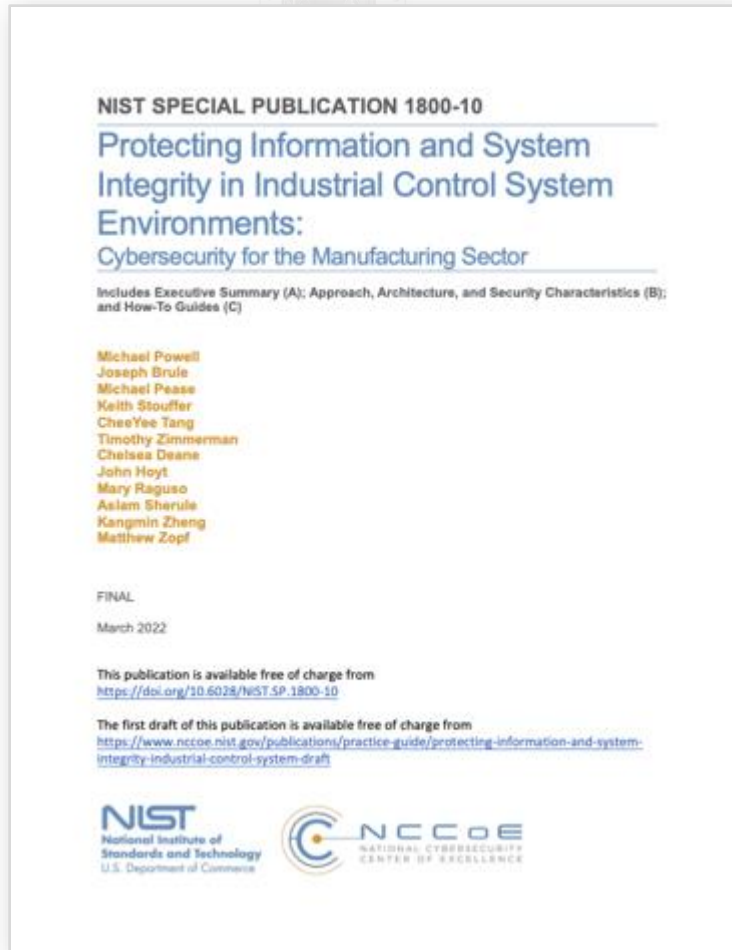
As part of the NIST family, the NCCoE has access to a foundation of expertise, resources, relationships, and experience.

Information Technology Laboratory

Applied Cybersecurity Division



Cybersecurity Best Practice Guide



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

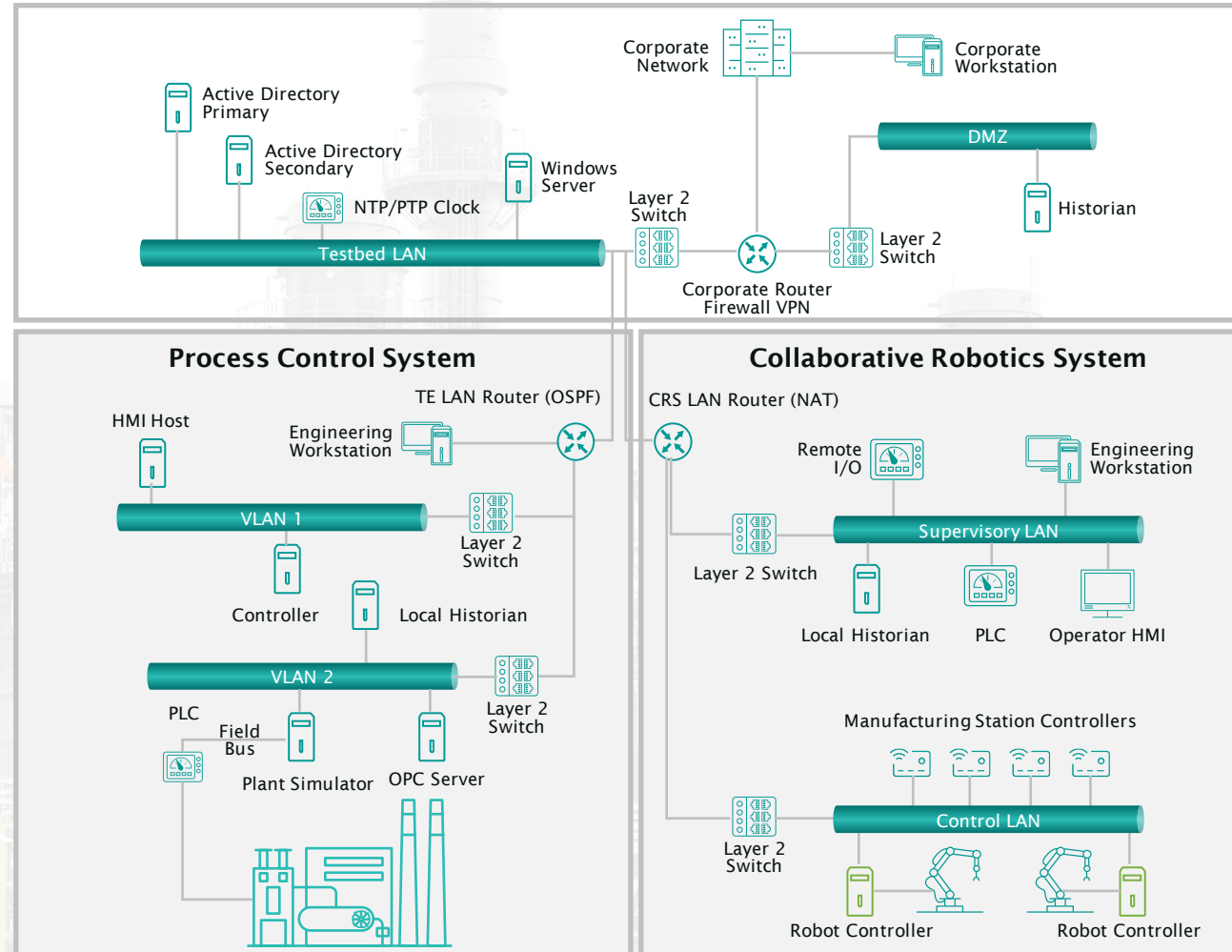
Detect Unauthorized Modification of PLC Logic

Scenario 4

Detect Unauthorized Firmware Modification

NIST Engineering Laboratory Testbed

Common Components

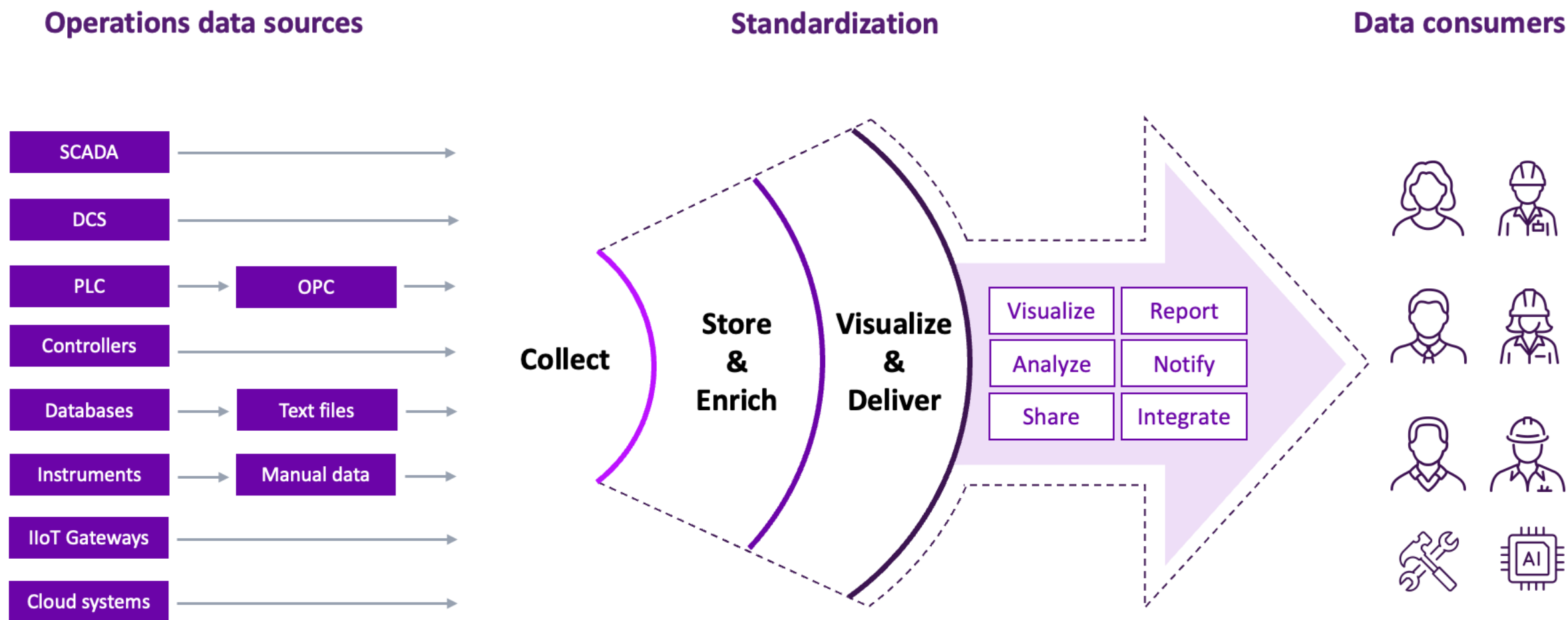


NISTIR 8089: An Industrial Control System Cybersecurity Performance Testbed,
<http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf>

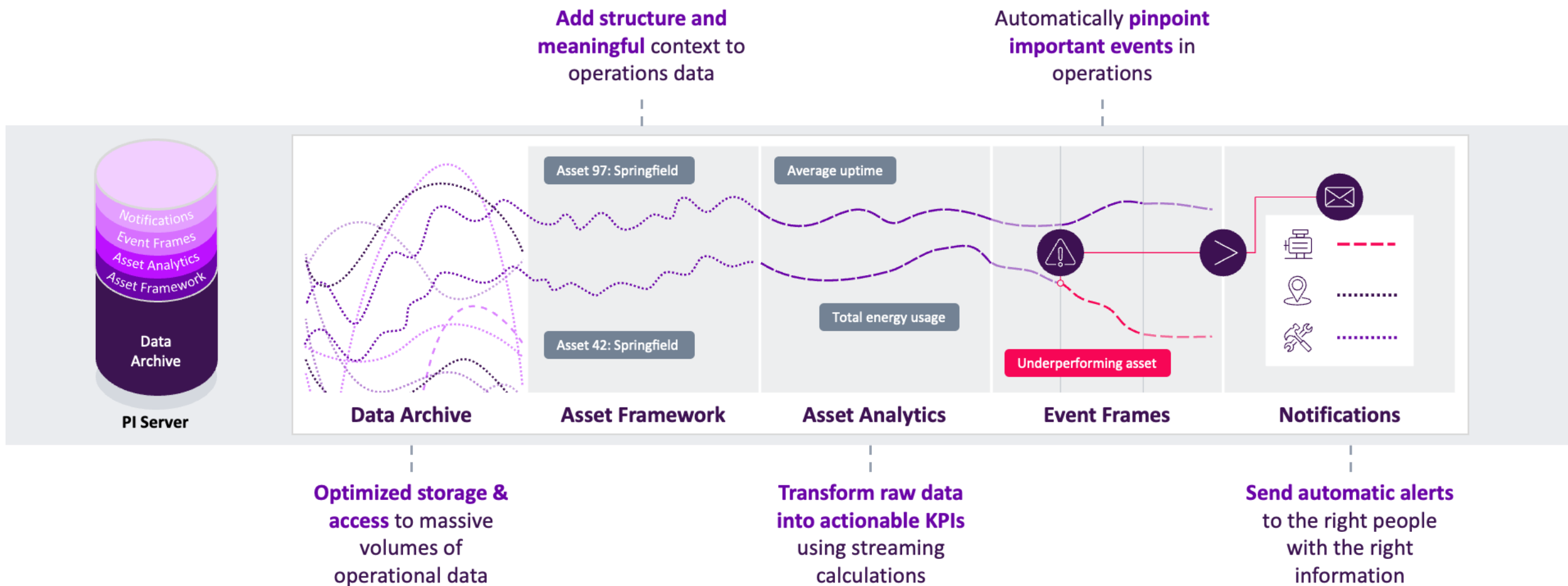
The Dragos Platform



AVEVA PI Server Provides Underlying Data Infrastructure



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



Scenario 1: Detect Unauthorized Device-to-Device Communications



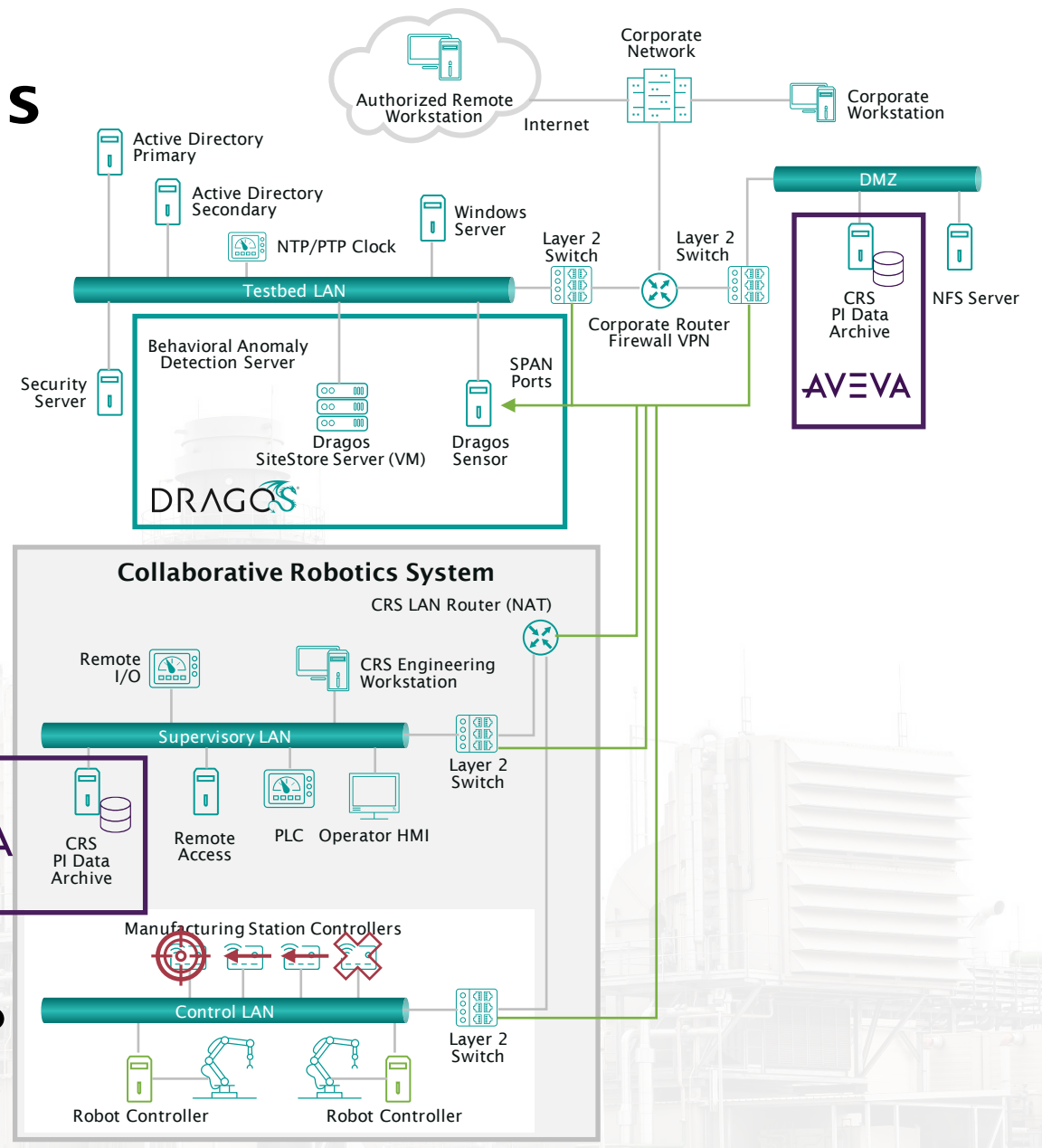
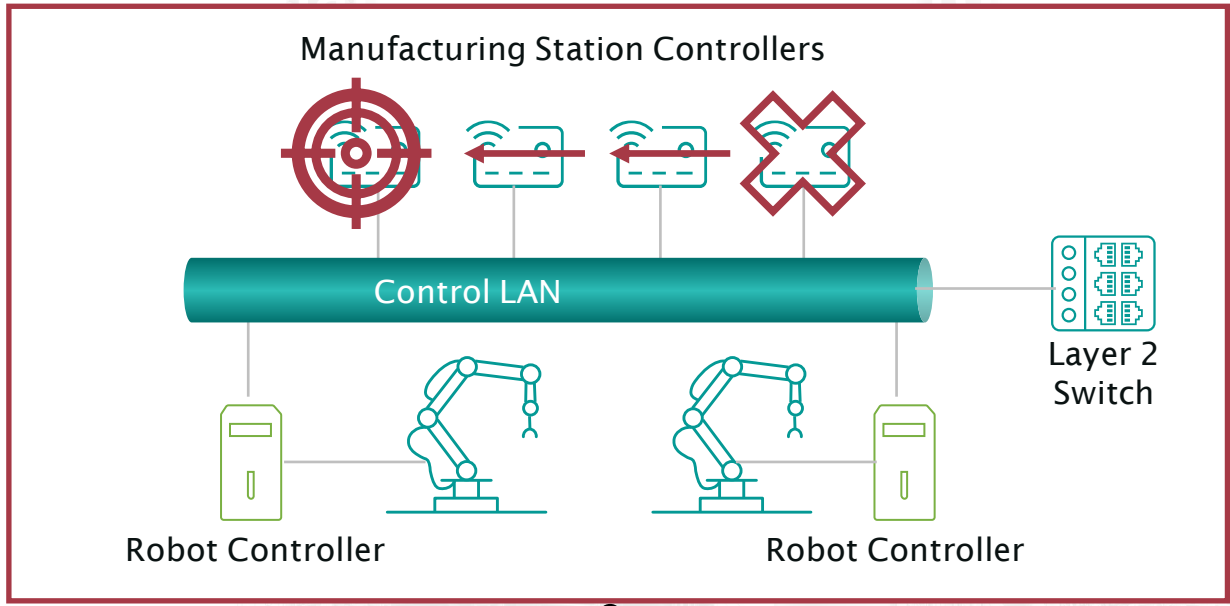
A device authorized to be on the network attempts to establish an unapproved connection.

Objective: Demonstrate the detection of unauthorized communications between devices.

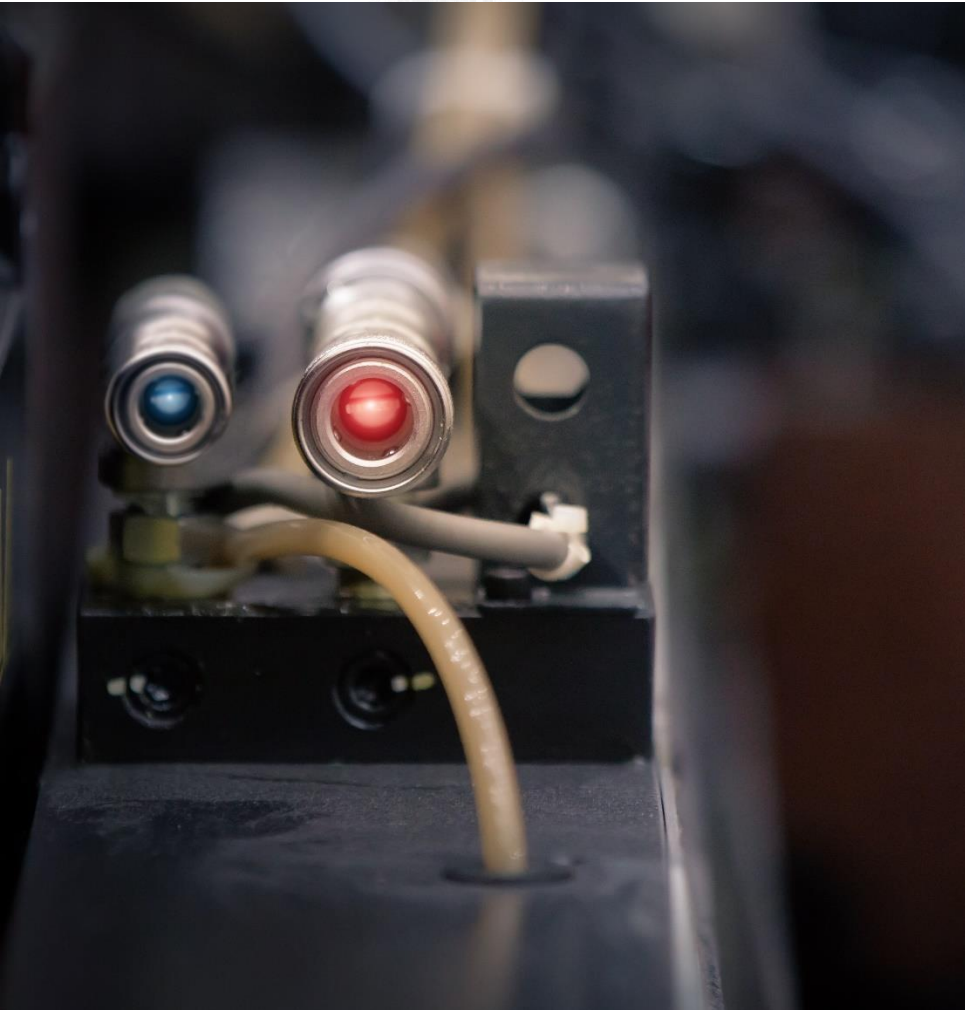
Test: The device attempts to establish an unapproved connection.

Results: Capture the suspicious traffic and generate an alert.

Scenario 1: Detect Unauthorized Device-to-Device Communications



Scenario 2: Detect Sensor Data Manipulation (PI)



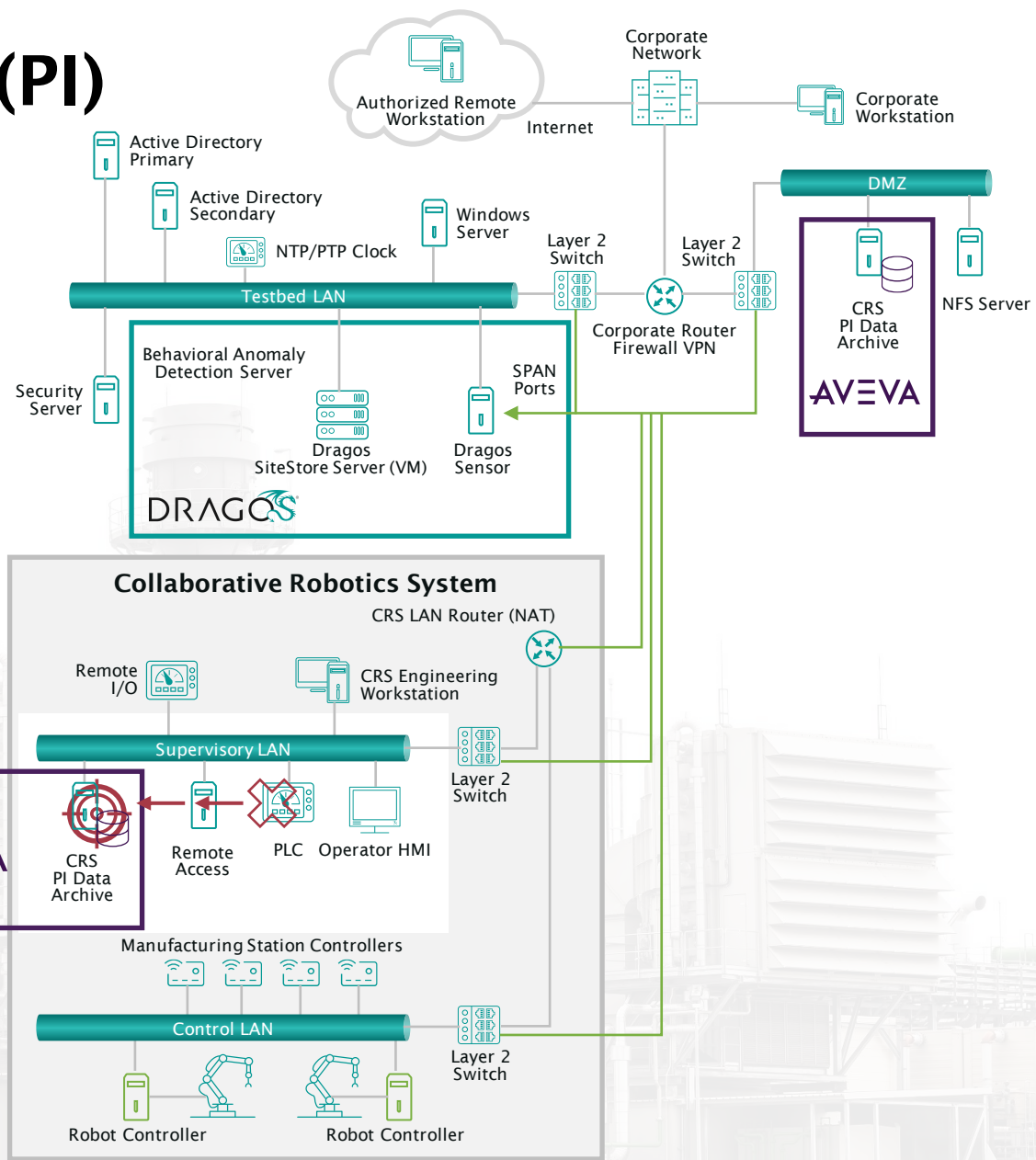
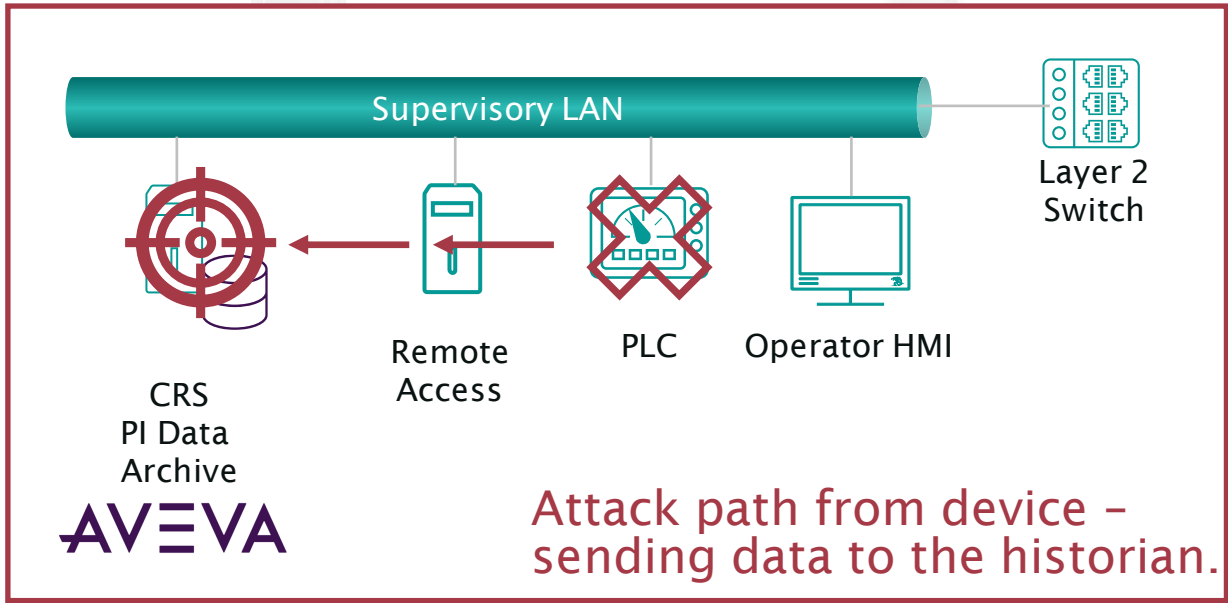
A sensor in the manufacturing system begins sending atypical data values to the historian.

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



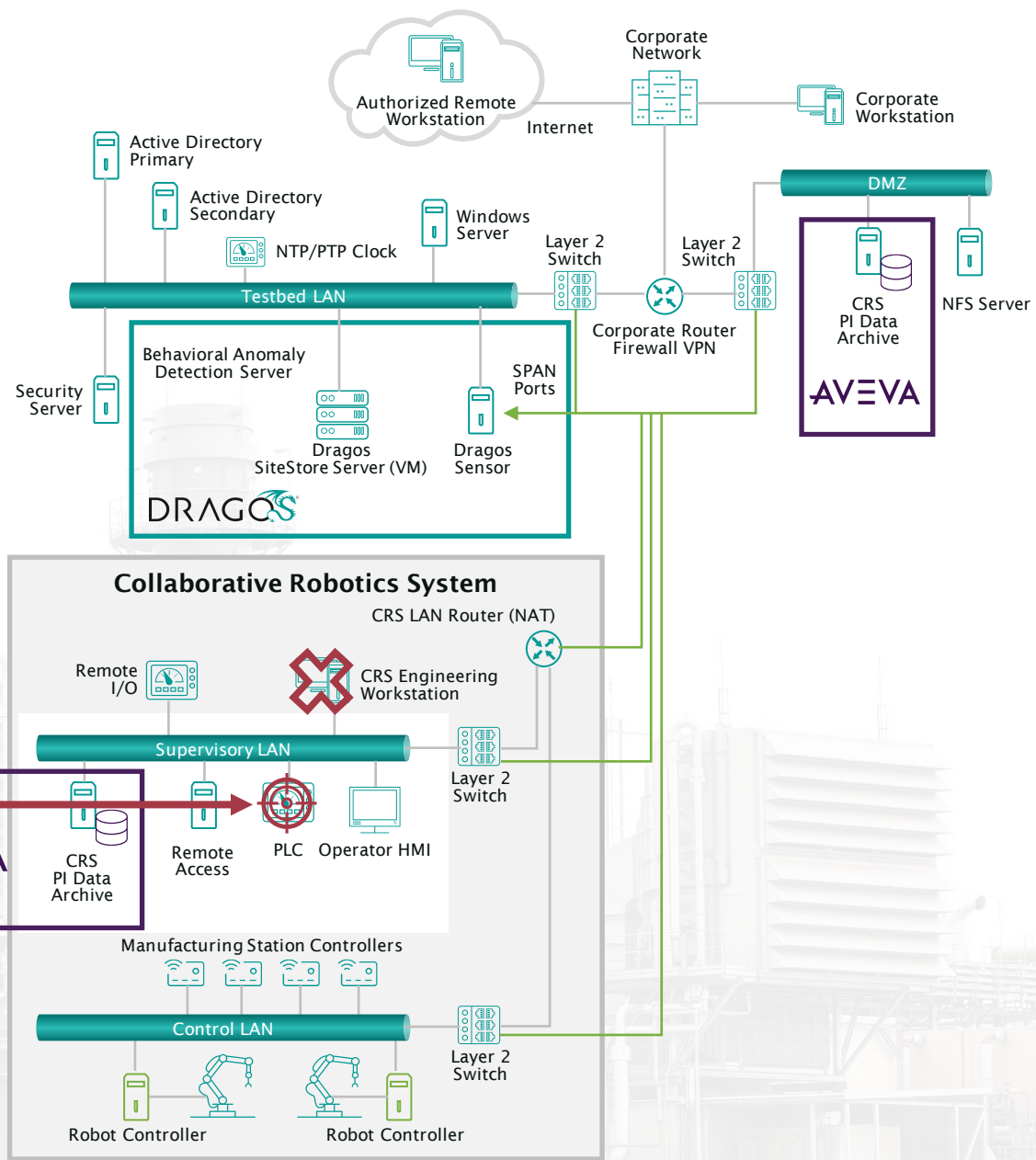
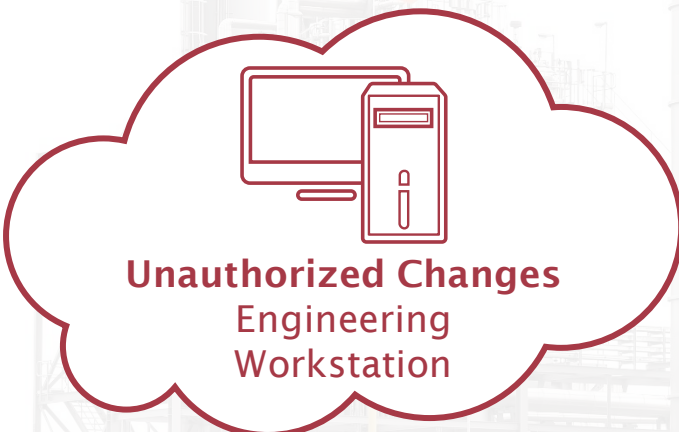
An authorized user performs an unapproved or unauthorized modification of the PLC logic from an engineering workstation.

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

Notification Manager

ASSET NOTIFICATIONS

Filtering: From 02/11/21, 02:45 PM UTC To 02/12/21, 04:45 PM UTC

Severity: 2

	View	Sever...	ID	Occurred At	Detection Quadrants	Summary	Message	Detected By	Asset IDs	Source IPv4	Dest. IPv4	Other IPv4
<input type="checkbox"/>	VIEW	4	138858	02/12/21, 02:25:43...	Indicator	1N-2020-27 related indicator detected in the environment	6 logs matching on the 1N-2020-27 Indicator /2.21.91.29 were seen in...	Dragos IOC: 1N-2020-27	144, 162			/2.21.91.29 ..
<input type="checkbox"/>	VIEW	3	138857	02/12/21, 03:23:16...	Change Detection	New Logic Applied To PLC via Beckhoff ADS	New Logic Applied To PLC via Beckhoff ADS	Beckhoff ADS Logic Change	35, 15	192.168.0.20	192.168.0.30	
<input type="checkbox"/>	VIEW	2	138842	02/12/21, 02:49:51...	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3 ...	Authentication to Multiple Hosts				
<input type="checkbox"/>	VIEW	2	138841	02/12/21, 02:49:52...	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3 ...	Authentication to Multiple Hosts				
<input type="checkbox"/>	VIEW	2	138840	02/12/21, 02:49:56...	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3 ...	Authentication to Multiple Hosts				
<input type="checkbox"/>	VIEW	2	138839	02/12/21, 02:49:54...	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3 ...	Authentication to Multiple Hosts				
<input type="checkbox"/>	VIEW	2	138838	02/12/21, 02:49:53...	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3 ...	Authentication to Multiple Hosts				
<input type="checkbox"/>	VIEW	2	138837	02/12/21, 02:49:55...	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3 ...	Authentication to Multiple Hosts				
<input type="checkbox"/>	VIEW	2	138836	02/12/21, 02:49:57...	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3 ...	Authentication to Multiple Hosts				
<input type="checkbox"/>	VIEW	2	138835	02/12/21, 02:49:58...	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3 ...	Authentication to Multiple Hosts				
<input type="checkbox"/>	VIEW	2	138834	02/12/21, 02:50:02...	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3 ...	Authentication to Multiple Hosts				
<input type="checkbox"/>	VIEW	2	138833	02/12/21, 02:50:01...	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3 ...	Authentication to Multiple Hosts				
<input type="checkbox"/>	VIEW	2	138832	02/12/21, 02:50:00...	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3 ...	Authentication to Multiple Hosts				
<input type="checkbox"/>	VIEW	2	138831	02/12/21, 02:50:03...	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3 ...	Authentication to Multiple Hosts				

Showing 1 to 14 of 14 Notifications

Build 3 (CRS) Behavior Anomaly Detection: Dragos

03 New Logic Applied To PLC via Beckhoff ADS

DETECTION INFORMATION

WHAT HAPPENED:
New Logic Applied To PLC via Beckhoff ADS

OCURRED AT:
02/12/21, 02:25 PM UTC

SOURCE:
Network Traffic

ZONES:
CRS - Level 1

ACTIVITY GROUP:
N/A

ICS CYBER KILLCHAIN STEP:
None

QUERY-FOCUSED DATASETS:
No Associated Query-Focused Datasets

PLAYBOOKS:
No Associated Playbooks

CASES:
No Cases Linked

DETECTED BY:
Beckhoff ADS Logic Change

DETECTION QUAD:
Change Detection

ICS ATTACK TACTIC:
Execution

ICS ATTACK TECHNIQUE:
Change Program State

NOTIFICATION RECORD:
No Associated Record

NOTIFICATION COMPONENTS:
None (0)

ASSOCIATED ASSETS

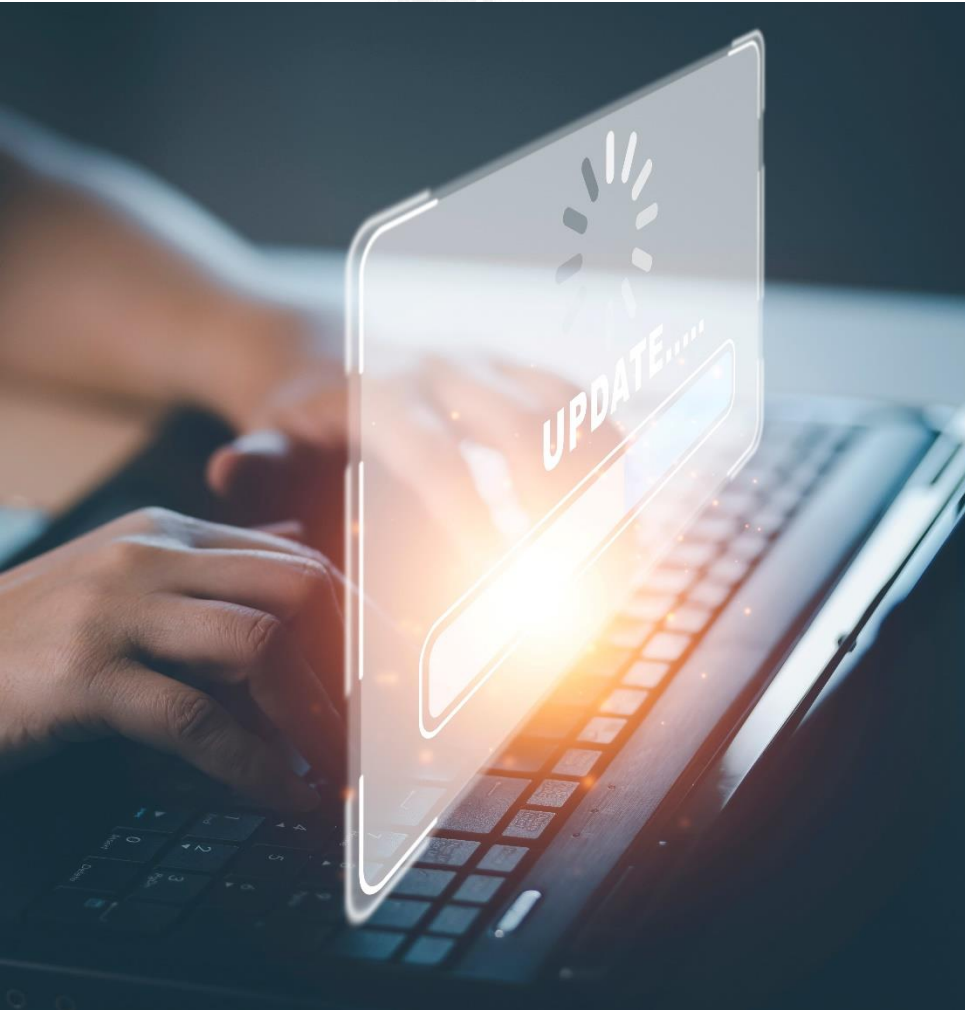
View	Type	ID	Name	IP	OS
VIEW	Engineering PC	35	PLC-ARM	192.168.0.30	WIN
VIEW	Process Digital	15	Supervisory PLC	192.168.0.20	WIN

RELATED NOTIFICATIONS (0)

ID	Occurred At	Summary
No Related Notifications		

CREATE A RULE CREATE CASE NEXT

Scenario 4: Detect Unauthorized Firmware Modification



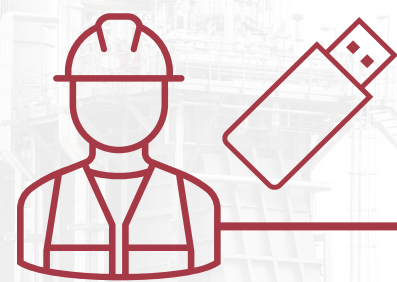
An authorized user performs a change of the firmware on a PLC.

Objective: Demonstrate the detection of device firmware modification.

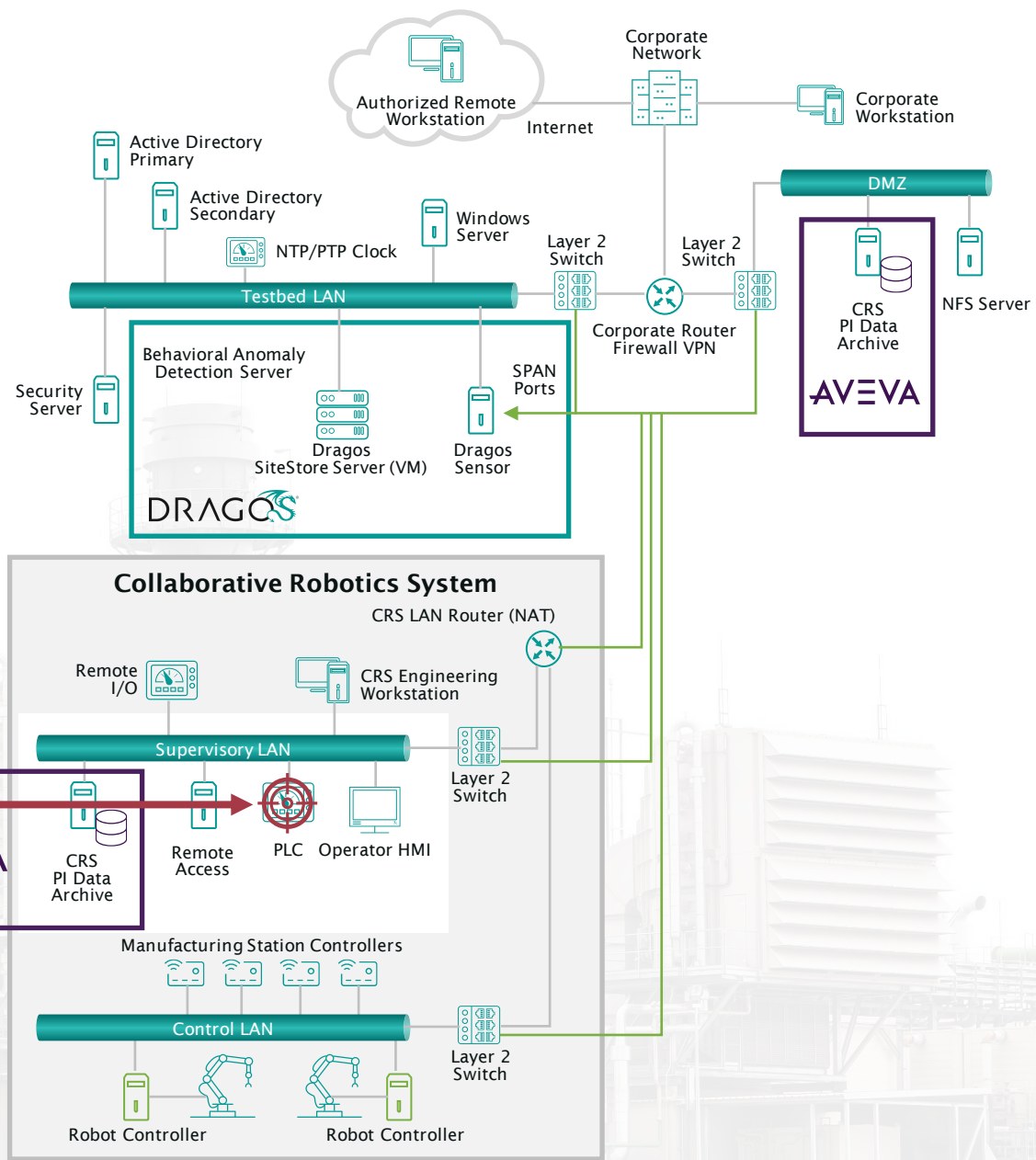
Test: An authorized user with local access to the PLC replaces the memory card containing the PLC Firmware with a memory card containing new firmware.

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

Scenario 4: Detect Unauthorized Firmware Modification



Unauthorized Maintenance update



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>



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