NIST SPECIAL PUBLICATION 1800-26A

Data Integrity

Detecting and Responding to Ransomware and Other Destructive Events

Volume A:
Executive Summary

Jennifer Cawthra
National Cybersecurity Center of Excellence
NIST

Michael Ekstrom
Lauren Lusty
Julian Sexton
John Sweetnam
Anne Townsend
The MITRE Corporation
McLean, Virginia

January 2020

DRAFT

This publication is available free of charge from https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond.

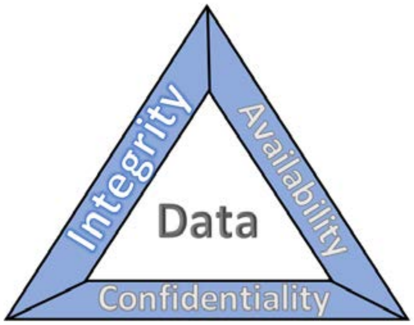
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Executive Summary

The CIA triad represents the three pillars of information security: confidentiality, integrity, and availability, as follows.

- Confidentiality – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- Integrity – guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity
- Availability – ensuring timely and reliable access to and use of information



This series of practice guides focuses on data integrity: the property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. (Note: These definitions are from National Institute of Standards (NIST) Special Publication (SP) 800-12 Rev 1, *An Introduction to Information Security*.)

- Destructive malware, ransomware, malicious insider activity, and even honest mistakes all set the stage for why organizations need to quickly detect and respond to an event that impacts data integrity. Businesses must be confident that these events are detected quickly and responded to appropriately.

- Attacks against an organization's data can compromise emails, employee records, financial records, and customer information—impacting business operations, revenue, and reputation.
- Examples of data integrity attacks include unauthorized insertion, deletion, or modification of data to corporate information such as emails, employee records, financial records, and customer data.
- The National Cybersecurity Center of Excellence (NCCoE) at NIST built a laboratory environment to explore methods to effectively detect and respond to a data integrity event in various information technology (IT) enterprise environments, to immediately react to the event in an effort to prevent a complete compromise.
- This NIST Cybersecurity Practice Guide demonstrates how organizations can develop and implement appropriate actions during a detected data integrity cybersecurity event.

CHALLENGE

Some organizations have experienced systemic attacks that force operations to cease. One variant of a data integrity attack–ransomware–encrypts data, leaving it modified in an unusable state. Other data integrity attacks may be more dynamic, targeting machines, spreading laterally across networks, and continuing to cause damage throughout an organization. In either case, behaviors are exhibited—such as files inexplicably becoming encrypted or network activity—that provide an ability to immediately detect the occurrence and respond in a timely fashion to curtail the ramifications.

SOLUTION

NIST published version 1.1 of the Cybersecurity Framework in April 2018 to provide guidance on protecting and developing resiliency for critical infrastructure and other sectors. The framework core contains five functions, listed below.

- **Identify** – develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities
- **Protect** – develop and implement appropriate safeguards to ensure delivery of critical services
- **Detect** – develop and implement appropriate activities to identify the occurrence of a cybersecurity event
- **Respond** – develop and implement appropriate activities to take action regarding a detected cybersecurity incident
- **Recover** – develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY
FRAMEWORK
VERSION 1.1

For more information, see the Framework for Improving Critical Infrastructure Cybersecurity v1.1.

Applying the Cybersecurity Framework to data integrity, this practice guide informs organizations of how to quickly **detect** and **respond** to data integrity attacks by implementing appropriate activities that immediately inform about the data integrity events.

The NCCoE developed and implemented a solution that incorporates multiple systems working in concert to **detect** an ongoing data integrity cybersecurity event. Additionally, the solution provides guidance on how to **respond** to the detected event. Addressing these functions together enables organizations to have the necessary tools to act during a data integrity attack.

The NCCoE sought existing technologies that provided the following capabilities:

- event detection
- forensics/analysis
- integrity monitoring
- logging
- mitigation and containment
- reporting

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

BENEFITS

The NCCoE's practice guide to Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events can help your organization:

- develop a strategy for detecting and responding to a data integrity cybersecurity event
- facilitate effective detection and response to adverse events, maintain operations, and ensure the integrity and availability of data critical to supporting business operations and revenue-generating activities
- manage enterprise risk (consistent with foundations of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*)

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at ds-nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations 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). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

CISCO GLASSWALL MICRO FOCUS SEMPERIS Symantec. tripwire

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order 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.

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

Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200