BUILDING BLOCK

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DATA INTEGRITY

Identifying and Protecting Assets Against Ransomware and Other Destructive Events

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenges associated with identifying and protecting an organization's assets from data integrity destructive events by collaborating with industry and the information technology community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the Identifying and Protecting Assets Against Ransomware and Other Destructive Events Project, including background, challenge, goals, and benefits. If you would like to propose any changes or know of products that might be applicable to this challenge, please contact us at ds-nccoe@nist.gov.

BACKGROUND

Ransomware, destructive malware, malicious insider activity, and user errors can potentially harm an organization's infrastructure and compromise or destroy valuable data such as database records, system files, configurations, and customer information.

Organizations can reduce the likelihood of such events by implementing a cyber defense strategy that includes maintaining awareness of organizational assets, identifying and mitigating potential attack vectors, making backups, and generally implementing procedures prior to an attack to ease detection, response, and recovery.

CHALLENGE

Creating a cyber defense strategy requires a combination of technical expertise, time, and resources, which are often scarce in small- and medium-size organizations. For instance, the first step in building a strategy requires an organization to inventory its assets. This involves identifying systems, applications, data sources, users, and other relevant entities and also identify vulnerabilities within these assets that may enable them to become targets or facilitators of data integrity attacks. Once this exercise is complete, an organization can then create a customized strategy to protect the identified assets against the possibility of data corruption, modification, and/or destruction.

GOAL

This project aspires to empower organizations by providing them with readily available solutions that they can use to protect their assets. These solutions will include, but are not limited to, inventorying, file integrity monitoring, backup, secure storage, auditing, vulnerability management, and policy enforcement.

BENEFITS

By having a cyber defense strategy in place, organizations can:

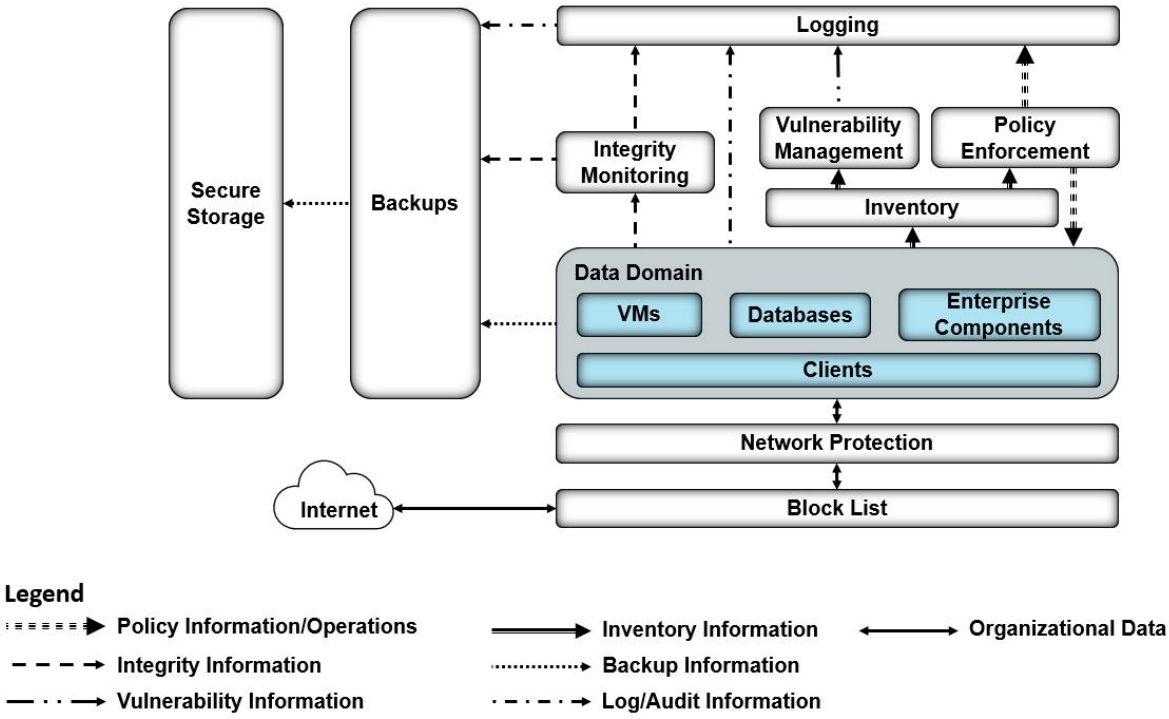
- develop an inventory solution
- baseline systems prior to an attack
- protect assets against attacks
- protect its data/infrastructure
- identify and analyze vulnerabilities prior to an attack
- build a policy enforcement solution to manage software versioning and patch distribution

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://nccoe.nist.gov

CONTACT US
ds-nccoe@nist.gov
301-975-0200

HIGH-LEVEL ARCHITECTURE



The above figure identifies a high-level architecture of the enterprise system and the associated components for this project. During the development of the laboratory environment implementing this project, the figure was refined to describe detailed components and mapped to the physical architecture in the lab environment for the specific scenario being implemented. A goal of this figure is to help spur identification of project participants and hardware and software components for collaborative use in a laboratory environment to build open, standards-based, modular, end-to-end reference designs.

TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution. Technology collaborators on this project include:

Certain commercial entities, equipment, products, or materials may be identified in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

DOWNLOAD THE PROJECT DESCRIPTION

For more information on this and other Data Security projects, visit: https://www.nccoe.nist.gov/projects/building-blocks/data-security.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you are interested in contributing technology or expertise to this project, please email ds-nccoe@nist.gov.