National Cybersecurity Center of Excellence

Quarterly Planning End of Q3 FY2021

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

AGENDA

Q3 Project Numbers

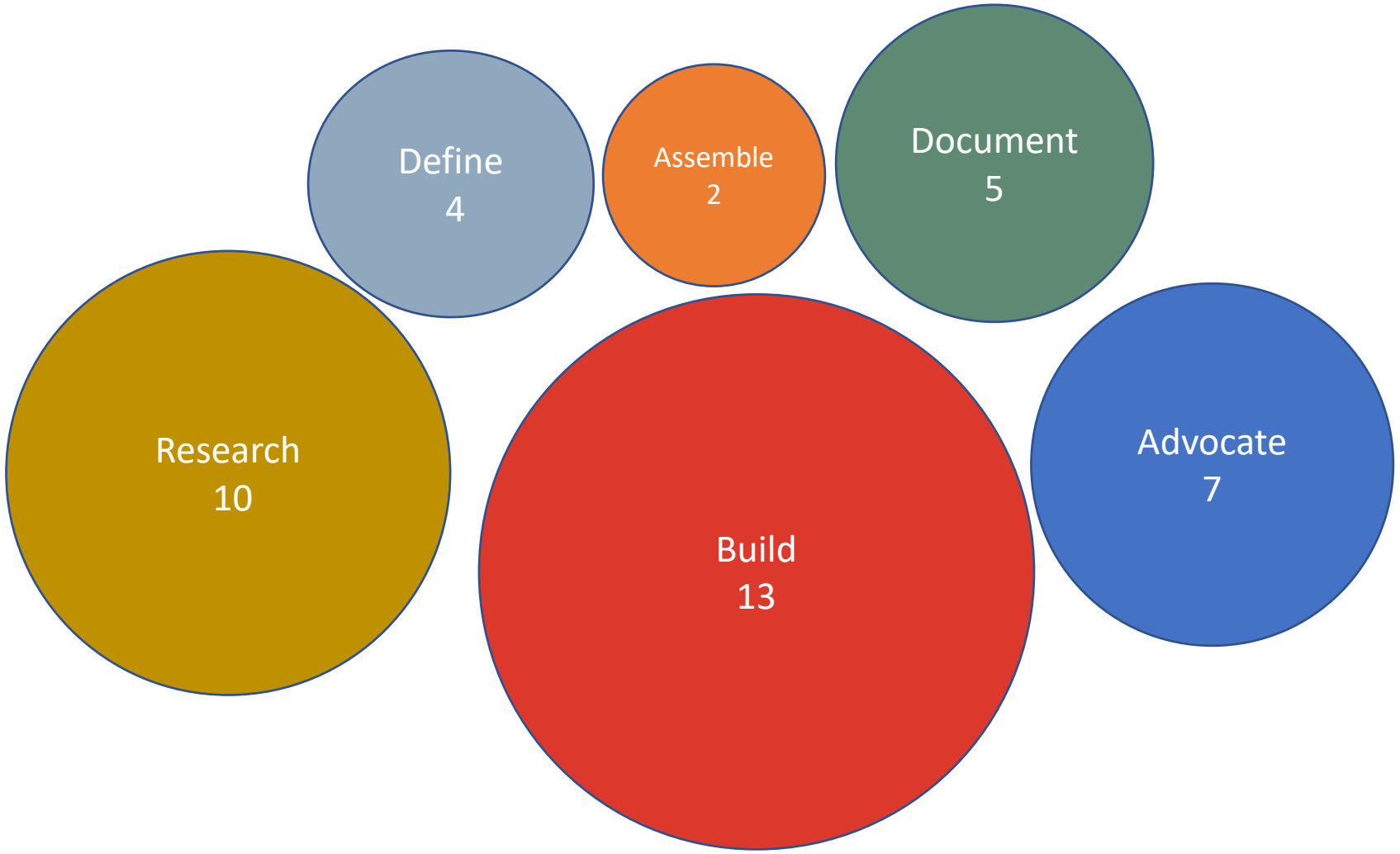
Current Projects

Proposed Projects (none for this submission)

PROJECTS BY SECTOR/TECHNOLOGY

Sector/Technology and count of Project. Color shows details about Sector/Technology. Size shows count of Project. The marks are labeled by Sector/Technology and count of Project. The view is filtered on Sector/Technology, which keeps 16 of 17 members.

PROJECTS BY PHASE



Current Projects

CURRENT PROJECTS - RESEARCH

NCCoE ID	Project	PI	PI- All	MITRE PL	Execution Business Model
P010	Preventing and Recovering from Ransomware and Other Destructive Cyber Events	Bill Fisher	Murugiah Souppaya/Curt Barker/Bill Fisher		MITRE R&D - TBD
P011	Cybersecurity for the Electric Utility Distribution Grid	Jim McCarthy	Jim McCarthy/ Avi Gopstein/ Nelson Hastings	Don Faatz/ Eileen Division	MITRE R&D
P005	Cybersecurity Resources for Small Manufacturers	Michael Powell	Michael Powell/Celia Paulsen/Jim McCarthy	John Hoyt	MITRE R&D
P012	Manufacturing - Recovery from destructive malware attacks	Michael Powell	Keith Stouffer/ Michael Powell	John Hoyt	MITRE R&D
TL	Trusted Laboratory Network Infrastructure	Murugiah Souppaya	Murugiah Souppaya/ Alper Kerman/ Curt Barker	Parisa Grayeli	MITRE R&D
P008	DevSecOps Practice Guide	Murugiah Souppaya	Murugiah Souppaya/ Kevin Stine/ Matt Scholl		MITRE R&D
P006	Autonomous vehicles - cybersecurity and privacy concerns	Nakia Grayson	Nakia Grayson	Mike Hadjimichael	AI portion of the scope
GN	Cybersecurity of bio genomic data	Ron Pulivarti	Natalia Martin/Jim McCarthy/Leah Kauffman/ Justin Wagner/ Ron Pulivarti	Ann-Marie France	Separate TO w/MITRE
P009	Telehealth: Smart Home Integration	Ron Pulivarti	Nakia Grayson/ Ron Pulivarti	Sue Wang	MITRE R&D
NT	Artificial Intelligence Research Initiatives	Tim McBride	Elham Tabassi/ Harold Booth/ Nakia Grayson/Timothy McBride	Anne Townsend	MITRE R&D - Optional

Ransomware Mitigation – Follow on to data security

Research | Define | Assemble | Build | Document | Advocate

Project Team: Bill Fisher; Project Requested by: Industry (AWS, Motorola, Institute for Security and Technology)

Date: May 2021

What problems are we solving?

The Problem – The frequency and impact of ransomware attacks continue to rise in 2020 reaching the stage of Ransomware as a Service (RaaS).

From the recent IST ransomware report: "*Yet adoption of preparedness best practices remains limited, and ransomware attackers continue to find sectors and elements of society that are woefully underprepared for this style of attack. The sheer volume of content published on the topic of ransomware is part of the challenge; with so much information and noise surrounding this threat, time- and resource-constrained organizations and individuals struggle to identify the most relevant and accurate sources of useful information. In addition, many guides are reportedly either too simple, too complicated and overwhelming, or not specific to ransomware.*"

Impact

Educate decision makers on ransomware risks. Provid clear, succinct and precisely scoped guidance on ransomware mitigation strategies and best practices. To help organizations make risk-informed decisions about ransomware response and recovery.

Why should NCCoE do this project?

NCCoE/NIST should consider new, succinct, ransomware specific guidance that may include but not be limited to: education for executives, technical best practices, a recovery playbook that includes a cost benefit analysis for deciding to pay ransoms, etc…

What is new in this approach?

NCCoE/NIST shall publish a call for papers where subject experts can express opinion on the ransomware challenge. This call will be followed up with a virtual workshop to discuss the topic. With input from this community of interest NCCoE/NIST will determine a path forward for new guidance.

Risks

Unknown. Will update after call for papers.

Resources Needed

No Mitre or lab resources needed yet.

Project Name : Cybersecurity for the Electric Utility Distribution Grid - Smart Grid Profile Implementation

Research | Define | Assemble | Build | Document | Advocate

Project Team Leadership: Jim McCarthy and Eileen Division Date 07/13/2021 Id: P011

Overview /Purpose

This project seeks to demonstrate secure interoperability of smart inverters with system operators/distribution operations using the NIST/SEPA interoperability profiles

Audience

Distributed energy (solar inverter) resource owners/operators – primarily utility-scale, commercial-scale, and microgrid/campus distributed energy resource owners/operators

Outcome

A document that details the implementation of the Smart Grid interoperability profiles (not certain what format but unlikely an SP) which also demonstrates securing of solar inverters.

Project Status

- *Current outlook is to begin work on profile implementation in Q4 FY22 (Project has an approximate 2-year lifecycle)*
- *Currently in the process of defining / finalizing scope although project has been agreed to by NCCOE / NIST EL and NIST ITL Smart Grid Lead*
- *Assessing whether "collaboration" will be needed, especially if it is decided to use actual solar inverters*

Tags

energy; IIoT; distributed energy resources; microgrid

Next Steps

- *Review project proposal with NIST Engineering Laboratory (EL) and ITL Smart Grid Program Lead*
- *Finalize scope early Q1 FY 2022*
- *Determine equipment needs to demonstrate securing of solar inverters*

Challenges or barriers to success

- *None*

Cybersecurity Resources for Small Manufacturers

Research | Define | Assemble | Build | Document | Advocate

Project Requestor(s): Michael Powell (PL) and John Hoyt (TL) Date: 04/02/2021

What problems are we solving?

Small manufacturers are increasingly under threat from cyberattacks. A successful infiltration from a cybercriminal could shut down a plant's operations or start making equipment produce faulty products without the knowledge of managers, among other things. Most manufacturers are small businesses that do not have established Operational Technology (OT) security practices to combat or cope with a cyber incident. This lack of preparedness not only makes it easier for cybercriminals to attack, NCCoE along with MEP will develop solutions.

Impact

Creation of the whitepapers will assist small manufacturers with limited resources and budgets with cybersecurity guidance, solutions, and training that is practical, actionable, cost-effective and helps manage their cybersecurity risks.

- NCCoE, NIST, MEP, Manufacturing, IIOT
- Network segmentation for manufacturing environment – is one of the first white papers to be considered.

What is new in this approach?

NCCoE and MEP will develop white papers to assist with:

- Network segmentation
- Secure email security (including how to evaluate the provider's security, what security they need to provide, and when to migrate to a new provider)
- Multi-factor authentication & complex password requirements
- Physical security basics
- How to lock down ports

Risks (low)

TBD

Resources Needed

TBD

Manufacturing - Recovery from destructive malware attacks

Project Requestor(s): Michael Powell (PL) and John Hoyt (TL) Date: 07/12/2021, ID P012

What problems are we solving?

Cyber attacks against manufacturing entities are on the rise. Mitigations are being applied, but attackers are still gaining access. Successful attackers can cause loss of production or damage facilities. Manufactures need reliable solutions to respond and recover from cyber attacks to Operational Technology (OT).

Impact

Manufacturers can benefit from a practice guide which demonstrates how commercially available technologies can be operationalized in OT environments for response and restoration of systems such as, engineering workstation, human machine interfaces, programable logic controllers, historians and lower-level devices.

Advocates and adopters:

- NCCoE, Manufacturing, IIOT

What is new in this approach?

Current IT solutions for responding to and recovering from cyber attacks are not readily applicable to OT environments such as Industrial control systems (ICS) used in discrete manufacturing. Solutions should consider the unique nature of OT and build on existing data integrity work contained in SP 1800-11.

Risks (low)

Recovery products may be vendor specific.

Resources Needed

NCCoE Manufacturing Laboratory

Trusted Enterprise Infrastructure

Research | Define | Assemble | Build | Document | Advocate

Murugiah Souppaya, Mike Bartock, Alper Kerman, Curt Barker, Parisa Grayeli, Alan Tan, Yemi Fashima, Josh Klosterman, and Karen Scarfone

July 13, 2021

Overview /Purpose

Design and build a typical enterprise network environment on-premises and connected the cloud components to include common shared services, tools, and security and compliance capabilities

Audience

- NCEPs and IT technology companies
- Regulated industries like financial services, healthcare, and government

Outcome

- Design and build a common infrastructure to support the projects at the NCCoE to efficiently use of NCEPs' resources, eliminate duplicate effort across projects, integrate the the project teams with NCCoE ITOps team who is modernizing the NCCoE lab infrastructure
- 4QFY21: Draft SP 1800-xx and papers

Project Status

- Review and award the invested equipment purchase for the MPLS and SDN (Kudos to Fred Byers)
- Continue to develop user stories to support the integration across projects (Supply Chain, 5G, Enterprise Patching and ZTA) and establish coordination meetings
- Focus of DevOps to support software defined data center and orchestrating the physical and virtual lab

Keywords

- cloud computing; enterprise architecture; network infrastructure; network protocols; shared services

Next Steps

- Design and plan for the deployment of the MPLS and software defined network in coordination with ITOps
- Continue to plan the tactical activities to identify opportunities and challenges

Challenges or barriers to success

- Identify an approach that will improve the efficiency of executing projects at the center but still support the Center's open, transparent, and inclusive principles for engaging with industry participants

DevSecOps Practice Guide (targeting specific programming languages and use cases)

Murugiah Souppaya, Kevin Stine, Matt Scholl, and Karen Scarfone

August 30, 2020

What problems are we solving?

- Traditional organizations in regulated industry are struggling with integrating security in DevOps practices to take advantage of cloud native technology
- Assist organizations with practical guidance for trusted continuous integration and continuous deployment (CI/CD) pipeline for one or more software development language targeting cloud native applications
- Complement NIST's initiative to develop recommended guidance for DevSecOps
- Leverage existing NIST guidance related to RMF, CSF, SSDF, NICE framework, containers security, OSCAL, service-mesh, micro-services, virtualization, and NCCoE trusted platforms and network infrastructure projects
- Strong interest from the NCEPs to develop and sho
  tooling

Impact

- Lessons learned can benefit the NCCoE ITOps team in adopting the modern practices to be agile and efficient to support the projects
- Develop actionable guidance for specific programming language and industry sector specific use cases (e.g., cloud native apps, IoTs, etc.)
- IT industry and financial services are the early adopters
- NCEPs can demonstrate their current practices and share their toolchain

Coordinate and synchronize this project with Software Supply Chain Security EO

What is new in this approach?

- **Current State**
  - Lack of NIST led and industry consensus, authoritative, practical, and demonstrable practices for DevSecOps
- **Proposed approaches**
  - Collaborate with industry to translate industry and NIST existing guidance into practices leveraging open source and commercial tools
  - Integrate, automate, and orchestrate security recommended guidance into the CI/CD pipeline
  - Generate security and compliance artifacts as part of the DevOps toolchain to support the SSDF practices and SP 800-53 controls
  - Leverage modern cloud technology like Docker container, Kubernetes orchestration, open source and commercial security tools to enhance the DevOps toolchain

Risks

- Diverse requirements to cover all software development languages and industry use cases like financial services, healthcare, IoTs, IIoTs, etc

Resources Needed

- 12 to 18 months to define, design, build, and develop the practice guide, demonstration videos, open source toolchain, etc.
- 2 to 4 MITRE engineers and a technical writer/editor
- Focus on leveraging cloud services or hosted solutions in conjunction with on-premise infrastructure and physical lab

Project Name : AI in AVs

Project Team Leadership: Nakia Grayson (NIST PI) and Mike Hadjimichael (MITRE PL) Date:7/8/21, Id:P006

Overview /Purpose

Understand the use of AI/ML and associated risks in semi-autonomous and autonomous vehicles.

Audience

The audience is NIST/NCCoE, to understand the cyber-risks introduced by integration of AI into autonomous vehicles, and to understand if standards and technology are mature enough to pursue an 1800 series-like project in this space.

Outcome

- Foundation for lab exploration of AI-introduced cyber risks
- Guidance on the need for further development of a practice guide or standards to support safe industry deployment of AI in autonomous vehicles.
- Draft White Paper or Position Paper -End of FY21

Project Status

- Research on current technology, industry R&D, and applicable standards completed
- Vehicle architecture and operating environment models completed
- Identification of relevant autonomy-supporting AI methodologies in progress

Tags

Artificial Intelligence,

Autonomy,

Autonomous Vehicles,

Adversarial Machine Learning,

Cybersecurity

Next Steps

- Complete identification of AI components of autonomous vehicle system
- Perform cybersecurity threat analysis of AI components

Challenges or barriers to success

- Much of the industry efforts in this field are proprietary, so report results or industry work are only based on publicly available information

Telehealth-Smart Home Integration

Project Team Leadership: *Ron Pulivarti and Sue Wang* Date: July 2021, Id: P009

<Graphical representation of the project phase. Select Blue – completed, Grey – current, Unfilled – not started>

Overview /Purpose

Create an example solution to address the cybersecurity challenges of an ecosystem that incorporates smart home devices into an HDO-managed telehealth solution.

Audience

Patients use smart home devices as an interface into the telehealth ecosystem and healthcare providers who are interested in applying cybersecurity and privacy principles in their telehealth program.

Outcome

- *Empower patients with knowledge to securely use smart speakers as part of managing their healthcare.*
- *Increased awareness and adoption of NCCoE cybersecurity and privacy solutions for healthcare providers' telehealth programs.*

Project Status

- *Obtained the approval for the proposed project idea*
- *Conducted feasibility study and research, such as, industry assessment, technology and standards readiness, and stakeholders*
- *Developed draft PD and submitted for leadership review*
- *Perform multiple runs of peer reviews with relevant NIST groups on the draft PD*

Tags

application programming interface; API; application security; cybersecurity; data privacy; data privacy and security risks; health delivery organization; HDO; internet of things; IoT; smart home; telehealth

Next Steps

- *Complete the peer review process on the draft PD and incorporate the feedback and update the draft PD*
- *Continue and complete the tech-editing and web-pub process for the draft PD with public comment period **(Q4FY21?)***
- *Adjudicate public comments received and publish the final PD along with a FRN for this project*

Challenges or barriers to success

- *None for now.*

Project Name : AI Healthcare Research

Project Team Leadership: Elham Tabassi, Tim McBride and Anne Townsend Date: July 13, 2021, Id:NT

Overview /Purpose

internal research project investigating the cyber and privacy risks due to the healthcare industry's usage of AI. Research will investigate the relevant technologies and standards readiness to mitigate these risks.

Audience

The audience for this research is NIST/NCCoE in order to understand if the standards and technology are mature enough to pursue an 1800 series-like project.

Outcome

- Pursue an 1800 like project with the healthcare industry to address cyber and privacy challenges incurred from the usage of AI

Project Status

- Developed initial draft documents (70% complete) covering:
  - Industry Assessment Report
  - Standards Readiness Report
  - Technology Readiness Report
  - Cyber and Privacy Risks and Challenges
- Exploring potential reference architectures

Tags

Healthcare; AI; Privacy challenges, Cyber

Next Steps

- Use cyber and privacy challenges to develop a reference architecture using identified technologies and standards

Challenges or barriers to success

- Technologies or standards are not mature enough to proceed with a follow-on project

CURRENT PROJECTS - DEFINE

NCCoE ID	Project	PI	PI- All	MITRE PL	Execution Business Model
M4	Data Classification in Support of Data Management across the Lifecycle of Data	Bill Newhouse	Murugiah Souppaya/Bill Newhouse	Ken Sandlin	MITRE R&D
M3	Applied Crypto: Automation of the Cryptographic Module Validation Program (CMVP)	Murugiah Souppaya	Apostol Vassilev/ Curt Barker/ Tim Polk/ Murugiah Souppaya		MITRE R&D
M2	Applied Crypto: Challenges with Compliance, Operations, and Security with TLS 1.3 for Enterprise Data Centers	Murugiah Souppaya	Curt Barker/Tim Polk/Murugiah Souppaya		MITRE R&D
QT	Crypto agility: PQC Migration Playbook for IT Manufacturers and Enterprise	Murugiah Souppaya	Lily Chen/Curt Barker / Dustin Moody/Murugiah Souppaya	Sallie Edwards	MITRE R&D

Project Name : Data Classification

Project Team Leadership: Murugiah Souppaya, Curt Barker and Bill Newhouse and MITRE Technical Lead Ken Sandlin Date: July 13, 2021, Id: M4

Overview /Purpose

Data classification a fundamental step in the context of data management and information protection to support various business use cases. Multiple phases project supports the life cycle of managing information security at the data level and demonstrate compliance to various requirements.

Audience

- NCEPs and IT technology companies
- Regulated industries like financial services, healthcare, and government

Outcome

- *Develop guidance and associated demonstrations focusing on data management activities (definition, classification, governance policy, and enforcement) across the data lifecycle (generate data, store/process, transmit/share, and retain/repurpose/destroy).*
- *4QFY21: Finalize and post PD, deliver FRN package*

Project Status

- Draft Project Description (PD) posted for public comment on May 19, 2021.
- Comment Period closed on June 21, 2021 with 13 comments submitted by 8 parties
- Project Description website and emails also asked for individuals who wished to shape and contribute on the project ; to-date 20 volunteers have signed up to assist.
- On June 16, Curt and Bill discussed the project with the Financial Services Sector Coordinating Council R&D Committee (JP Morgan co-chair already involved in project)

Tags

data classification; data security; information protection

Next Steps

- *Week of July 12: Adjudicate comments received, update project description, and publish Federal Registry Notice with the project description, component list and desired security characteristics that will result in receipt of Letters of Interest .*

Challenges or barriers to success

- *None except to keep pace with the need to provide guidance for data classification as a foundational need for implementations of zero trust architectures.*

Applied Crypto: Automation of the Cryptographic Module Validation Program (CMVP)

Apostol Vassilev, Gavin O'Brien, Chris Celi, Tim Hall, Murugiah Souppaya, Curt Barker, and Karen Scarfone

July 13, 2021

Overview /Purpose

Work with industry innovators to modernize the FIPS 140 validation program by automating the CMVP

Audience

- Hardware, software, services developers and manufacturers and enterprise
- Crypto community

Outcome

- Develop test methodologies to provide consistent and reproducible evidence generated and reported by the producers of technologies that implement cryptographic capabilities.
- Integrate the output of the project into the NIST formal FIPS 140 validation program.
- 4QFY21: Draft SP 1800-xx and supporting papers and open source tools

Project Status

- Publish final project description
- Build the community of interest
- Hosted a virtual industry day workshop on October 5, 2020 and released the video recording and supporting slides

Keywords

- automation; certification; cryptography; FIPS 140; test; validation

Next Steps

- Submit FRN/LOI package
- Identify MITRE staff to support the project

Challenges or barriers to success

- Execute the project from the start and engage with the community virtually

Applied Crypto: Challenges with Compliance, Operations, and Security with TLS 1.3 for Enterprise Data Centers

Tim Polk, Curt Barker, Andy Regenscheid, David Cooper, Murugiah Souppaya, and Karen Scarfone

July 13, 2021

Research | Define | Assemble | Build | Document | Advocate

Overview /Purpose

Enhancements introduced in TLS 1.3 to address security concerns on the public internet reduce visibility within enterprise network to include data centers and hybrid cloud. Develop risk-based approaches to allow network visibility to meet enterprise's business, security, and functional requirements.

Audience

- Hardware, software, services developers and manufacturers and enterprise from regulated industry like financial services, healthcare, and government
- Crypto community and TLS protocol designers and implementers

Outcome

- Identify the practical and implementable approaches to help those regulated industries adopt TL 1.3 in their private data centers and the hybrid cloud without impacting regulatory compliance, security, or operations
- 4QFY21: Draft SP 1800-xx and supporting papers

Project Status

- Publish final project description
- Submitted FRN/LOI package
- Communicate with ETSI and IETF
- Continue to build the community of interest
- Continue to engage with the community including technology companies and financial services industry sector
- Hosted a virtual industry day workshop on September 25, 2020 and released the video recording and supporting slides

Keywords

- cryptography; network security protocols; TLS; visibility

Next Steps

- Publish FRN, LOI, and initiate CRADA process
- Reach out to SDOs to solicit their participation
- Identify MITRE staff to support the project

Challenges or barriers to success

- None

Crypto agility: PQC Migration Playbook for IT Manufacturers and Enterprise

Project Team Leadership: Curt Barker, Bill Newhouse, and Murugiah Souppaya Date: July 13, 2021 Id: QT

Overview /Purpose

To complement the PQC standard development process by initiating a campaign to bring awareness to the issues involved in migrating to PQ algorithms and develop papers, playbooks, and proof-of-concept implementations

Audience

- Hardware, software, services developers and manufacturers and enterprise
- Crypto community

Outcome

- Identify recommended crypto agility practices to execute a smooth transition and demonstrate tools and techniques that can help developers and implementers of algorithms and protocols
- 4QFY21: Draft SP 1800-xx and supporting papers and open source tools

Project Status

- *June 4, 2021, released draft project description Migration to Post Quantum Cryptography for public comment.*
  - Comment Period closed last week on July 7, 2021
  - Project Description website and emails also asked for individuals who wished to shape and contribute on the project.
- On June 8, at the 3rd PQC Standardization Conference, Bill kicked off the 2nd day by presenting this project which allowed us to clarify the project's target audience and reason for our focus on automated tools via questions from Slack conference channel.

Tags

- cryptography; crypto agility; crypto transition; digital signatures; post-quantum cryptography; public-key encryption; key establishment mechanism (KEM); quantum resistant; quantum safe

Next Steps

- *Identify MITRE staff to support the project*
- *Adjudicate comments received, update project description, and publish Federal Registry Notice with the project description, component list and desired security characteristics that will result in receipt of Letters of Interest .*

Challenges or barriers to success

- *Execute the project from the start and engage with the community virtually*

CURRENT PROJECTS - ASSEMBLE

NCCoE ID	Project	PI	PI- All	MITRE PL	Execution Business Model	CRADA Partners
ZT	Zero Trust Architecture (ZTA) Project	Alper Kerman	Murugiah Souppaya/Alper Kerman/ Scott Rose / Oliver Borchert	Parisa Grayeli	MITRE R&D	Amazon Web Services, Inc. Appgate Cisco Systems, Inc. F5 Networks, Inc. FireEye, Inc. Forescout Technologies, Inc. International Business Machines Corporation (IBM) McAfee Corp. Microsoft Corporation MobileIron, Inc. an Ivanti Company Okta, Inc. Palo Alto Networks PC Matic, Inc. Radiant Logic, Inc. SailPoint Technologies, Inc. Symantec, a Division of Broadcom Tenable, Inc. Zscaler, Inc.
AD1	Trusted IoT Device Network-Layer Onboarding & Lifecyle Management	Paul Watrobski	Paul Watrobski/ Curt Barker/Mike Fagan/ Jeff Marron/ Scott Rose/ Murugiah Souppaya	Blaine Mulugeta	MITRE R&D	n/a

Implementing a Zero Trust Architecture

Project Team: Alper Kerman, Murugiah Souppaya, Scott Rose, Oliver Borchert, Parisa Grayeli, Allen Tan, Yemi Fashina, Nedu Irrechukwu, Eileen Division, Josh Klosterman

Date: July 13, 2021, **ID:** ZT

Research | Define | Assemble | Build | Document | Advocate

Overview / Purpose

Due to several high-profile cyber attacks in recent years, organizations are being forced to rethink the traditional network security perimeter. A Zero Trust Architecture (ZTA) is a paradigm shift that focuses on protecting resources instead of network perimeters, as the network location is no longer viewed as the prime component to the security posture of the resource. To demonstrate this paradigm shift, the NCCoE and its collaborators will be developing an example ZTA using commercially available products.

Audience

- Everyone

Outcome

- Example implementations of various Zero Trust Architectures that can be used as a foundational framework for building extended and more complex versions tailored to more specific requirements.
- A 1800 Special Publication – Practice Guide – FY22 Deliverable

Project Status

- Received 66 LOIs, met with each member and then, selected 19 vendors, signed and executed a CRADA with each one for participation on the project.
- Created a capability matrix that summarizes each vendor's technology contribution with specific capabilities applicable for use in ZTAs
- Created a high level notional ZTA architecture and identified number of builds by analyzing and mapping various vendor technologies and capabilities. And then, selected vendors.
- Created integration matrix showing integration points of collaborators' products
- Provisioned a lab environment and built a network infrastructure that mimics 3 different enterprises to accommodate various implementations based on 3 ZTA approaches (Enhanced Identity Governance (EIG), Software Defined Perimeters (SDP), and Micro-segmentation)
- Provisioned Ansible as the automation tool for creating VMs and their services such as AD, DNS, DHCP. Exploring possibility of integrating it with Terraform.

Tags

- Zero Trust, Access Management, Software Defined Perimeter, Micro-segmentation

Next Steps

- Conduct the project kickoff meeting scheduled for July 21st and 23rd
- Create detailed architectures and agree on the number of builds to accommodate various modular implementations based on 3 ZTA approaches.

Challenges / Barriers

- Exploring integration point among the 19 collaborators and their products

Project Name : Trusted IoT Device Network-Layer Onboarding & Lifecyle Management

Research | Define | Assemble | Build | Document | Advocate

Project Team Leadership: Paul Watrobski, Murugiah Souppaya, and Blaine Mulugeta Date: 2021-07-13, Id: AD1

Overview /Purpose

Demonstrate trusted network layer onboarding as a secure and scalable mechanism to increase assurance that

- networks are not put at risk as IoT devices are added to them
- IoT devices will not be taken over by unauthorized networks
- IoT devices can be safely managed throughout their lifecycles

Audience

IoT device manufacturers, integrators, and vendors; network admins; service providers; industry consortia; standards organizations

Outcome

Demonstration of an example trusted network-layer onboarding solution that is built using commercially available technology

Project Status

- Cybersecurity Paper Draft – converting to a NISTIR
- Global Platform Conference – Presented on March 17th
- RSA Conference – Presented on May 19th
- PD – Published final on May 20th
- FRN – Initiated in May
- Meeting with prospective collaborators

Tags

- IoT, network-layer onboarding, application-layer onboarding, bootstrapping, attestation, device lifecycle management, network security

Next Steps

- Cybersecurity Paper – Complete conversion to a NISTIR, start the ERB process
- FRN – Publish and solicit LOI
- Establish CRADA

Challenges or barriers to success

- Trusted network-layer onboarding solutions are relatively new and are expected to develop further over the next two years; additional mechanisms may emerge
- Existing solutions are at various stages of development and each solution has its own strengths and weaknesses. The solution targeted for wired, zero-touch onboarding (ANIMA BRSKI) in particular needs some further extensions

CURRENT PROJECTS - BUILD

NCCoE ID	Project	PI	PI- All	MITRE PL	Execution Business Model	CRADA Partners
1333ND21FNB770020	Assisting Foreign Nations to Improve Cyber Capacity by Implementing USG/NIST Frameworks and Guidelines	Adam Sedgewick, Amy Mahn	Amy Mahn / Adam Sedgewick/ Maj Franco	Johanna Vazzana	Interagency/DOS	n/a
PT	Critical Cybersecurity Hygiene: Patching the Enterprise	Alper Kerman	Murugiah Souppaya/Alper Kerman	Parisa Grayeli	MITRE R&D	Tenable, Inc. Cisco Systems, Inc. Eclypsium, Inc. Microsoft Corporation Salt Stack, Inc. ForeScout Technologies, Inc. Lookout, Inc. IBM (pending)
DC	Data Security – Data Confidentiality	Bill Fisher	Bill Fisher/Jen Cawthra	Michael Ekstrom	MITRE R&D	Cisco Systems, Inc. Dispel, LLC FireEye, Inc. Avrio Software, Inc. Cisco Systems, Inc. Dispel, LLC StrongAuth, Inc. PKWARE, Inc. Symantec, a Division of Broadcom FireEye, Inc. GreenTec-USA, Inc. PKWARE, Inc.
1333ND20FNB770292	Cybersecurity Capability Maturity Model, Port Security Framework Profile and Practical Guidance	Bill Newhouse	Bill Newhouse	Josie Long	Interagency/DOE	n/a

CURRENT PROJECTS - BUILD

NCCoE ID	Project	PI	PI- All	MITRE PL	Execution Business Model	CRADA Partners
5G	5G cybersecurity	Jeff Cichonski	Jeff Cichonski/ Mike Bartock/ Murugiah Souppaya	Parisa Grayeli	MITRE R&D	Cisco Systems, Inc. Nokia of America Keysight Technologies Palo Alto Networks AT&T, Inc. Dell Technologies, Inc. Intel Corporation Red Hat, Inc. MiTAC Computing AMI US Holdings, Inc. Cable Television Laboratories, (dba CableLabs) T-Mobile Us, Inc.
BN/1333ND20FNB770274	Blockchain for supply chain traceability	Keith Stouffer	Keith Stouffer	Harvey Reed	Separate TO w/MITRE	n/a
1333ND21FNB770028	Global Position System (GPS)	Matt Scholl	Fred Byers/ Matt Scholl/Maj Franco	John Emilian	Interagency/AF/SMC/PCEP	n/a
MN	Simulating industrial control systems (ICS) Protecting Information System Integrity in Manufacturing Environments	Michael Powell	Michael Powell	John Hoyt	MITRE R&D	ForeScout Technologies, Inc. OSIsoft, LLC CyberX, Inc. Dispel, LLC Dragos, Inc. TDi Technologies, Inc. Tenable, Inc. Carbon Black, Inc. (subsidiary of Vmware) GreenTec-USA, Inc.

CURRENT PROJECTS - BUILD

NCCoE ID	Project	PI	PI- All	MITRE PL	Execution Business Model	CRADA Partners
M0	Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud IaaS Environments	Murugiah Souppaya	Mike Bartock/Murugiah Souppaya		MITRE Support Services only	*Expired* - International Business Machines (IBM) Corporation VMware, Inc. RSA Security LLC HyTrust, Inc. Microsoft Corporation Trapezoid, Inc. Dell Federal Systems LP EMC Corporation Docker, Inc. Twistlock, Inc. SafeNet, Inc. (subsidiary of Gemalto, Inc.) Intel Corporation Thales Group
1333ND21FNB770118	DoT/VOLPE - CSF Intelligent Transportation Systems (ITS)	Nakia Grayson	Fred Byers/Nakia Grayson/ Ray Resendes - VOLPE	Julie Snyder	Interagency/DoT/VOLPE	n/a
1333ND21FNB770106	Systems Security Engineering Next Generation Concepts and Methodologies Support Services	Ron Ross	Mai Nguyen/Ron Ross	Mark W Winstead	Separate TO w/MITRE	n/a
1333ND21FNB770008	AFRL Cyber Survivability Attributes (CSA) Tool - Year 2	Ron Ross	Fred Byers/Ron Ross	Linda Jones	Interagency/DoD/AFRL	n/a
NT/1333ND19FNB775320	Securing AI Research	Tim McBride	Elham Tabassi/Tim McBride	Paul Rowe	Separate TO w/MITRE	n/a

Project Name : Foreign Nations Cybersecurity

Research | Define | Assemble | Build | Document | Advocate

Project Team Leadership: Adam Sedgewick and Amy Mahn; and Johanna Vazzana Date: 14 July 2021 Id: 2721NT87

Overview /Purpose

Provision of cyber capacity building to foreign partners by implementing U.S. Government/NIST frameworks and guidelines to enable Department of State mission outcomes.

Audience

Civilian foreign governments, foreign industry partners, and other foreign civilian stakeholders as appropriate, in low- and lower-middle income partner nations.

Outcome

- *Provide Foreign partner nations with awareness of USG/NIST cybersecurity and privacy frameworks to increase international stability and reduce the risk of conflicts arising from or involving cyber-attacks.*

Project Status

- *Designed , built, and executed virtual pilot workshop for four Western Hemisphere nations; Chile, Colombia, Dominican Republic, and Panama, June 8-10, 2021.*
- *Evaluated participant feedback and feedback from implementation partner, the Organization of American States to refine our approach and make recommendations for next steps.*
- *Created framework for evaluating which partner nations and which stakeholder groups are most likely to have the capacity to absorb foreign assistance on standards and guidelines to assist in targeted stakeholder selection.*

Tags

International Engagement, Cyber Capacity Building, Privacy Framework, CSF, Standards, Guidelines

Next Steps

- *Selection of targeted partner nations for engagement*
- *Selection of targeted stakeholder groups within the selected nation for engagement*
- *Creation or tailoring of content, materials, and workshops for the targeted audiences.*

Challenges or barriers to success

- *Partner nations are making requests for "NIST Standards" assistance without understanding what that means in practice. Partners identified for capacity building assistance should be selected based on defined criteria that ensures they are capable of absorbing the assistance provided.*

Critical Cybersecurity Hygiene: Patching the Enterprise

Project Team: Alper Kerman, Murugiah Souppaya, Parisa Grayeli, Brian Johnson, Chris Peloquin, Vanessa Ruffin, Tyler Diamond, Karen Scarfone, Mary Raguso

Date: July 13, 2021, **ID:** PT

Overview / Purpose

Patching is an important regimen of cyber hygiene, but existing tools in many organizations are insufficient for many situations. Many organizations also struggle to prioritize patches, test them before deployment, and adhere to policies that advise how quickly they need to be deployed in different situations. To address this challenge, the NCCoE and its collaborators will be developing a proposed approach to improve enterprise patching practices for general IT systems.

Audience

- Everyone

Outcome

- An example approach to improve enterprise patching practices for general IT systems.
- A NIST SP 1800-31, Practice Guide, FY21 Deliverable

Project Status

- Completed configuration and integration of Phase 1 components for patching and configuration of “traditional” endpoint systems
- Working on configuration and integration of Phase 2 components for patching, updating and configuration of “mobile and containerized” devices/endpoints
- Developing PG Vol B, C, and D
- Developing video demonstrations

Tags

- Patch Management, Vulnerability Management, Configuration Management

Next Steps

- Publish PG Vol B, C, and D
- Update 800-40 Rev. 4
- Continue phase 2 (mobile/container) configuration and integration
- Initiate phase 3 for patching, updating and monitoring endpoints located on IaaS offerings

Challenges / Barriers

- None

Project Name : Data Confidentiality

Define | Assemble | Build | Document | Advocate

Project Team Leadership: Jennifer Cawthra and Michael Ekstrom Date: July 2021, Id: DC

Overview /Purpose

Identify, Protect, Detect, Respond to and Recover from data breaches that lead to compromised confidentiality. Two separate projects running concurrently. Originating from FS-ISAC.

Audience

Small to medium size businesses, associations and non-profits in all sectors challenged by data confidentiality problems.

Outcome

- *Build on the success of the data integrity projects to extend the NCCoE's guidance and serve as a basis for other NCCoE projects*
- **2QFY22**: *Draft SP 1800-28 and 1800-29*

Project Status

- Continued development of Data Confidentiality use cases
- Continued bringing in vendors to Data Confidentiality lab environment
- Conducted meetings with vendor collaborators to discuss build architectures for both Data Confidentiality projects
- Working with collaborators to install/configure products
- Generating Part B content

Tags

data security, data confidentiality

Next Steps

- *Continue development of use cases*
- *Continue building reference architecture*
- *Start Drafting Parts B & C*

Challenges or barriers to success

- *Response Time from collaborators*
- *NCCoE Ransomware work*

Project Name: Maritime Transportation Systems

Project Team Leadership: Bill Newhouse and Josie Long (*MITRE TL)* Date: July 13, 2021, Id: 1333ND20FNB770292

Overview /Purpose

Research and development of a CSF Profile, standard best practices, and practical guidance for organizations and stakeholders engaged in operations under the regulatory requirements of the DOE within the maritime environment.

provide support services to determine the maturity of the sector's cybersecurity capabilities using the C2M2. The C2M2 is a voluntary non-attributed approach to improve the security posture of the U.S. energy infrastructure.

Audience

This CSF profile is intended to act as non-mandatory guidance to organizations and stakeholders engaged in the transfer of energy production through intermodal transportation operations within Port facility complexes and offshore platforms

Outcome

- *Collaborate with DOE to develop Liquified Natural Gas (LNG) CSF Profile*
- *Support DOE's development of* Cybersecurity Capability Maturity Model (C2M2) v2
- *Add maritime transportation system and DOE input to the next revision of NIST SP 800–82 Guide to Industrial Control System Security*

Project Status

- *Completed Liquified Natural Gas (LNG) CSF Profile Mission Objective definition and rationales via 3 2-hour workshops*
- *Completed 5 of 6 LNG 2-hour CSF Profile Mission Objective Subcategory Scoring Sessions*
- *Collaborating regularly with DOE leads on C2M2v2 updates enabling CSF mapping efforts to continue when possible, which will result in OLIR C2M2v2 to CSF submission*
- *Since last quarterly offered two Lunch and Learn 90-minute sessions on Liquified Natural Gas Liquification and the alchemy of LNG*

Tags: *CSF profile, ports, liquified natural gas, risk assessment, CSF profile, DOE C2M2, CICAT, MITRE ATT&CK, OLIR*

Next Steps

- *Create draft LNG CSF Profile*
- *Provide MTS Cybersecurity focused feedback to Keith Stouffer and the team of NIST colleagues updating NIST SP 800-82*

Challenges or barriers to success

- *DOE was pushed by the administration to publish C2M2 v2 earlier than scheduled. Disruption of their schedule impacts MITRE mapping efforts as language changes are made in the lead up to C2M2v2 publishing first expected in June now expected July.2021*
- *National Maritime Cybersecurity Plan was posted by last White House administration on January 6 and disappeared from new administration White House webpages on January 15 – MTS not directly called for in recent EO or cyber PCCs*

Research | Define | Assemble | Build | Document | Advocate

Project Name : 5G Cybersecurity

Project Team : J Cichonski, M Bartock, M Souppaya, P Grayeli B Mulugeta, C Teague, S Dey, S Sharma

Date 03/11/2021 Id: 5G

Overview /Purpose

Collaboration with industry to demonstrate how the components of 5G architectures can leverage cybersecurity standards and recommended practices to showcase 5G's robust security features

Audience

- *Commercial Mobile Network Operators*
- *Private Mobile Network Operators*
- *Mobile network users*
- *Mobile network service procurement officers*

Outcome

- *Introduce the use of cutting-edge platform roots of trust capabilities to support and secure mobile network workloads.*
- *Demonstrate security features and capabilities provided by 5G standards and relevant best practice.*

Project Status

- Initiated 5 Focus Working Groups looking at specifics around hardware, software, infrastructure requirements, and architecture for each focus area.
- Published preliminary draft of SP 1800-33A
- Started development of functional demonstration plan
- Initiated deployment of 1 of 3 compute stacks to support the project.
- Working with collaborators to plan deployment of the Ran equipment with NCCoE facility.
- Provisioned remote access to our collaborators to initiate some software deployments.
- Working with facilities to outfit lab with appropriate power capabilities.
- Working with roofing company to mount GPS antenna for timing.
- Continue discussion with collaborators to finalize hardware / software ~~contributions~~ delivery and installations.

Tags

5G, Mobile Network, Trusted Cloud,

Next Steps

- Continue planning / scheduling
- Finalize security capabilities that will be implemented
- Continue the equipment shipment and installation
- Continue configuration and integration
- Continue working on practice guide
- Working on RF chamber and other equipment purchases

Challenges or barriers to success

- *Technology Readiness*
- *Complexity and cost of the proposed build*
- *Maturity of standard*

Blockchain for Supply Chain Traceability

Research | Define | Assemble | Build | Document | Advocate

Project Team Leadership: : Keith Stouffer(NIST PI) Harvey Reed (MITRE TL) Date: July 2021, Id: BN/1333ND20FNB770274

Overview /Purpose

Explore the use of blockchain and alternative mechanisms for industry to address supply chain traceability.

Audience

Supply chain and logistics staff in manufacturing, ICS, and agri-food.

Outcome

- *Provide practical guidance for ICS, manufacturers, and critical infrastructure to improve supply chain traceability.*

Project Status

- The team solicited case studies from the community of interest which illustrate projects using blockchain and related technologies to improve traceability.
- Leveraging team research, applicable guidance, and material gained during Industry Day/Virtual Workshops on Using Blockchain to Improve Manufacturing Supply Chain Traceability, the team is composing a whitepaper to address the findings of using distributed ledgers to address ICS supply chain traceability.
- Team composition: Keith Stouffer, Josh Lubell, Michael Pease, Evan Wallace, Frank Riddick, Harvey Reed, Steve Granata, Vivian Martin, Daniel Eliot, Connor Freeberg, Andrew Noh, Sallie Edwards

Tags

ICS, Blockchain, manufacturing, supply chain assurance, agri-food

Next Steps

- *Complete draft of white paper*
- *Share the draft white paper for NIST peer review with the supply chain team and leadership review.*

Challenges or barriers to success

- *None*

Project Name : Global Position System (GPS) Cyber Security Framework (CSF)

Research | Define | Assemble | Build | Document | Advocate

Project Team Leadership: Matt Scholl (NIST) and John Emilian (MITRE), Date: 14 July 2021, Id: 1333ND21FNB770028

Overview /Purpose

USSF/SMC is seeking to leverage the existing National Institute of Standards and Technology (NIST) Cybersecurity expertise and techniques to identify cybersecurity approaches to increase the resiliency of GPS IT Enterprises that support government and industry sectors.

Audience

Military satellite ground system stakeholders

Outcome

- *Leveraging commercial approaches to military satellite ground/control segment security*
- **GPS CSF Profile**

Project Status

- *Completed delivery #1 – Task 1 – Use Case Documentation (Initial List of GPS IT Enterprise Use Cases)*
- *Held Satellite Ground Segment Cybersecurity Workshop on 25 June*

Tags

Global Positioning System (GPS); Architecture Evolution Program (AEP); satellite ground control; Cyber Security Framework (CSF)

Next Steps

- *Continue development of Deliverable #2 by correlating known adversary ATT&CK activities with categories of Satellite Ground Segment components with the resulting product contributing to a risk assessment for Task 3*
- *Continue development of CSF profile (Task 3)*

Challenges or barriers to success

- *Navigating between NIST unclassified and USSF SMC classified environments*

Project Name : *Detecting and Protecting Against Data Integrity Attacks in Industrial Control Systems Environments*

Research | Define | Assemble | Build | Document | Advocate

Project Team Leadership: *Michael Powell NIST PI, John Hoyt TL, Date July 2021, ID MN*

Overview /Purpose

This project will demonstrate an example solution that manufacturing companies can use to protect the integrity of their information system data from destructive malware, malicious insider attacks threats, advanced persistent threats, and unlicensed unapproved software and other threats.

Audience

- Manufacturing organizations
- Industrial Control Systems (ICS) operators

Outcome

- Introduce practical steps needed to implement the cybersecurity reference design that addresses challenge of protecting ICS against data integrity attacks by cybersecurity technologies & capabilities
- 4QFY21: Publish draft SP 1800-10 for public comment

Project Status

- June 2021 Volume A and Volume B Draft Project Practice Guide for NCCoE. Received comments from CRADA Partners
- July 2021 Volume A and Volume B Draft Project Practice Guide for NCCoE Leadership Review
- July 2021 Volume C Draft Project Practice Guide for CRADA Partners Review

Tags

Manufacturing, ICS network

Next Steps

- *Mid-July: Volumes A and B Internal Review*
- *Late July: Volume C CRADA Partner Review then Internal Review*
- *August: Volumes A and B Release for Public Comment*
- *September: Volume C Release for Public Comment*

Challenges or barriers to success

- *Completing build using WebEx*
- *Some vendor's products must be modified to meet scenarios' testing requirements*

Trusted Cloud

Project Team Leadership: Mike Bartock, Murugiah Souppaya, and Karen Scarfone, ID M0

Research | Define | Assemble | Build | Document | Advocate

Overview /Purpose

Accelerate the adoption of cloud computing technologies by improving the security of cloud technology and establishing a trusted cloud platform to deliver trusted resource pools based on hardware root of trust, data protection, micro-segmentation, and compliance solution

Audience

- NCEPs and cloud technology companies
- Regulated industries like financial services, healthcare, telecommunication, and government

Outcome

- Demonstrate a trusted IaaS hybrid cloud deployment to support virtual machines while continue research/develop prototypes to support containers workload
- 4QFY21: SP 1800-19 and a series of draft NIST IRs supporting hardware-enabled security (NISTIR 8320, 8320A, and 8320B)

Project Status

- Published draft NIST IR 8320 Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for for Cloud and Edge Computing Use Cases
- Published NISTIR 8320A Hardware-Enabled Security: Container Platform Security Prototype
- Completing the draft NIST IR 8320B Hardware-Enabled Security: Policy Based Governance in Trusted Container Platform
- Completing the draft SP 1800-19 Volume C
- Completing implementation of secure enclave to demonstrate protection of private certificate in cloud deployment (NIST IR 8320C)

Keywords

automation; cloud computing; containers; hardware-enable security; hardware root of trust; hybrid cloud; orchestration; virtualization

Next Steps

- Publish complete draft SP 1800-19 Volume A, B, and C
- Publish the draft hardware-enabled security IR 8320s

Challenges or barriers to success

- *Collaborate in-person with external participants at the NCCoE facility*

CSF Intelligent Transportation Systems (ITS)

Research | Define | Assemble | Build | Document | Advocate

Project Leadership Team: Melissa Wong (Volpe PM), Nakia Grayson (NIST PI) Julie Snyder (MITRE PL) ID 1333ND21FNB770118

June 2021

Overview /Purpose

Build upon previous work to support the Intelligent Transportation Systems Joint Program Office (ITS JPO) and Federal Highways Administration (FHWA) with applying the Cybersecurity Framework to the ITS ecosystem.

Audience

State and Local Departments of Transportation decision-makers.

Outcomes

- Cybersecurity Framework Profile for ITS ecosystem ("ITS Profile"), addressing traffic management initially
- Security controls overlays for ITS physical objects
- Guidance to support State and Local ITS practitioners with applying the ITS Profile and security controls baselines

Project Status

- PoP began June 1
- Kick-off held June 17 (formal deliverable)
- Project plan delivered June 30 (formal deliverable)
- Awaiting further direction from USDOT and Volpe regarding ITS Profile
- In the process of planning workshops to obtain stakeholder input

Tags

Cybersecurity Framework Profile, controls overlay, Intelligent Transportation Systems (ITS), ARC-IT, Volpe, USDOT, Federal Highways Administration (FHWA)

Next Steps

- Begin planning workshops to gather stakeholder input
- Identify relevant ITS-related standards to align with the ITS Profile and security controls overlays

Challenges or barriers to success

- *Volpe has not yet identified the offices/program within USDOT with which it needs to coordinate, which is causing delays identifying stakeholders and the scope of the ITS Profile beyond traffic management*

Systems Security Engineering Next Generation Concepts and Methodologies

Project Team Leadership: Dr. Ron Ross (NIST) and Dr. Mark Winstead (MITRE) Date: 8 July 2021, Id:1333ND21FNB770

Overview /Purpose

Update NIST SP 800-160 Volume 1 Systems Security Engineering with lessons learned and advancements, including agile and DevSecOps methodologies

Audience

Systems engineers, security engineers, other engineering professionals with security concerns, project managers.

Outcome*

- Use of systems security engineering in engineering and modifying systems, including with agile methodologies
- **2QFY22**: Draft NIST SP 800-160 Vol 1 Rev 1
- **TBD (Option period)**: Finalized draft
- **TBD (Option period)**: Draft agile development framework

* Dates reflect Admin Mod to contract in process

Project Status

- On contract, team formed
- Initial planning complete
- Early outreach
  - Met with NSA's Standards Center of Excellence
  - Scheduled to brief INCOSE SSE Working Group on 14th
- Identified and acting to update Appendices
  - Will drive updates of chapters 1-3

Tags

Systems Engineering, Systems Security Engineering

Next Steps

- Complete Appendix D Secure By Design
- Update Appendix F Design Principals
- Revise remaining draft to reflect Appendix D & F

Challenges or barriers to success

- Project relies on deep SMEs, who are not plentiful: may be delays or lessened product quality if they become unavailable or less available

Project Name: AFRL Cyber Survivability Attributes (CSA) Tool

Project Team Leadership: *NIST PI Dr. Ron Ross* and Mr. James Reilly (AFRL); *MITRE TL: Linda K. Jones* Date: 14 July 2021, ID: ***1333ND21FNB770008***

Overview /Purpose

Facilitate the adoption of NIST SP 800-160 V2, *Developing Cyber Resilient Systems*, by updating and accelerating the adoption of the AFRL Cyber Survivability Attributes (CSA) Tool

Audience

Systems engineers and systems security engineers who seek to improve the cyber resiliency of enterprise or critical infrastructure systems or the cyber survivability of weapon systems

Outcome

- *Systems engineers use resources (AFRL CSA Tool, publicly released report) for threat-informed rather than compliance-driven engineering*
- **4QFY21** IPD *NIST SP 800-160 v2 Rev 1*

Project Status

- *Obtained public release for MITRE Technical Report (MTR) Cyber Resiliency Approaches and Controls to Mitigate Adversary Tactics, Techniques, and Procedures (TTPs): Mapping Cyber Resiliency to the ATT&CK® Framework – Revision 1*
- *Provided NIST with initial draft of recommendations for NIST 800-160 Vol2 Revision 1. Comments sent back to MITRE.*
- *Completed mappings to ATT&CK v8.2 and the CSEIG* CSAs to 800-53 Rev5 security controls; mappings imported into the AFRL CSA Tool*
- *Completed mappings to ATT&CK v9 but not yet imported into the AFRL CSA Tool*

Tags

Cyber Resiliency Engineering, Systems Engineering, Systems Security Engineering, Cyber Resiliency, Cyber Survivability

Next Steps

- *Update internal draft 800-160 v2 Rev 1 to address comments and ensure consistency with AFRL CSA Tool*
- *Complete cyber hygiene and standard practices mapping*
- *Initiate ATT&CK for Industrial Control Systems (ICS) mapping effort*

Challenges or barriers to success

- *Slow pace of Joint Staff/Community validation of CSEIG CSAs mapping*
- *Synchronization of this work with ATT&CK for ICS evolution*
- *Visibility of cyber resiliency contribution via the AFRL CSA Tool interface deferred pending CNSSI 1253 revision*
- *Looking for opportunities to increase visibility and outreach*

***CSEIG: Cyber Survivability Endorsement Implementation Guide**

Project Name : AI Testbed

Research | Define | Assemble | Build | Document | Advocate

Project Team Leadership: Elham Tabassi, Harold Booth, Tim McBride and Paul Rowe Date: July 13, 2021, ID: NT/1333ND19FNB775320

Overview /Purpose

Create Adversarial Machine Learning (ML) testbed capability to facilitate evaluation of ML algorithms under diverse conditions.

Audience

Those with a need to evaluate security of ML algorithms, examples include but not limited to:

- 2nd party testers
- Adversarial ML researchers
- Standards Developing Organizations

Outcome

- NIST can lead community in best practices and standards for evaluating security of ML algorithms and defensive techniques against attacks.

Next Steps

- Identify users and establish user base
- Feature enhancements to respond to user needs

Project Status

- Base-level capability completed and delivered with documentation covering
  - Background, purpose, scope, etc.
  - Installation, setup, and tutorial walkthroughs
- Outreach activities and materials
  - Presentations to RSA and NIST AI COI
  - Introductory videos
- Open-source release: https://github.com/usnistgov/dioptra

Tags

- Artificial Intelligence (AI), Adversarial Machine Learning (AML), Testing & Evaluation

Challenges or barriers to success

- Users may find the testbed too “heavyweight” for their intended purposes. They may gravitate to alternative frameworks with fewer capabilities.
  - This would promote continued lack of uniform community norms on evaluation best practices.
- We can mitigate this by active user engagement and tight feedback loop.

CURRENT PROJECTS - DOCUMENT

NCCoE ID	Project	PI	PI- All	MITRE PL	Execution Business Model	CRADA Partners
VT/1333ND20FNB770248	Election Security - Voting	Andrew Regenscheid	Gema Howell/Andrew Regenscheid/Jeff Marron/	Carter Casey	Separate TO w/MITRE	n/a
B2	Mobile Device Security: Bring Your Own Device (BYOD)	Gema Howell	Gema Howell	Ken Sandlin	MITRE R&D	International Business Machines (IBM) Corporation Zimperium, Inc. Kryptowire, LLC Lookout, Inc. Qualcomm Technologies, Inc. (QTI) MobileIron, Inc. Palo Alto Networks, Inc.
EI	IIoT DER Cybersecurity – Securing the Industrial Internet of Things	Jim McCarthy	Jim McCarthy	Don Faatz/ Eileen Division	MITRE R&D	Cisco Systems, Inc. Sumo Logic, Inc. Radiflow, Ltd. BlackRidge Technology, Inc. TDi Technologies, Inc. Spherical Analytics Anterix, Inc. University of Maryland (UMD) Xage Security Dots and Bridges, LLC

CURRENT PROJECTS - DOCUMENT

NCCoE ID	Project	PI	PI- All	MITRE PL	Execution Business Model	CRADA Partners
RT	Supply Chain Assurance: Validating the Integrity of Servers and Client Devices project	Nakia Grayson	Nakia Grayson	Chris Brown	MITRE R&D	Eclypsium, Inc. Seagate Federal, Inc. (dba Seagate Government Solutions) HP Inc UK Ltd Hewlett Packard Enterprise Company (HPE) RSA Security LLC Intel Corporation Dell Technologies, Inc.
HT	Securing Telehealth Remote Patient Monitoring (RPM)	Ron Pulivarti	Jen Cawthra/Nakia Grayson/Ron Pulivarti	Sue Wang	MITRE R&D	Accuhealth Technologies, LLC INOVA Health System Tenable, Inc. LogRhythm, Inc. Cisco Systems, Inc. University of Mississippi Medical Center (UMMC) Vivify Health, Inc. MedCrypt, Inc. MedSec LLC Onclave Networks, Inc.

Project Name : Election Security - Voting

Research | Define | Assemble | Build | Document | Advocate

Project Team Leadership: Andy Regenschied, Gema Howell (NIST) and Carter Casey(MITRE),

Date: July 2021. Id: VT/1333ND20FNB770248

Overview /Purpose

Provide cybersecurity expertise to support the Voluntary Voting System Guidelines (2.0) implementation guidance, an online infrastructure threat analysis, and to develop executive level guidance for election officials

Audience

Voting technology vendors, voter registration system vendors, state & local election officials; Election Assistance Commission

Outcome

- Long-term impact: to improve the cybersecurity of voting and non-voting technologies that enable and underpin the U.S. elections infrastructure

Project Status

- Completed VVSG 2.0 *Wireless* implementation guide
- Drafted VVSG 2.0 *Airgap* implementation guide
- Completed 3 election security guides and infographics: Trustworthy Email, Multifactor Authentication (MFA), and Data Security and Recovery
- Created a Visual Aid/Social Media Video for the Election security guides

Tags

Election, cybersecurity, voting technologies, non-voting technologies

Next Steps

- Complete other VVSG Implementation Guides: *Auditing, Digital Signatures, E2E verifiable, Identifiers*
- Complete online infrastructure threat analysis
- Create another visual aid to summarize voting guidance

Challenges or barriers to success

- N/A

Mobile Device Security for Enterprises

Research | Define | Assemble | Build | Document | Advocate

Project Team Leadership: *Gema Howell (NCCoE) / Ken Sandlin (MITRE)* Date: July 13, 2021 Id: B2

Overview /Purpose

Reasonable security & privacy controls for using mobile devices in the enterprise

Audience

Almost any type of organization from Government or Private Sector, from nearly any domain (e.g., Healthcare, Financial, etc.)

Outcome

- *Help organizations increase security and privacy when deploying personally owned devices*
- *SP 1800-22 Mobile Device Security: Bring Your Own Device (BYOD)*
    - *Includes new format Supplement demonstrating how an example organization could successfully use the publication; expanded Privacy material as well*

Project Status

- *1800-22 BYOD (Draft) public comment period ended May 17*
- *Recent Outreach:*
    - *Federal Mobility Group presentation in early April;*
    - *April, May and June NCCoE webinars broke previous mobile device attendance records, all with really good engagement from attendees*
- *April's webinar polling questions = great input for future publications*
- *Adjudicated public comments: updating 1800-22*

Tags

Mobile device, mobile device management; mobile device security, bring your own device; BYOD, cybersecurity

Next Steps

- *Short form paper consideration for Unified Endpoint Management / Zero Trust. Coordinating with Zero Trust Team*
- *Renewing CRADAs*
- *Moving 1800-22 from Draft to Final*

Challenges or barriers to success

- *CRADA renewals – 3 out of 8 collaborators have not replied to the request to extend the CRADA*

Project Name : Energy IIoT DER Cybersecurity

Research | Define | Assemble | Build | Document | Advocate

Project Team Leadership: Jim McCarthy and Eileen Division Date 07/13/2021 Id: EI

Overview /Purpose

This project applies cybersecurity best practices and technology to protect the digital communication and control of cyber-physical grid edge devices while also providing an immutable record of commanded actions and responses across all devices.

Audience

Distributed energy resource owners/operators – primarily utility-scale, commercial-scale, and microgrid/campus distributed energy resource owners/operators

Outcome

- *Enable secure, large-scale integration of distributed energy resources into the power grid*
- *Final SP 1800-32 Q1 FY22*

Project Status

- *Completed adjudication of pre-release (Parts A&B) draft comments*
- *Submitted Parts A,B,C for initial tech editing review*
- *Also adding to Part C as tech review takes place*
- *Plan is to have to adjudicated Final draft to ERB on 09/17/2021*

Tags

energy; IIoT; distributed energy resources; microgrid

Next Steps

- *Complete draft based on pre-release draft comments*
- *Full draft (A,B,C) release to public August 2021*
- *Final publication October 2021*

Challenges or barriers to success

- *None*

Supply Chain Assurance: Validating the Integrity of Computing Devices

Project Team Leadership: Nakia Grayson (NIST PI), Andy Regenscheid, Murugiah Souppaya, Tyler Diamond, & Chris Brown (MITRE TL), Chelsea Deane, Thomas Walters, 7/9/2021 ID: RT

Overview /Purpose

- Use hardware root of trust to measure, validate and detect malicious component swaps during product acceptance /server manufacturers)

Audience

- Supply chain companies (client/server manufacturers), Original Equipment Manufacturers (OEMs) , Third-party Component Suppliers

Outcome

- *Long-term desired outcome: help organizations achieve better visibility into supply chain attacks and detect advanced persistent threats.*
- *Preliminary Draft SP 1800-34 B <FY 21, Early Quarter 3*

Project Status

- Adjudicated comments received on Volume A preliminary draft
- Working on Volume B and C preliminary draft and routing to Karen Scarfone, collaborators and then leadership for feedback
- Laptop Build will be included in preliminary draft and Server Build will be included in draft
- Continue bi-weekly joint collaborator meetings and separate workstreams to discuss build workstreams and project status
- Conclude Laptop Build Phase and continue working to finalize Server Build

Tags

Supply chain; hardware roots of trust

Next Steps

- Finalize and submit collaborators panel proposal for RSA Conference
- Publish Preliminary Drafts Volume B and C
- Move Volume A to Draft status

Challenges or barriers to success

- Manufacturer solutions are at various stages of maturity and some are in the proof-of-concept stage

Project Name : Telehealth-Remote Patient Monitoring

Project Team Leadership: *Ron Pulivarti and Sue Wang* Date: July 2021, Id: HT

<Graphical representation of the project phase. Select Blue – completed, Grey – current, Unfilled – not started>

Overview /Purpose

Create an example solution to address the cybersecurity challenges of a telehealth RPM ecosystem. Driven by HC-COI.

Audience

Healthcare providers who are interested in developing a new telehealth program or enhance an existing telehealth service with cybersecurity and privacy principles

Outcome

- *Increased awareness and adoption of NCCoE-provided cybersecurity and privacy solutions as healthcare providers implement or expand telehealth programs.*
- ***Publication: 3QFY21:*** *2nd Draft SP 1800-30*
- ***Target publication: 2QFY22:*** *Final SP 1800-30*

Project Status

- *Presented at RSA21, AAMI21, and HIPAA summit and will present at HIMSS21*
- *Published 2nd draft of SP 1800-30 with incorporated NIST IoT team's input and privacy team's input*

Tags

access control; authentication; authorization; behavioral analytics; cloud storage; data privacy; data security; encryption; HDO; healthcare; healthcare delivery organization; remote patient monitoring; RPM; telehealth

Next Steps

- *Adjudicate public comments for the 2nd draft, update PG and prepare for ERB process*
- *Complete ERB process and publish Final SP 1800-30*
- *Continue to advocate and educate HDOs and Health IT security professionals in adopting SP 1800-30*

Challenges or barriers to success

- *The pandemic limited availability of some vendors who were directly involved in the pandemic response. This slowed the initial engagement.*

CURRENT PROJECTS - ADVOCATE

NCCoE ID	Project	PI	PI- All	MITRE PL	Execution Business Model	CRADA Partners
1333ND20FNB670037	Public Safety Communications Research (PSCR)	Bill Fisher	Bill Fisher	Sudhi Umarji	Separate TO w/MITRE	
DI	Data Security – Data Integrity	Bill Fisher	Bill Fisher/Jen Cawthra	Michael Ekstrom	MITRE R&D	Cryptonite, LLC Tripwire, Inc. Cisco Systems, Inc. Micro Focus Government Solutions Semperis, Inc. Glasswall Government Solutions, Inc. GreenTec-USA, Inc. Symantec Corporation International Business Machines (IBM) Corporation Hewlett Packard Enterprise Company (HPE) Veeam Software AG
PM	Securing Property Management Systems	Bill Newhouse	Bill Newhouse	Jeff Finke	MITRE R&D	StrongAuth, Inc. Intelligent Automation, Inc. (fka Cryptonite, LLC) Remediant, Inc. TDi Technologies, Inc. ForeScout Technologies, Inc.

CURRENT PROJECTS - ADVOCATE

NCCoE ID	Project	PI	PI- All	MITRE PL	Execution Business Model	CRADA Partners
ME	Mobile Devices Security: Corporate-Owned Personally Enabled (COPE)	Gema Howell	Gema Howell	Ken Sandlin	MITRE R&D	International Business Machines (IBM) Corporation Zimperium, Inc. Kryptowire, LLC Lookout, Inc. Qualcomm Technologies, Inc. (QTI) MobileIron, Inc. Palo Alto Networks, Inc.
NV	PNT work	Jim McCarthy	Jim McCarthy	Theresa Suloway	MITRE R&D	n/a
1333ND20FNB770143	DHS Continuous Diagnostics and Mitigation Task	Mai Nguyen	Mai Nguyen	Cassandra Browning	Interagency/DHS	n/a
PQ	Securing Picture Archiving and Communication System (PACS)	Ron Pulivarti	Jen Cawthra/Nakia Grayson	Sue Wang	MITRE R&D	Cisco Systems, Inc. Hyland Software, Inc. DigiCert, Inc. Clearwater Compliance, LLC Philips Healthcare TDi Technologies, Inc. ZingBox, Inc. Tempered Networks, Inc. ForeScout Technologies, Inc. Virta Laboratories, Inc. Tripwire, Inc. Microsoft Corporation Broadcom

Project Name: Public Safety Task Order

Research | Define | Assemble | Build | Document | Advocate

Project Team Leadership: Bill Fisher (NIST PI) Sudhi Umarji (Mitre TL)

Date: July 2021. Id: 1333ND20FNB670037

Overview /Purpose

Helping the Public Safety community adopt security standards and best practices, specifically in the Identity, Credential and Access Management space.

Audience

Public Safety decision makers & technologists

Outcome

- *Standards and Best Practice Adoption*
- *Education on Risk Based Decision Making around ICAM technologies*

Project Status

- *Working on three documents right now:*
  - *Using Mobile Device Biometrics for Authenticating First Responders – Published Draft*
  - *Identity as a Service (IDaaS) for the Public Safety and First Responder Community – Published Draft*
  - *Using Identity Federation Technology to Achieve Public Safety Missions – Published Draft*
- *Lab environment update:*
  - *Deploying public safety technologies including: MS Azure and Datamaxx deployed, Axon, working on CAD/RMS vendor*

Next Steps

- *Each document will be sent for review by the following parties:*
  - *Adjudicate public comments*

Challenges or barriers to success

- *Any community objection to document contents*
- *Any ERB complications*

Project Name : Data Integrity

Define | Assemble | Build | Document | Advocate

Project Team Leadership: Jennifer Cawthra and Anne Townsend Date: July 2021, Id: DI

Overview /Purpose

Identify, Protect, Detect, Respond to and Recover from data attacks that lead to compromised integrity. Three separate projects originating from FS-ISAC and Malware Task Force.

Audience

Small to medium size businesses, associations and non-profits in all sectors challenged by data security problems such as ransomware or malware

Outcome

- *Be a foundation for NCCoE that demonstrates the impact 1800 series projects may have while also being a building block for other NCCoE projects*
- **1QFY21**: *Final SP 1800-11,1800-25 and 1800-26*

Project Status

- SP *1800-25* Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events – Final as of 12/2020
- *SP 1800-26 Detecting and Responding to Ransomware and Other Destructive Events – Final as of Dec 2020*

Tags: *data security, data integrity, ransomware*

Next Steps

- *Advocate*

Challenges or barriers to success

- *None*

Property Management Systems

Project Team Leadership: Bill Newhouse (NIST), Technical Lead: Jeff Finke (MITRE); July 13, 2021 Id: PM

Overview / Purpose

- *Push for adoption of standards-based approaches to help hospitality organization meet their cybersecurity needs for protecting property management systems.*

Audience

- *Those within organizations who seek to mitigate cybersecurity and privacy risks to their property management system (PMS) and the connected system to the PMS*

Outcome

- *A PMS reference design which incorporates aspects of zero trust architecture, moving target defense, and data tokenization to reduce cybersecurity and privacy risk for a hotel's PMS, and inspires the hospitality sector to adopt the documented best practices.*

Project Status

- *Final NIST SP 1800-27 was published on March 30, 2021 along with video.*
- *Bill Newhouse attended an Hospitality and Technology Professionals (HFTP®) Hangout where he led an interactive discussion on the NCCoE, our hospitality and financial services activities, and the Property Management System practice guide.*
- *John Bell, an expert contributor to our project, drafted an article that references our practice guide and zero trust for Hospitality Upgrade magazine .*

Tags *access control, hospitality cybersecurity, moving target defense, PCI DSS, PMS, privacy, property management system, role-based authentication, tokenization, network security, zero trust architecture*

Next Steps

- *Track Retail Hospitality – ISAC and Hospitality Technology Next Generation membership groups to listen for opportunities to draw their members to NIST SP 1800-27 Securing Property Management Systems and to listen for potential projects in this space for the NCCoE.*

Challenges or barriers to success

- *Hospitality industry hard hit by COVID-19.*

Mobile Device Security for Enterprises

Research | Define | Assemble | Build | Document | Advocate

Project Team Leadership: *Gema Howell (NCCoE) / Ken Sandlin (MITRE)* Date: March 19, 2020, Id: ME

Overview /Purpose

Reasonable security & privacy controls for using mobile devices in the enterprise

Audience

Almost any type of organization from Government or Private Sector, from nearly any domain (e.g., Healthcare, Financial, etc.)

Outcome

- *Help organizations increase security and privacy when deploying organizationally owned devices*
- *Deliverables:*
  - *Final SP 1800-21 Mobile Device Security: Corporate-Owned Personally-Enabled (COPE) published*

Project Status

- *1800-21 COPE (Final): PDFs were published in September; web version and updated PDFs posted February 2021*
- *Outreach Videos published to NIST YouTube channel*

Tags

- *Corporate-owned personally-enabled; COPE; mobile device; mobile device management; mobile device security, cybersecurity*

Next Steps

- *Continue Outreach and Engagement along with 1800-22's O&E activities*
- *Considering future webinars/events to share guidance*

Challenges or barriers to success

- *High focus and demand for BYOD has led to limited outreach and engagement for COPE*

Project Name : PNT Profile Development

Research | Define | Assemble | Build | Document | Advocate

Project Team Leadership: Jim McCarthy and Theresa Suloway Date: 07/13/2021 Id: NV

Overview /Purpose

This is a NIST project which addresses Executive Order (EO) 13905, Strengthening National Resilience Through Responsible Use of Positioning, Navigation and Timing (PNT). NIST is required to have a PNT profile published by 02/12/2021.

Audience

All users of PNT services, PNT technology vendors, Federal agencies, any interested members of the public

Outcome

- *A Cybersecurity Framework (CSF) based profile for users to assess their risk and strengthen the security of their PNT services and data. .*
- *PNT Profile Public release – 02/11/2021*

Project Status

- *Through Profile Publication, have assisted Fed agencies with developing plans for Cybersecurity profile(s) – TSA*
- *Provided PNT Profile briefing to private sector (Orolia) 03/20210*
- *RSA 2021 – Virtual RSA presentation provided 05/2021 (NIST / DHS CISA co-presentation)*
- *Assisting DHS / CISA with development of their own PNT Profile for Sector Risk Management Agencies (SRMAs)*

Tags

Positioning, Navigation, Timing, Executive Order 13905

Next Steps

- *Continue NIST representation and involvement in public and private sector specific Profile development.*
- *EO 13905 calls for NIST to update PNT Profile every two years or as needed.*
- *Begin assembling team for 2-year update Q2 FY2022*

Challenges or barriers to success

- *None foreseen at this time.*

Project Name : NCCoE/DHS Continuous Diagnostic & Mitigation (CDM) Dashboard

Project Team Leadership: Mai Nguyen, *NCCoE COR; Rita Wilson, DHS COR* and Dr. Cassie Browning, *MITRE PL – April 2021*

Overview /Purpose

- The DHS CISA (Cybersecurity and Infrastructure Security Agency) CDM dashboard is used as a dashboard to connect to civilian federal agencies to help agencies produce customized reports and to alerts analysts to the most critical cybersecurity risks.
- This tool also consolidates summary information from each agency's dashboard to a ***federal generic/demo/beta dashboard providing a picture of cybersecurity status across all civilian agencies.***
- The NCCoE/MITRE CDM team provides support services to develop, design, implement, and maintain a current generic CDM dashboard for concept exploration, technology analysis, and integration lessons learned.

Outcome: *Deliver automated tools to federal agencies to strengthen their ability to monitor and manage the threat of cyber vulnerabilities*

Project Status

- *Completion of POP with 109 user stories/tasks/projects completed. SOW required 35.*
- *Cloud team delivered a whitepaper which explained cloud risk for AWS, Azure and M365, as a reference architecture for system integrators.*
- *Dashboard team upgraded the ECE platform to a later version so that it will resolve some of the known issues and support the later CDM releases.*
- *Lab team deployed several new capabilities for lab virtual machines, such as AWX accessibility.*
- *Tools and Expertise team delivered a report on Tanium's unauthorized users lessons learned.*
- *Mobile team delivered several reports such as types of cyber-related risk/threats the MAV tool identify.*

Next Steps

- *As of April 30, 2021, waiting contract renewal for next period of performance.*

Challenges or barriers to success

- *Delays in DHS security processing limits who can access the DHS Jira board for task management.*
- *Contractual gap impacts technical staff retention*

Project Name : Picture Archiving & Communication System (PACS)

Research | Define | Assemble | Build | Document | Advocate

Project Team Leadership: *Ron Pulivarti and Sue Wang* Date: July 2021, Id: HT

Overview /Purpose

Develop an example solution for HDOs that addresses the cybersecurity challenges surrounding the PACS ecosystem.

Audience

HDOs and Health IT security professionals who seek to protect the PACS ecosystem from cybersecurity risks

Outcome

- *Adoption of the principles in this guide to better protect their enterprise architecture and patient data from cybersecurity risks.*
- ***Publication: 1QFY21**: Final NIST SP 1800-24*
- ***Target Publication: 4QFY21**: Interactive Securing PACS PG*

Project Status

- *Develop Interactive Securing PACS Practice Guide*

Tags

access control; auditing; authentication; authorization; behavioral analytics; cloud storage; DICOM; EHR; electronic health records; encryption; microsegmentation; multifactor authentication; PACS; PAM; picture archiving and communication system; privileged account management; vendor neutral archive; VNA

Next Steps

- *Continue to advocate and educate HDOs and Health IT security professionals in adopting SP 1800-24*
- *Publish Interactive Securing PACS Practice Guide during week of July 19th*

Challenges or barriers to success

- *None*

NATIONAL CYBERSECURITY EXCELLENCE PARTNERS

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Natalia Martin, Acting Director

nccoe.nist.gov

@NISTcyber