

RSACConference2022

San Francisco & Digital | June 6 – 9

SESSION ID: PDSC-M02

Validating the Integrity of Computing Devices

TRANSFORM



MODERATOR: Nakia Grayson
IT Security Specialist
NIST/NCCoE

PANELISTS: Themistocles Chronis
Principal Consultant
Archer

Tom Dodson
Supply Chain Security Architect
Intel Corporation

John Loucaides
SVP of Strategy
Eclypsium

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

Panel Group

Moderator



Nakia Grayson
NIST
IT Security Specialist

Panelist



Themistocles Chronis
Archer
Principal Consultant

Panelist



Tom Dodson
Intel
*Supply Chain Security
Architect*

Panelist



John Loucaides
Eclypsium
SVP of Strategy



@NISTCyber
#NCCoE

Panel Discussion Topics

- **Supply Chain Challenges**

[Supply Chain Security Goes Digital \(Intel\)](#)

- **Supply Chain Threats and Risk Management**

[Risk at the Firmware Layer \(Eclipsium Blog\)](#)

[Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1](#)

[Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#)

- **Industry Cyber Supply Chain Risk Management (C-SCRM) Collaborative Efforts**

[NIST Cybersecurity Supply Chain Risk Management Fact Sheet](#)

- **Post-DETECT Remediation**

[Key Practices in Cyber Supply Chain Risk Management: Observations from Industry](#)

- **NIST's NCCoE Supply Chain Assurance Project**

[NIST's NCCoE SP 1800-34, Validating the Integrity of Computing Devices Project Page](#)



Call to Action/Key Takeaways

- **Review NIST SP 1800-34 Volumes A, B, C based on your role in your organization**
 - Provide feedback on Draft Practice Guide starting June 23rd until July 25th
 - Send project ideas to NCCoE Supply Chain Assurance Team at supplychain-nccoe@nist.gov
- **Implement tools and technologies identified in NIST SP 1800-34**
- **Implement ongoing or continuous monitoring for an organization's devices**
- **Encourage your organization to work with original equipment manufacturers (OEMs) to ensure devices and components are genuine and haven't been tampered with**
- **Check out the Cybersecurity Supply Chain Risk Management Program site for additional information on other NIST work on C-SCRM**
 - <https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management>
 - [National Initiative for Improving Cybersecurity in Supply Chains \(NIICS\)](#)

RSA®Conference2022

MODERATOR:

Nakia Grayson

IT Security Specialist
NIST/NCCoE

PANELISTS:

Themistocles Chronis

Principal Consultant
Archer

Tom Dodson

Supply Chain Security Architect
Intel Corporation

John Loucaides

SVP of Strategy
Eclypsium

