USE CASE | Healthcare

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

PICTURE ARCHIVING COMMUNICATION SYSTEM

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of securing the Picture Archiving and Communication System (PACS) ecosystem in Healthcare Delivery Organizations (HDOs) by collaborating with industry and the information technology community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the Healthcare PACS project, including its background and challenge, approach, and benefits. If you have feedback on the architecture or the relevance and usefulness of this practice guide, please contact us at hit_nccoe@nist.gov.

BACKGROUND

Medical imaging plays an increasingly important role in diagnosing and treating patients. PACS facilitates medical image management. Over the past few decades, imaging technology has evolved from physical film to digital images which may be stored or shared across different departments or other care teams. PACS acts as a medical imaging central storage and repository and acts as a core component for Radiology and other image-intensive clinical departments. PACS interoperates with other clinical systems such as the electronic health record system, hospital information system, or other clinical systems with which an HDO integrates.

CHALLENGE

PACS, by its nature, is a system that cannot operate in isolation. The overall PACS ecosystem consists of diverse technologies that include medical imaging devices, patient registry systems, and worklist management systems. PACS also relies on systems to manage and maintain medical image archives, which may include cloud storage capabilities. The primary role of PACS is interaction with disparate medical imaging devices, interconnectivity with other clinical systems, and allowing a geographically and organizationally diverse team of healthcare professionals to review medical images to provide quality and timely patient care. Therefore, the threat landscape is broad, and allows for a large attack surface. The PACS environment may include vulnerabilities. Unauthorized individuals may leverage vulnerabilities and compromise or corrupt stored information. Also, unauthorized individuals may use components found in the PACS ecosystem as pivot points to further compromise components in an integrated healthcare information system.

APPROACH

This project demonstrates how an organization may implement a solution to mitigate identified risks. The reference architecture includes technical and process controls to implement:

- a defense-in-depth solution, including network zoning practices that allows more granular control of network traffic flows and limits communications capabilities to the minimum necessary to support business function
- access control mechanisms that include multifactor authentication for care providers, certificate-based authentication for imaging devices and clinical systems, and mechanisms that limit vendor remote support to medical imaging components
- a holistic risk management approach that includes medical device asset management that augments enterprise security controls, and leveraging behavioral analytic tools for near real-time threat and vulnerability management in conjunction with managed security solution providers

BENEFITS

The NCCoE's practice guide, *Securing Picture Archiving and Communication System*, can help your organization:

- improve resilience in the network infrastructure, including limiting a threat actor's ability to leverage components as pivot points to attack other parts of the HDO's environment
- limit unauthorized movement within the HDO environment by authorized system users to address the "insider threat" as well as limit unauthorized actors once they gain network access
- analyze behavior and detect malware throughout the ecosystem to enable HDOs to determine when components

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

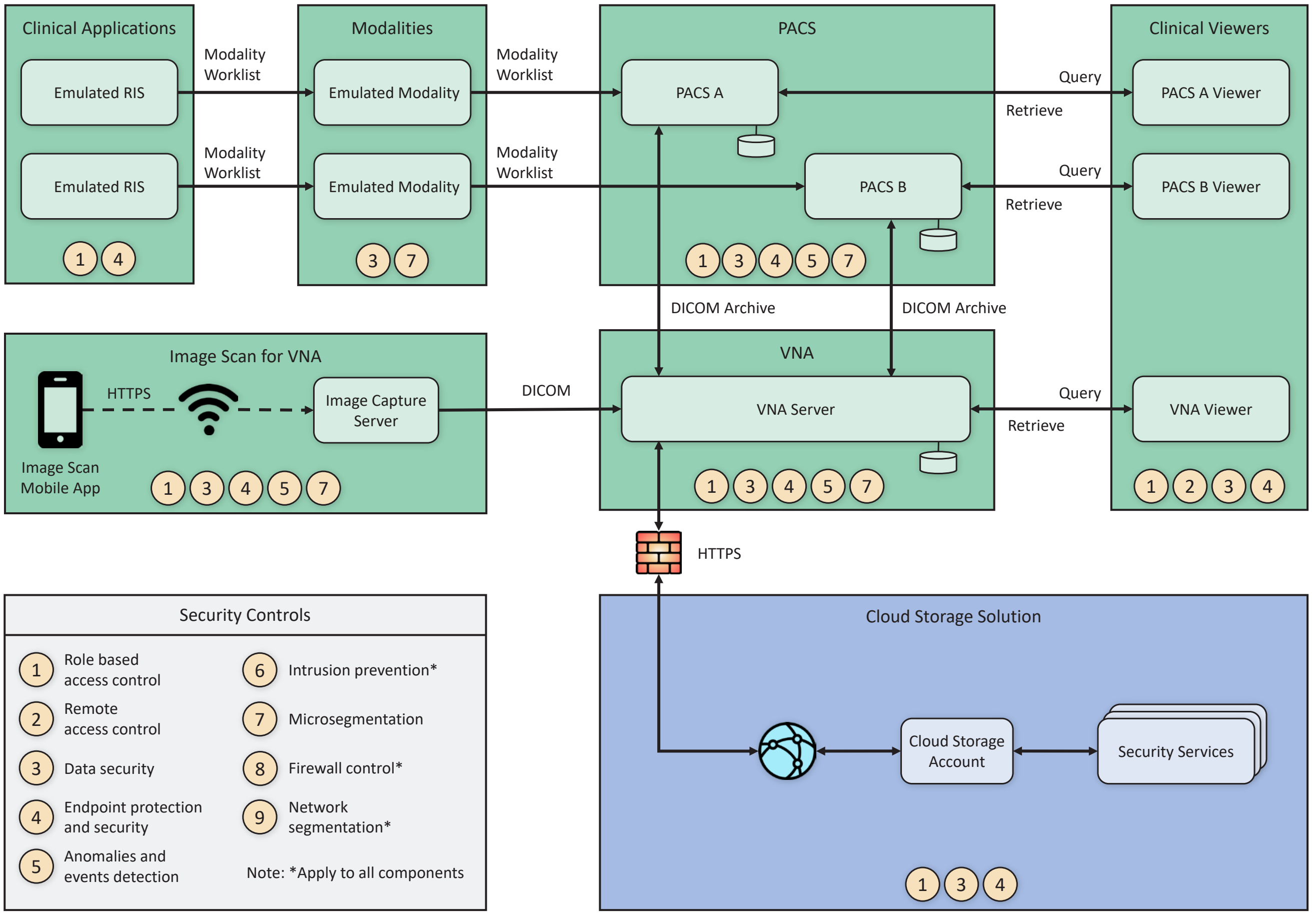
LEARN MORE ABOUT NCCOE
Visit https://www.nccoe.nist.gov

CONTACT US
hit_nccoe@nist.gov
301-975-0200

evidence compromise and to enable those organizations to limit the effects of a potential advanced persistent threat such as ransomware

- secure sensitive data (e.g., personally identifiable information or protected health information) at rest, in transit, and in cloud environments; enhancing patient privacy by limiting malicious actors' ability to exfiltrate or expose that data
- consider and address risks that may be identified as HDOs examine cloud storage solutions as part of managing their medical imaging infrastructure
- helps protect patient privacy

HIGH-LEVEL ARCHITECTURE



COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

CISCO · CLEARWATER COMPLIANCE · digicert · FORESCOUT · Hyland · Microsoft · PHILIPS

Symantec · tdi technologies · TEMPERED NETWORKS · tripwire · VIRTA LABS · Zingbox

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

DOWNLOAD THE PRACTICE GUIDE

For more information about this project, visit https://www.nccoe.nist.gov/projects/use-cases/health-it/pacs.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have questions about this project or would like to join the Healthcare Community of Interest, please email hit_nccoe@nist.gov.

December 2020