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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DATA CONFIDENTIALITY: DETECT, RESPOND TO, AND RECOVER FROM DATA BREACHES

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of protecting data from unauthorized access and disclosure. This effort is being conducted through collaborative efforts with industry and the information technology (IT) community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the *Data Confidentiality: Detect, Respond to, and Recover from Data Breaches* project, including background, challenges, goals, and potential benefits. If you would like to propose another architecture or know of products that might be applicable to the challenge, please contact us at ds-nccoe@nist.gov

CHALLENGE

An organization's data is one of its most valuable assets and reacting to a data breach requires quick and diligent action. Large and small data breaches threaten the function and survival of an organization. As a data beach is occurring, it is critical to know if your operational, financial, employee, or customer data is being affected, and how to stop it. An inadequate breach response can lead to lingering issues and severe reputational damage.

GOAL

The goal of this project is to provide a practical solution to detect, respond to, and recover from incidents that affect data confidentiality. This project will also provide guidance on data confidentiality that parallels the *Identifying and Protecting Assets and Data Against Data Breaches* project. The NCCoE chose to address data confidentiality in two parallel projects to provide modular, adaptable guidance rather than an all-or-nothing approach.

BACKGROUND

The first group of data security projects at the NCCoE focused on data integrity (DI). The NIST Special Publications covered the ability to protect DI, detect and respond to attacks that impact DI, and recover DI after an attack. During presentations, demonstrations, Community of Interest calls, and other feedback mechanisms, many questions were raised related to data breaches and inclusion of technologies to prevent such attacks. While this was previously out of scope, the new data confidentiality projects seek to address this need.

BENEFITS

This project will demonstrate how an enterprise could build and/or utilize:

- a network baselining solution to establish normal parameters for activity
- an event detection solution with components that monitor:
  - systems for confidentiality events
  - networks for unusual activity and potential cybersecurity events
  - users for all activities, including unusual or unauthorized activity
  - data for attempted unauthorized access or movement
- an event data aggregation and correlation solution to assist in detection of and response to a data confidentiality event
- a file access monitoring solution to produce logs and alerts

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
For more information about this project, visit: https://www.nccoe.nist.gov/projects/building-blocks/data-security/dc-detect-respond-recover

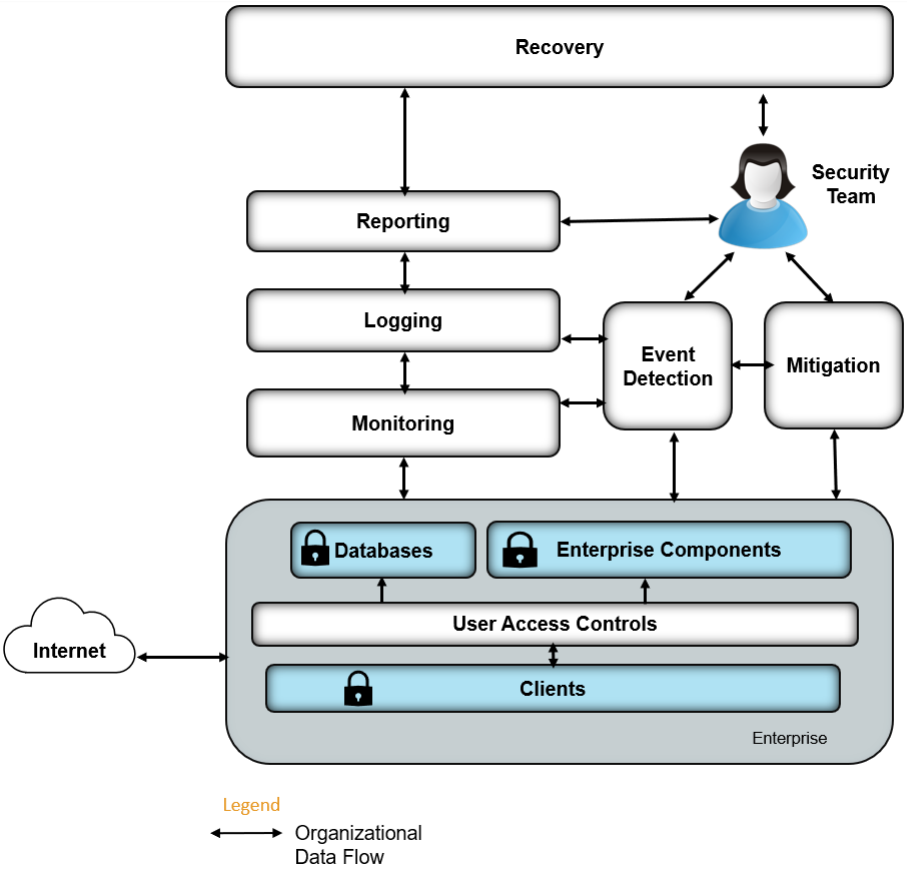
CONTACT US
nccoe@nist.gov
301-975-0200

- an exfiltration detection and mitigation solution to prevent data confidentiality loss
- tools that aid in identification of information that is necessary for a data confidentiality recovery event

This project will answer specific questions pertaining to identifying and protecting data from data confidentiality attacks, such as:

- What does normal data activity look like for your network?
- How can you tell when a breach has occurred? Or is still occurring?
- How can you tell what data has been lost in a breach?
- What technical capabilities does your organization need to execute a data breach response?

HIGH-LEVEL ARCHITECTURE



COMPONENT LIST

Solutions for this project include:

- monitoring
  - file
  - network
  - users
- event detection
  - exfiltration activity
  - unauthorized activity
  - anomalous activity
- log collection, collation, and correlation of all activities within the enterprise
- reporting events to the security team
- mitigating data loss

DOWNLOAD THE PROJECT DESCRIPTION

For more information about data security projects, please read the project descriptions at: 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.