

Validating the Integrity of Computing Devices

Cybersecurity & Information Systems Information Analysis Center (CSIAC) Webinar

Speakers:

Nakia Grayson – National Institute of Standards and Technology (NIST)

Chris Brown – The MITRE Corporation

Date: **May 23, 2024**

Agenda

- 1) Introduction/National Cybersecurity Center of Excellence (NCCoE) Overview**
- 2) Project Overview**
- 3) Reference Architecture**
- 4) Project Scenarios**
- 5) Industry Collaboration**
- 6) 1800-Series Publication**
- 7) Closing**

Who We Are

A **solution-driven, collaborative** hub addressing complex cybersecurity problems



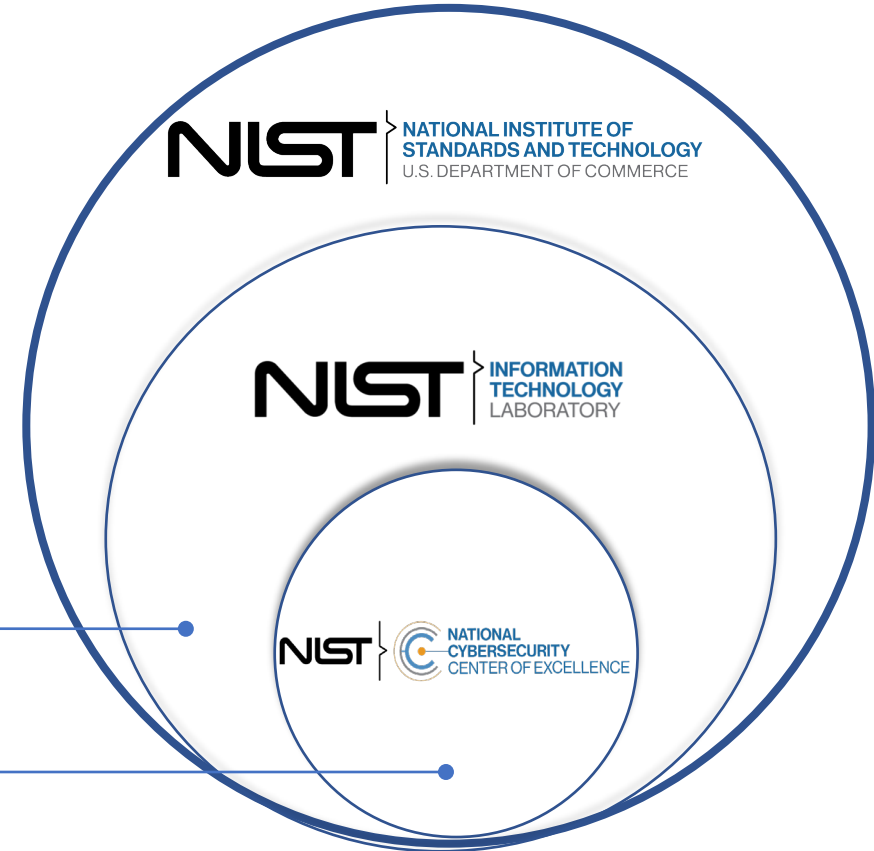
Who We Are

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

NIST is a **nonregulatory** agency. Our guidance is **voluntary**.

Information Technology Laboratory

Applied Cybersecurity Division



A man and a woman are sitting at a desk in a dimly lit room, looking at a computer monitor. The man is pointing at the screen, and the woman is looking at it with interest. The room has a textured wall and a desk lamp. The image is partially obscured by a dark blue curved overlay on the right side.

What We Do

We collaborate to develop modular, repeatable, applied cybersecurity architectures using:

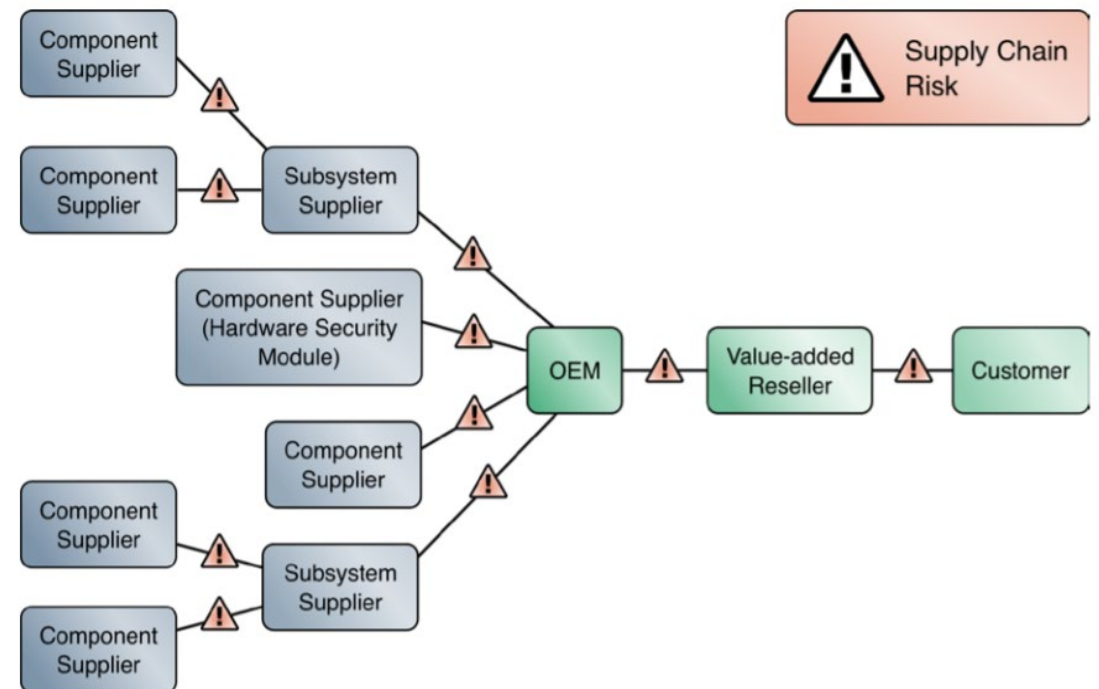
- ➔ Existing standards
- ➔ Existing guidance
- ➔ Commercially available technologies

Project Challenge

Organizations today face the challenge of identifying trustworthy products due to increased risk resulting from compromises in cyber supply chains.

Problems:

- Counterfeit products
- Substituted components
- Malware in system firmware/software
- Accountability/traceability in the supply chain



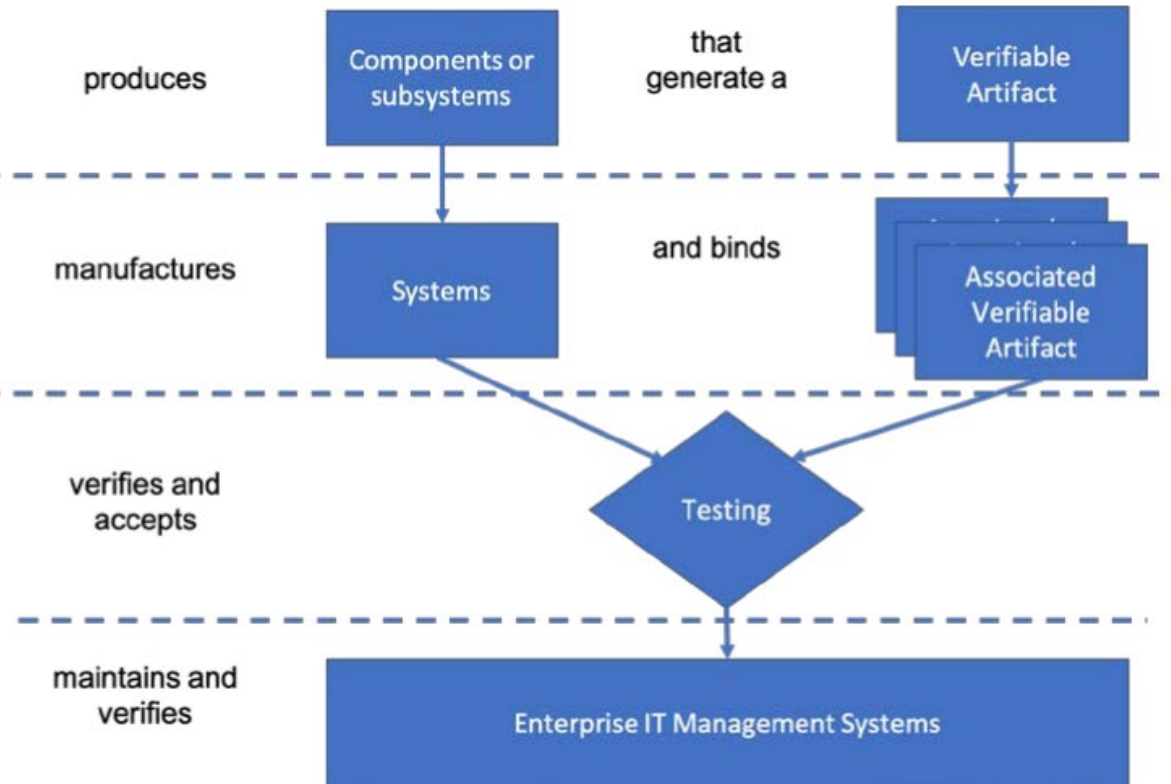
- Demonstrate scalable techniques to verify provenance and integrity of platform components throughout the device's life cycle
 - **Scenario 1: Creation of Manufacturing Artifacts**
Identify useful artifacts that can be generated in the manufacturing process
 - **Scenario 2: Verification of Components During Acceptance Testing**
Verify platform attributes and components using those artifacts during acceptance testing
 - **Scenario 3: Verification of Components During Use**
Monitor and verify platform attributes during operational use of the device
- Use commercially available technologies to address supply chain processes involving original equipment manufacturers (OEMs), platform integrators, information technology departments, and customers at subsequent stages in the system's life cycle of a purchased computing device

Project Architecture

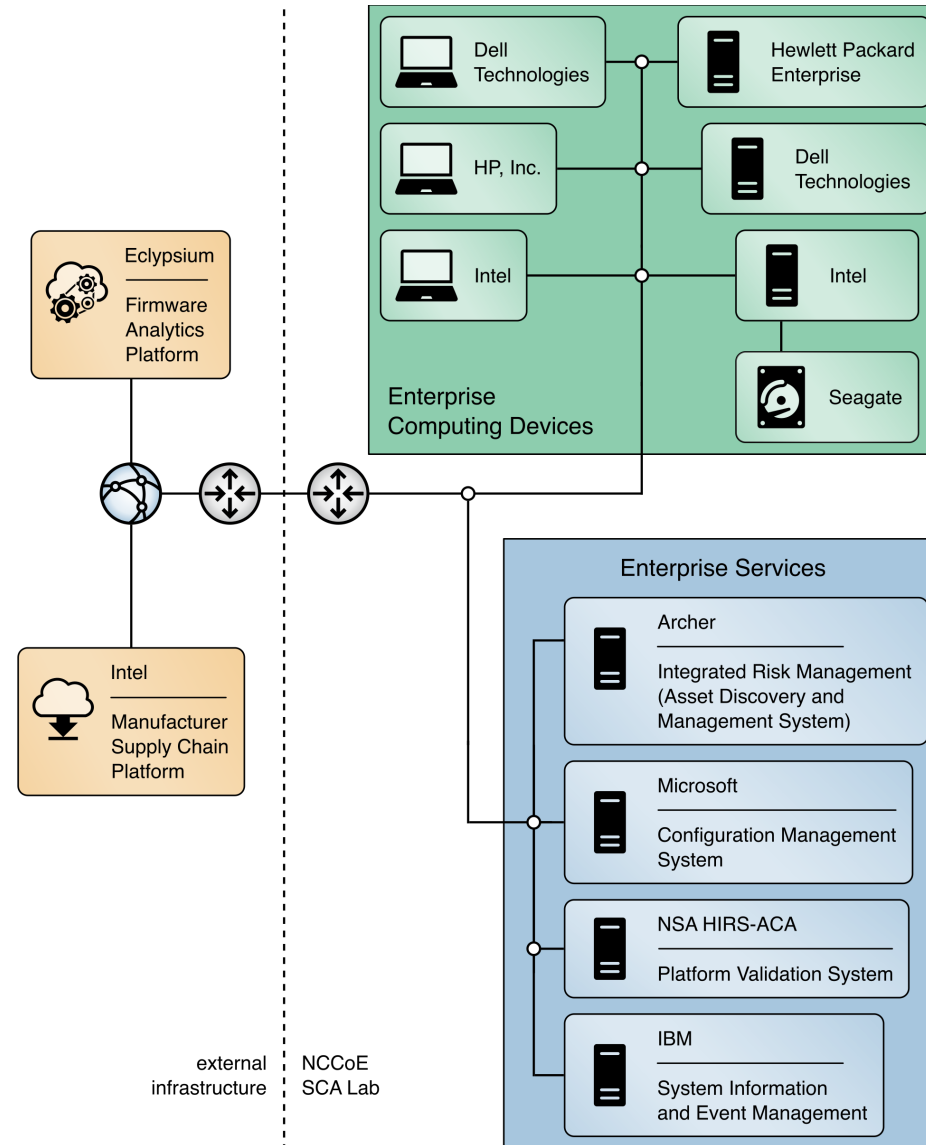
Collaborating Vendors



Enterprise Customer

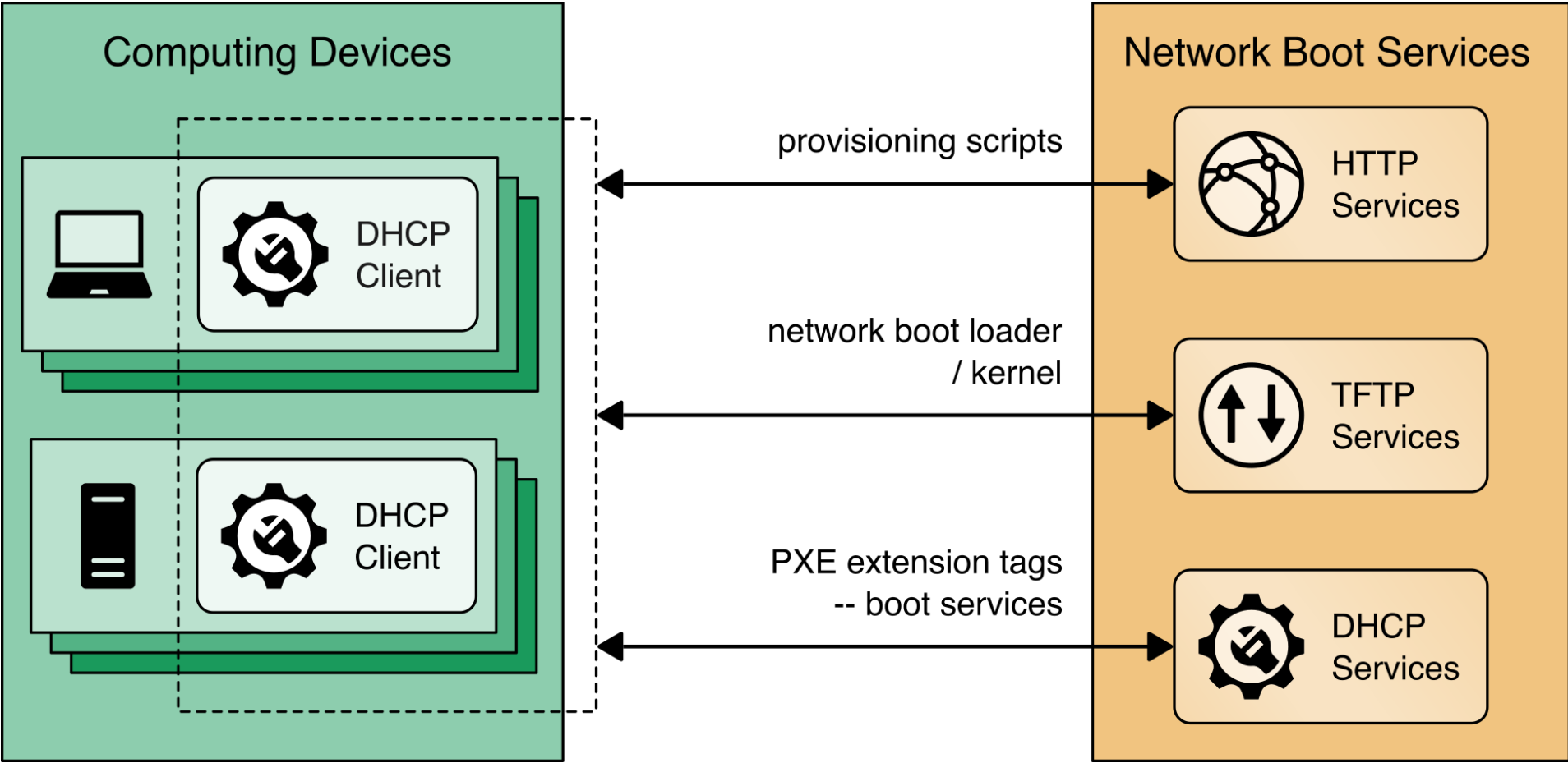


Project Architecture

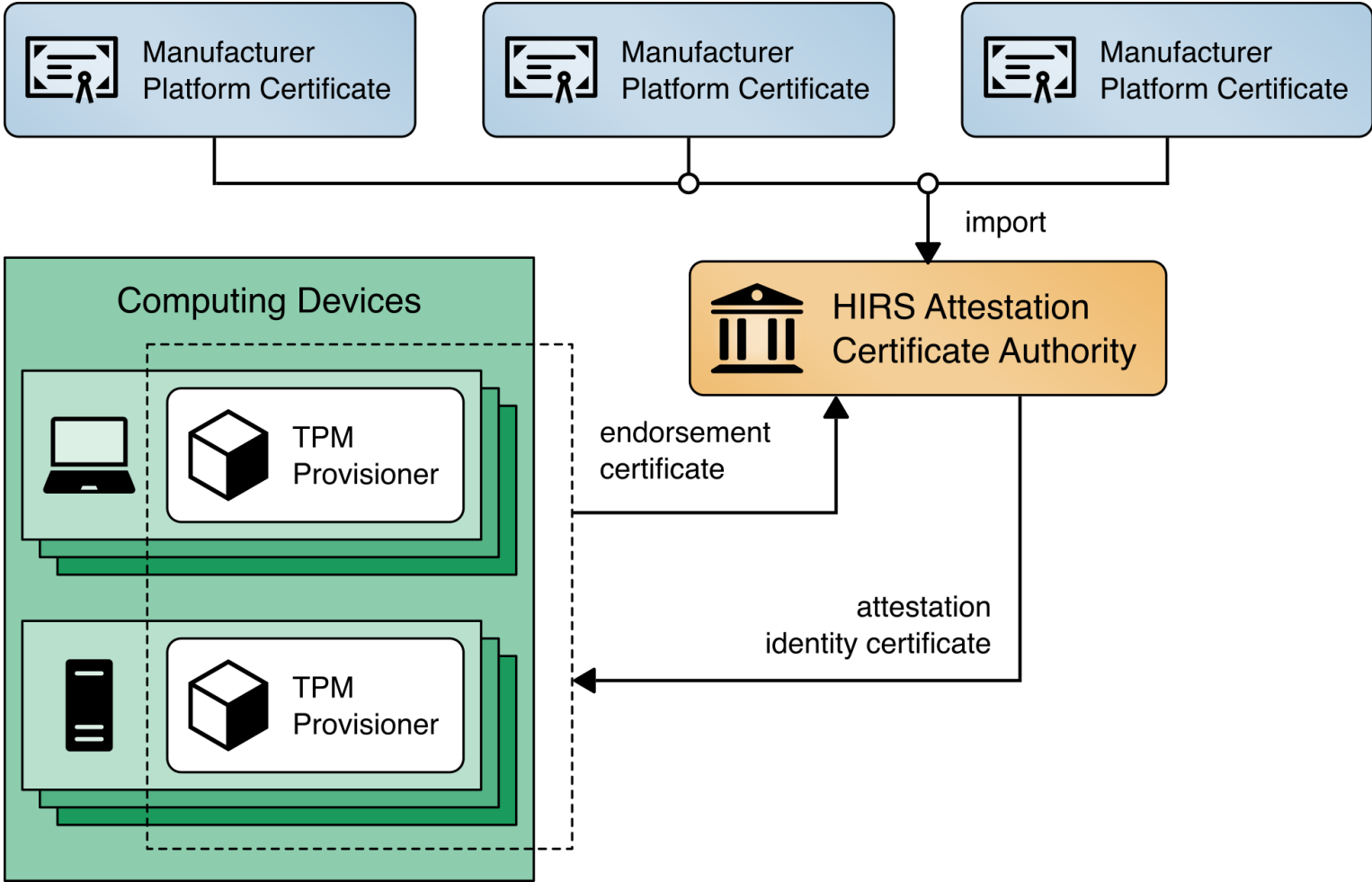


- Demonstrate scalable techniques to verify provenance and integrity of platform components throughout the device's life cycle
 - **Scenario 1: Creation of Manufacturing Artifacts**
Identify useful artifacts that can be generated in the manufacturing process
 - **Scenario 2: Verification of Components During Acceptance Testing**
Verify platform attributes and components using those artifacts during acceptance testing
 - **Scenario 3: Verification of Components During Use**
Monitor and verify platform attributes during operational use of the device
- Use commercially available technologies to address supply chain processes involving OEMs, platform integrators, information technology departments, and customers at subsequent stages in the system's life cycle of a purchased computing device

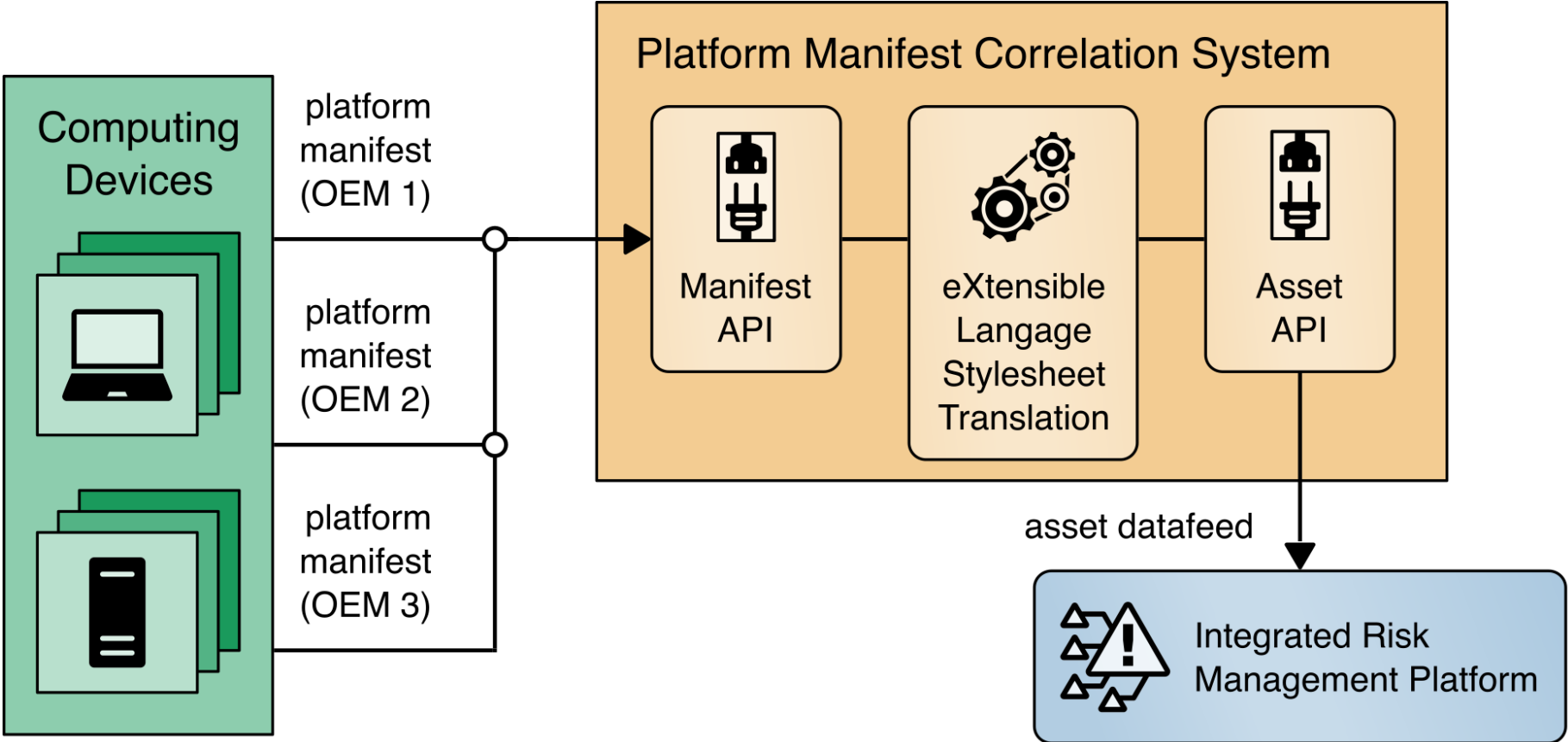
Scenario 2



Scenario 2



Scenario 2



Scenario 2 - Dashboard

Browser address bar: nccoe.supplychain-dashboard.example


GENERAL INFORMATION

Enterprise Unique Identifier: 00787415-1181-e411-906e-0012795d96dd **Serial Number:** 4734A10C

Platform Model: S2600WTT **Manufacturer:** Intel Corporation

Continuous Monitoring Platform Integrity Status: No Data from Configuration Management System

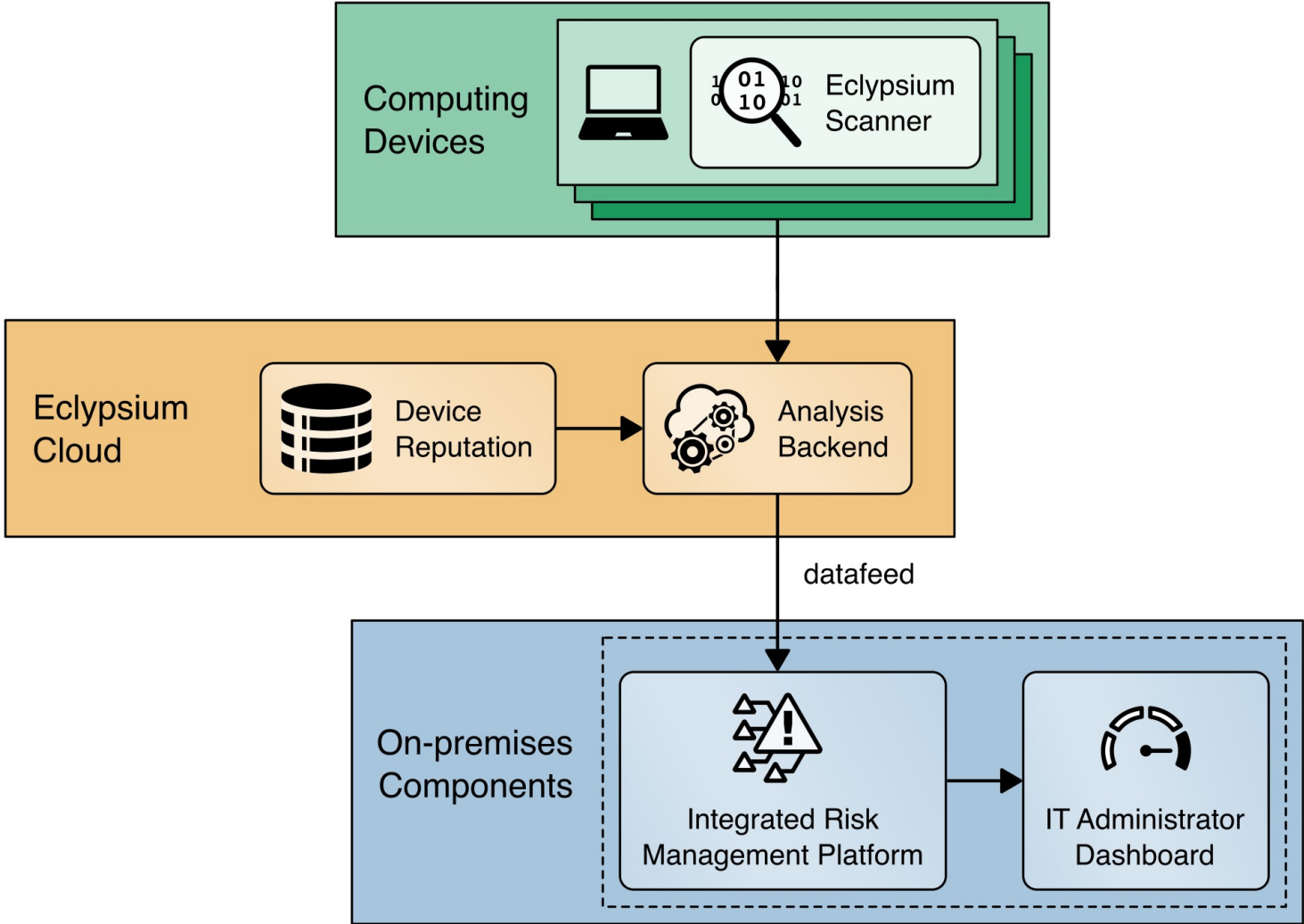
ASSOCIATED COMPONENTS [View Less](#)

 This section displays the computing device declared components.

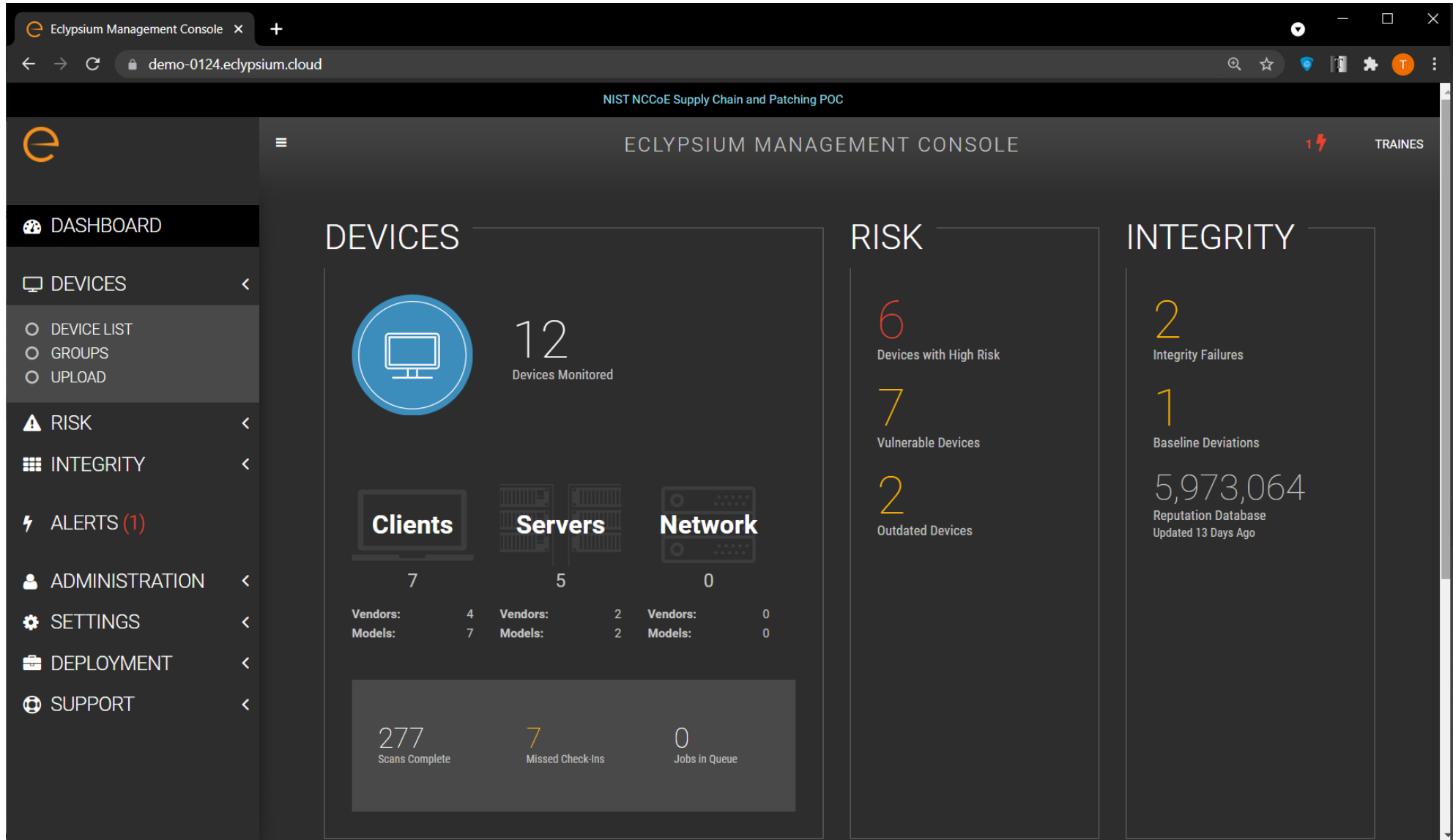
Tracking ID	Class	Manufacturer	Model	Serial
277286	Baseboard	Intel Corporation	S2600WTT	BQWL51650568
277287	CPU	Intel(R) Corporation	Central Processor	F2060300FFFBEBBF
277288	Memory	Micron	DDR4	0F663371
277290	Storage Drive	SEAGATE	ST18000NM005J	ZR5056HD0000C107GP5G
277291	Storage Drive	SEAGATE	ST18000NM005J	ZR5056GS0000C105D6S3
277292	Storage Drive	SEAGATE	ST18000NM005J	ZR504Z6W0000C105972J
277293	Trusted Platform Module	IFX	SLB9665	4734A10C

- Demonstrate scalable techniques to verify provenance and integrity of platform components throughout the device's life cycle
 - **Scenario 1: Creation of Manufacturing Artifacts**
Identify useful artifacts that can be generated in the manufacturing process
 - **Scenario 2: Verification of Components During Acceptance Testing**
Verify platform attributes and components using those artifacts during acceptance testing
 - **Scenario 3: Verification of Components During Use**
Monitor and verify platform attributes during operational use of the device
- Use commercially available technologies to address supply chain processes involving OEMs, platform integrators, information technology departments, and customers at subsequent stages in the system's life cycle of a purchased computing device

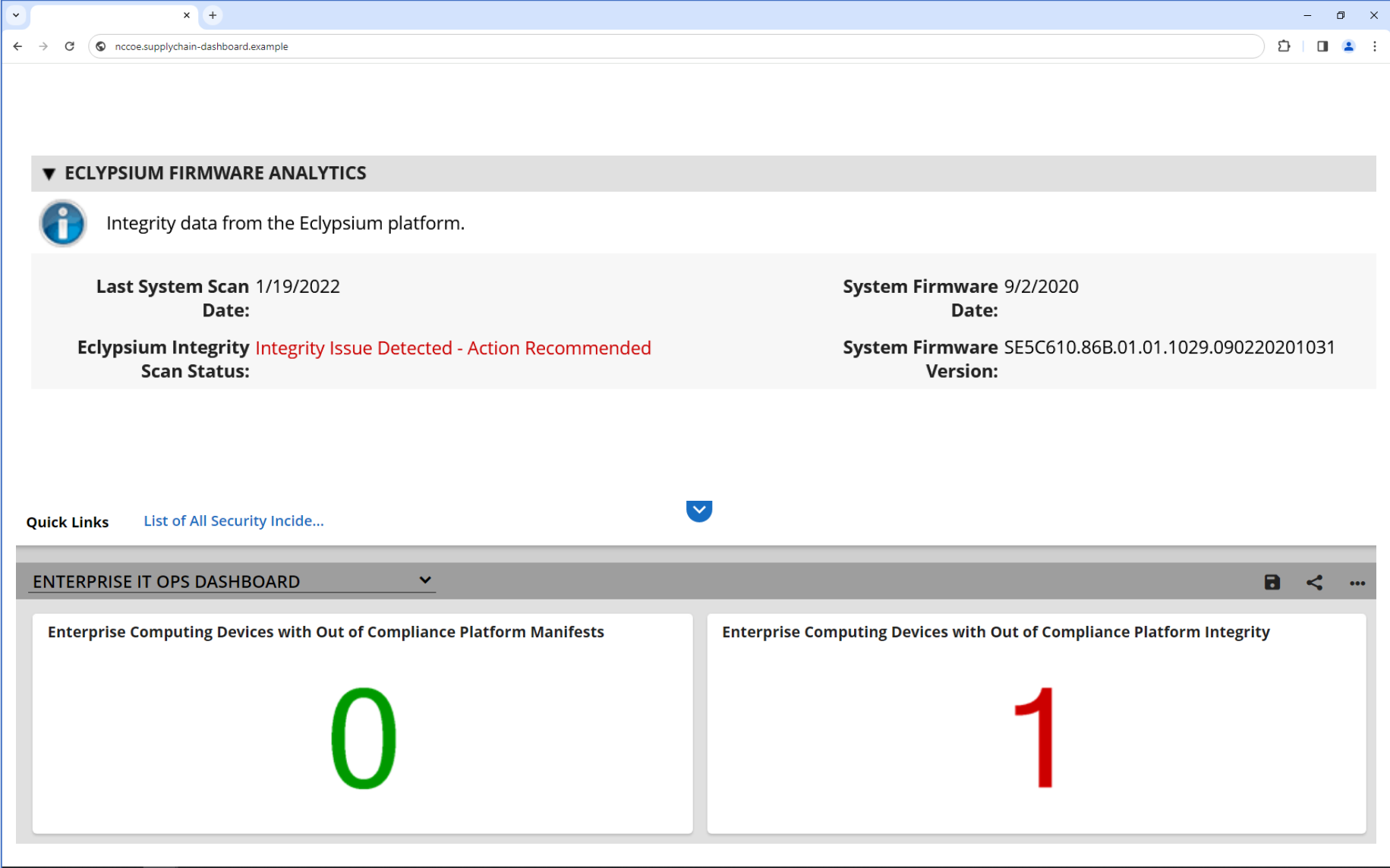
Scenario 3



Scenario 3 - Dashboard



Scenario 3 – Operational Use



The screenshot shows a web browser window with the URL `nccoe.supplychain-dashboard.example`. The main content area is titled "ECLYPSIUM FIRMWARE ANALYTICS" and contains an information icon and the text "Integrity data from the Eclypsum platform." Below this, there are two columns of data:

Last System Scan 1/19/2022 Date:	System Firmware 9/2/2020 Date:
Eclypsum Integrity Integrity Issue Detected - Action Recommended Scan Status:	System Firmware SE5C610.86B.01.01.1029.090220201031 Version:

Below the analytics section, there is a "Quick Links" section with a link "List of All Security Incide..." and a dropdown arrow. The bottom section is titled "ENTERPRISE IT OPS DASHBOARD" and contains two cards:

- Enterprise Computing Devices with Out of Compliance Platform Manifests**: 0
- Enterprise Computing Devices with Out of Compliance Platform Integrity**: 1

Scenario 3 – Operational Use

Automated incident ticket

Drag a column name here to group the items by the values within that column.					
	Incident ID	SCA Computing Device	Incident Summary	Days Open	Incident Status
<input type="checkbox"/>	INC-277233	3206d7fa-d7d3-b406-daf5-62d4c47d6d79	HP_Sure_Start Integrity violation	0 Day(s)	New

Page 1 of 1 (1 records)

INCIDENT SUMMARY

- Incident ID: INC-277233
- Source: IBM Qradar
- Title: HP_Sure_Start Integrity violation
- Incident Summary: HP_Sure_Start Integrity violation
- Incident Details: This indicates that HP Sure Start has detected that the main drive partition table has been altered, and HP Sure Start has returned the partition table to the desired state. This event could be indicative of an attack on the device in the event the change to the drive partition tables was made by an unauthorized party.

SCA Computing Device

Enterprise Unique Identifier

[3206d7fa-d7d3-b406-daf5-62d4c47d6d79](#)

Ticket details

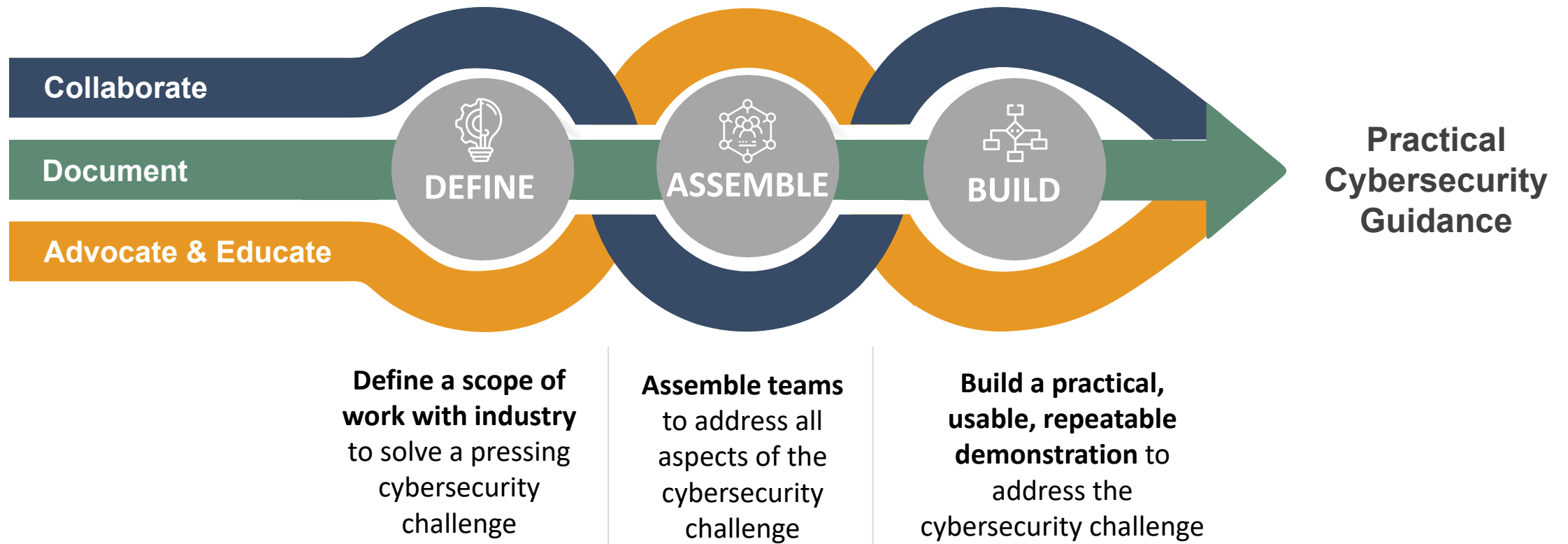
Remediation action

Overview | Impact Analysis | **Remediation** | Results

REMEDIATION ACTION REQUIRED

- Remediation Yes Required?:
- Remediation Action: Restrict the computing device from sensitive corporate network resources.

Our Approach: A Foundation of Trust



NIST's foundation of trust is based on an open, transparent, inclusive process.

Project Execution Timeline

DESCRIBE

FORM TEAM

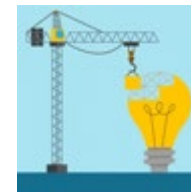
DESIGN

BUILD PLAN

BUILD

DOCUMENT

OUTREACH



Preliminary Research and Feasibility Discussion to Develop Initial Concept

Engage with industry to scope the project and publish the project description

Form the team, build the community of interest, and complete the FRN, LOI, and CRADA

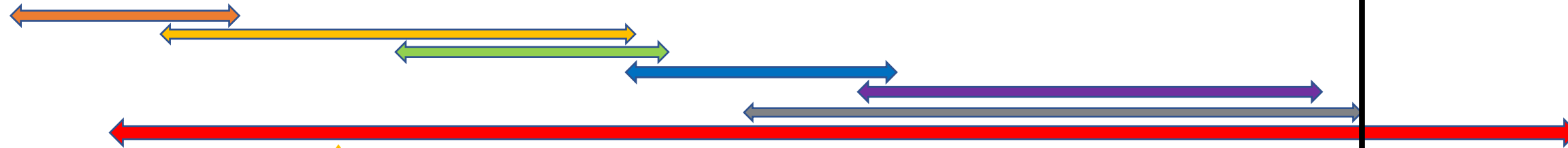
Design and engineer the architecture and usage scenarios

Develop the execution plan for building the demonstration based on the design

Build the demonstration in the NCCoE lab and perform security functional tests

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

Present at public events, engage with COI, and promote publication



Q1 2019-
Q2 2019

Q2 2019-
Q1 2020

Q1 2020-
Q4 2020

Q4 2020 –
Q3 2021

Q3 2021 –
Q1 2022

Q3 2021 –
Q1 2022

Q1 2022 –
Q4 2022

Q4 2022-

NCCoE Practice Guide Volumes

Volume A – Why we wrote this guide and our approach to solving the designated challenge

Volume B – What we built and why, including the risk analysis performed and the security/privacy control map

Volume C – How to build the example implementation, including all the details that would allow one to replicate all or parts of this project



NIST SP 1800-34

- Published the NIST Special Publication (SP) 1800-34 Practice Guide in December 2022
 - Final Volume A, B, C, including laptop and server build
- Encouraging adoption and welcoming feedback on SP 1800-34



Key Takeaways

- **“We gained a valuable understanding of requirements of a broad range of actors from manufacturers to end users, and this project helped create valuable opportunities and dialogue with customers and partners on supply chain security topics and future-looking innovations.” - *Hewlett Packard***
- **“NIST SP 1800-34 is now internally used by our organization as a reference to implement supply chain validation. Collaboration with participants was a key learning opportunity to understand organizationally how to work with industry partners on device attestation.” - *Intel***
- **“This project highlighted a need for standardization for a secure supply chain amongst industry partners and drove desire to expand collaborator partnerships.” – *Dell Technologies***

Additional Efforts & Resources

- NIST Cybersecurity Framework 2.0: Draft Quick Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)
 - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1305.ipd.pdf> -
- NIST Special Publication (SP) 800-161, Revision 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
 - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf>
- NIST Cybersecurity Supply Chain Risk Management (SCRM) Fact Sheet
 - https://csrc.nist.gov/csrc/media/Projects/cyber-supply-chain-risk-management/documents/C-SCRM_Fact_Sheet.pdf -
- NCCoE Software Supply Chain and DevOps Security Practices Project
 - <https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices> -

Get Involved

To join a community of interest, visit:

www.nccoe.nist.gov/get-involved/join-community-interest

Join a Community of Interest

Discuss Challenges

Contribute to Publications

Participate in a Project

Share a Project Idea



NCCoE Supply Chain Assurance Team

Team Email: supplychain-nccoe@nist.gov

Project Page: <https://www.nccoe.nist.gov/supply-chain-assurance>



[nccoe.nist.gov](https://www.nccoe.nist.gov)



[@NISTcyber](https://twitter.com/NISTcyber)