Agenda

• NCCoE Overview

• Introduction of Manufacturing Team

• Previous Manufacturing Project

• New Project: Detecting and Protecting Against Data Integrity Attacks in Industrial Control Systems Environments Project Description

• Questions/Comments
### NCCoE Manufacturing Team: Contacts / Roles

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
<th>Role</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Michael Powell</td>
<td>NIST/NCCoE</td>
<td>Principle Investigator</td>
<td><a href="mailto:Michael.Powell@NIST.gov">Michael.Powell@NIST.gov</a></td>
</tr>
<tr>
<td>Keith Stouffer</td>
<td>NIST</td>
<td>Principle Investigator</td>
<td><a href="mailto:Keith.Stouffer@NIST.gov">Keith.Stouffer@NIST.gov</a></td>
</tr>
<tr>
<td>Jim McCarthy</td>
<td>NIST/NCCoE</td>
<td>Senior Engineer</td>
<td><a href="mailto:James.McCarthy@NIST.gov">James.McCarthy@NIST.gov</a></td>
</tr>
<tr>
<td>CheeYee Tang</td>
<td>NIST</td>
<td>Project Engineer</td>
<td><a href="mailto:Cheeyee.Tang@NIST.gov">Cheeyee.Tang@NIST.gov</a></td>
</tr>
<tr>
<td>Timothy Zimmerman</td>
<td>NIST</td>
<td>Project Engineer</td>
<td><a href="mailto:Timothy.Zimmerman@NIST.gov">Timothy.Zimmerman@NIST.gov</a></td>
</tr>
<tr>
<td>Titilayo Ogunyale</td>
<td>MITRE/NCCoE</td>
<td>Project Lead</td>
<td><a href="mailto:TOgunyale@MITRE.org">TOgunyale@MITRE.org</a></td>
</tr>
<tr>
<td>Lura Danley</td>
<td>MITRE/NCCoE</td>
<td>Lead Social Scientist</td>
<td><a href="mailto:LDanley@MITRE.org">LDanley@MITRE.org</a></td>
</tr>
<tr>
<td>Lauren Acierto</td>
<td>MITRE/NCCoE</td>
<td>Outreach &amp; Engagement</td>
<td><a href="mailto:LAcierto@MITRE.org">LAcierto@MITRE.org</a></td>
</tr>
</tbody>
</table>
Mission

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs
NCCoE Tenets

**Standards-based**
Apply relevant industry standards to each security implementation; demonstrate example solutions for new standards

**Modular**
Develop components that can be easily substituted with alternates that offer equivalent input-output specifications

**Repeatable**
Provide a detailed practice guide including a reference design, list of components, configuration files, relevant code, diagrams, tutorials, and instructions to enable system admins to recreate the example solution and achieve the same results

**Commercially available**
Work with the technology community to identify commercially available products that can be brought together in example solutions to address challenges identified by industry

**Usable**
Design blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

**Open and transparent**
Use open and transparent processes to complete work; seek and incorporate public comments on NCCoE publications
Manufacturing Projects

Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection

• nccoe.nist.gov/nistir-8219

Detecting and Protecting Against Data Integrity Attacks in Industrial Control System Environments

• nccoe.nist.gov/ics-integrity
NISTIR 8219
Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection

• **Project focus:**
  - demonstrate behavioral anomaly detection techniques that businesses can implement and use to strengthen the cybersecurity of their manufacturing processes.

• **Three detection methods:**
  - network-based
  - agent-based
  - operational historian/sensor-based
NISTIR 8219 Build Team

CyberX

OSIsoft

FORESCOUT

SECUREnOK

National Cybersecurity Center of Excellence
nccoe.nist.gov

8
New Project: Detecting and Protecting Against Data Integrity Attacks in Industrial Control Systems (ICS) Environments

Project Focus:
• Provide a comprehensive approach that manufacturing organizations can use to address the challenge of protecting and detecting against data integrity attacks

Project Scope:
• Provide a proposed approach to prevent, mitigate, and detect threats from cyberattacks or insider threats within a manufacturing ICS environment
• Demonstrate how the commercially available technologies deployed in this build provide cybersecurity capabilities that manufacturing organizations can use to secure their operational technology (OT) systems
Cybersecurity Capabilities in New Project

Detecting and Protecting Against Data Integrity Attacks in ICS Environments

- behavioral anomaly detection
- security incident and event monitoring
- ICS application whitelisting
- malware detection and mitigation
- change control management
- user authentication and authorization
- access control least privilege
- file integrity checking mechanisms
Multiple Capabilities in Two Manufacturing Demo Environments
Detecting and Protecting Against Data Integrity Attacks in ICS Environments
Project Execution Timeline

Detecting and Protecting Against Data Integrity Attacks in ICS Environments

**DESCRIBE**
- Publish the NCCoE project description

**FORM TEAM**
- Form the team and complete the FRN, LOI, and CRADA

**DESIGN**
- Design and engineer the architecture and usage scenarios taking into consideration resources

**BUILD PLAN**
- Develop the execution plan for building the demonstration based on the design

**BUILD**
- Compose, build the demonstration, and perform security functional tests

**DOCUMENT**
- Develop the practice guide to publish as a public draft and final document

**OUTREACH**
- Present at public events and interact with community of interest

**Project Execution Timeline**

- **Q4 FY 2019**: Q4 FY 2019
- **Q1 FY 2020**: Q1 FY 2020
- **Q1 / Q2 FY 2020**: Q1 / Q2 FY 2020
- **Q2 FY 2020 / Q3 FY 2020**: Q2 FY 2020 / Q3 FY 2020
- **Q3 / Q4 FY 2020**: Q3 / Q4 FY 2020
- **Q4 FY 2020**: Q4 FY 2020
Next Steps

Detecting and Protecting Against Data Integrity Attacks in ICS Environments

Comment on the new Project Description:

- Submit comments online or via email to manufacturing_nccoe@nist.gov.
- Public comment period ends July 25th

Stay tuned for a call for collaborators via a Federal Register Notice (FRN):

- Look out for email from us announcing FRN
- Check status on project webpage:
  - nccoe.nist.gov/ics-integrity
We Value Your Feedback

Do you:

• Have a success story from using one of our guides?
• Have comments/feedback regarding our guidance?
• Have an idea that you think the NCCoE should pursue?
• Know of an event where NCCoE should present?

Please engage with us: manufacturing_nccoe@nist.gov
Contact Us

Michael Powell, Principle Investigator
Manufacturing Sector Lead
Michael.Powell@NIST.gov
301-975-0310

Titilayo Ogunyale
Project Lead
TOgunyale@MITRE.org
301-975-0219

http://nccoe.nist.gov
301-975-0200
nccoe@nist.gov