BUILDING BLOCK

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DATA INTEGRITY

Detecting and Responding to Ransomware and Other Destructive Events

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of detecting and responding to malicious malware and other damaging attacks by collaborating with industry and the information technology (IT) community, including cybersecurity solutions vendors. This fact sheet provides an overview of the Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events project, including background, challenges, goals, and potential benefits. For more information about this project, visit: https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond.

BACKGROUND

No organization is immune from cybersecurity threats and attacks, which can range from minor inconveniences to major catastrophic events that may take months—sometimes years—to overcome. Events such as ransomware, destructive malware, insider threats, and even honest mistakes, can threaten an organization's infrastructure, not to mention its most valuable asset—its reputation. Moreover, database records and structures, system files, configurations, user files, application code, and customer data are all at risk should an event occur.

Cyber threats are not abating, rather they are increasing and becoming more complex, pervasive, and damaging. Organizations that lack detection and response solutions are highly vulnerable to any number and types of data integrity events. This project aspires to assist organizations with addressing this challenge.

CHALLENGE

The process of mitigating an active attack on an organization's data integrity requires the use of stronger, more effective tools. Detection of a data integrity attack involves the identification of its source, the affected systems, and sufficient data collection to allow for impact analysis. Compromise can come from malicious websites, targeted e-mails, insider threats, and honest mistakes. Once detected, swift response to a threat is critical to mitigate the need for recovery action after an event occurs. Typical responses to active attacks can involve various forms of mitigation, such as network quarantining or account management. Forensics can be used to determine the impact of an attack, and analysis allows the organization to learn and improve their defenses. The implementation of these defenses allows an organization to monitor their systems for the signs of an attack and respond appropriately.

GOAL

This project aims to empower organizations by providing them readily available solutions they can use to detect and respond to compromises of data integrity. These solutions will include, but are not limited to, integrity monitoring, event detection, logging, reporting, forensics, mitigation, and vulnerability management.

BENEFITS

By implementing this example solution, organizations can:

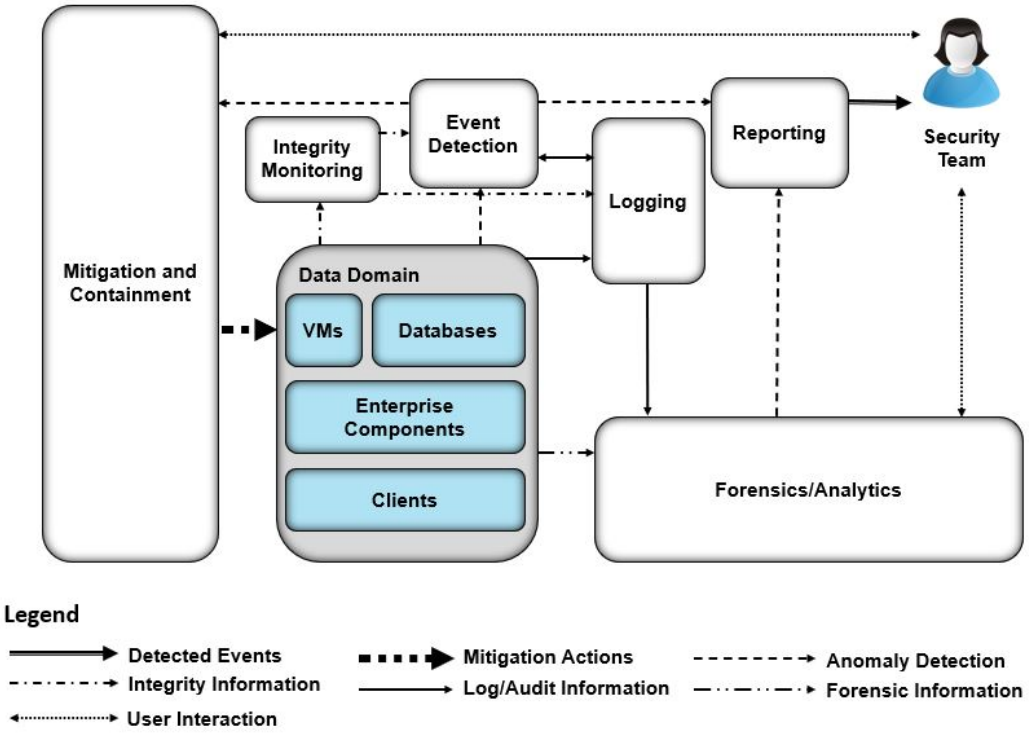
- become aware of data integrity events as they occur
- analyze, mitigate, and then contain data integrity events
- minimize any impact on worker productivity
- reduce or avoid financial and reputational damage

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



Component List

Data integrity solutions for this project include, but are not limited, to:

- integrity monitoring
- event detection
- malicious software detection
- unauthorized activity detection
- anomalous activity detection
- logging and data correlation software
- reporting capability
- vulnerability management
- forensics/analytics tools
- mitigation and containment software

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 about this project, visit: https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. Share your knowledge and expertise by joining the Data Integrity Community of Interest—send an email to ds-nccoe@nist.gov.

June 2020