

# National Cybersecurity Center of Excellence

Increasing the adoption of standards-based  
cybersecurity technologies

Data Integrity COI Call

December 13, 2017

# > Agenda

- Status on Data Integrity: Recovery project
- Data Integrity Projects
- Identify and Protect & Detect and Respond projects
- Project Schedule

# › Data Integrity: Recovering from Ransomware and Other Destructive Events

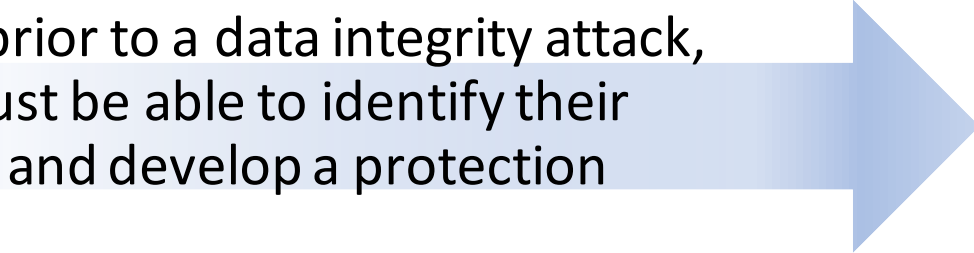
<https://nccoe.nist.gov/projects/building-blocks/data-integrity/recover>

- Release draft publications in September 2017
  - SP 1800-11a: Executive Summary ([PDF](#)) ([web page](#))
  - SP 1800-11b: Approach, Architecture, and Security Characteristics ([PDF](#)) ([web page](#))
  - SP 1800-11c: How-To Guides ([PDF](#)) ([web page](#))
- Comment period closed November 6, 2017



# › Data Integrity Projects

- In the stages prior to a data integrity attack, companies must be able to identify their infrastructure and develop a protection capability.



**Project Description: Data Integrity:  
Identifying and Protecting Assets  
Against Ransomware and Other  
Destructive Events**

- During a data integrity attack, companies must be able to detect the occurrence and respond in accordance with their response plan.



**Project Description: Data Integrity:  
Detecting and Responding to  
Ransomware and Other Destructive  
Events**

- After a data integrity attack, companies must be able to effectively and efficiently recover.



**Data Integrity: Recovering from  
Ransomware and Other Destructive  
Events (1800-11 series)**

# › Purpose – Identify & Protect

Develop a successful defense against data integrity attacks

- Crucial steps must be taken before the attack ever takes place
- Develop an ability to establish a baseline of activities
- Demonstrate that with the exception of zero-day exploits and privileged insider threat, most attacks can be prevented

## > Purpose – Detect & Respond

Help guide organizations in establishing the tools and procedures to detect data integrity events and respond in a way that is appropriate and timely

- Establish proper tools for detection
- Develop ability to enforce policies on affected systems
- Establish capability to compare present activity against an established baseline
- Produce a capability for response to include analyzing, containing, and mitigating the impact

# > Background

## Develop a successful defense against data integrity attacks

- Discovered in 2016, Petya ransomware infected email attachments attempted to encrypt both the user's files and the Master Boot Record (MBR)
- May 2017, the WannaCry ransomware infected over 200,000 systems worldwide, exploited a vulnerability that had a patch publicly released two months prior.
- June 2017, Petya came back as NotPetya! began using the *same* exploit that the WannaCry ransomware used, attacking servers worldwide
- Solutions existed at the time of these attacks
  - scan email attachments
  - proper maintenance and vulnerability management
  - protect MBRs from modification
  - provide systems patching and maintenance

# > Objective

Help organizations identify & protect assets and detect & respond to data integrity attacks

- NCCoE projects include
  - an architectural description that addresses the technical challenge
  - reference designs that integrate commercial and open source products to demonstrate an implementation of standards and best practices.
- Result in a publicly available NIST Cybersecurity Practice Guides
  - documents a detailed implementation guide
  - practical steps needed to implement a cybersecurity reference design that addresses this challenge



## > Scope for Identify & Protect

- This project will answer specific questions pertaining to identifying and protecting assets from data integrity attacks:

What systems, users, applications, data sources, and other entities are on the network?

What attack vectors are present?

What protection is available for data prior to an attempted attack on data integrity?

What processes can be implemented prior to an attack to ease detection, mitigation, and recovery later on?

- This project will contain the following:

Inventory solution

File integrity solution

Backup solution

Secure storage solution

Audit log solution

Vulnerability management solution

Maintenance solution

## > Scope for Detect & Respond

- This project will answer specific questions pertaining to detecting and responding to data integrity events:

What is the baseline activity of systems and networks?

Identifying the baseline activity will prepare for detection of anomalous activity.

When has a data integrity event occurred and what is the impact?

How will a previously-established response plan be executed?

How will incidents be contained and mitigated?

- This project will contain the following:

Network baselining solution

Event detection solution

Event data aggregation and correlation solution

Vulnerability scanning solution

Forensic solution

## > Scenario 1: Ransomware

- For financial gain an organized crime group has set up a seemingly legitimate domain with destructive malware disguised as a legitimate virus scanning program. Once installed, it encrypts the organization's filesystem and requests a ransom payment in order to decrypt the files to be restored. Left unmitigated, the malware on one system is designed to move laterally within the network to other client and server systems within an organization's network, encrypting those systems and demanding ransom in exchange for their files.



## ➤ Scenario 2: Data Destruction Malware

- An adversary wishing to impact the operations of an organization leaves several infected USB drives in the parking lot of the building. When an unsuspecting employee plugs in the drive, software on the drive immediately modifies text files and deletes media files on the user's machine.





## ➤ Scenario 3: Virtual Machine Data Loss

- A privileged user running an automatic maintenance on the organization's virtual machines accidentally deletes one of the virtual machines. Though the deletion is accidental, the change is not noticed by the user immediately.



## > Scenario 4: Server Permissions Change

- An adversary wishing to gain access to the operations of an organization launches a spear-phishing campaign against privileged individuals in the target corporation, through the use of an infected email attachment. When one of the privileged users opens the attachment, the malware immediately begins creating backdoors for the adversary to use at a later point.





## Scenario 5: Database Metadata Change

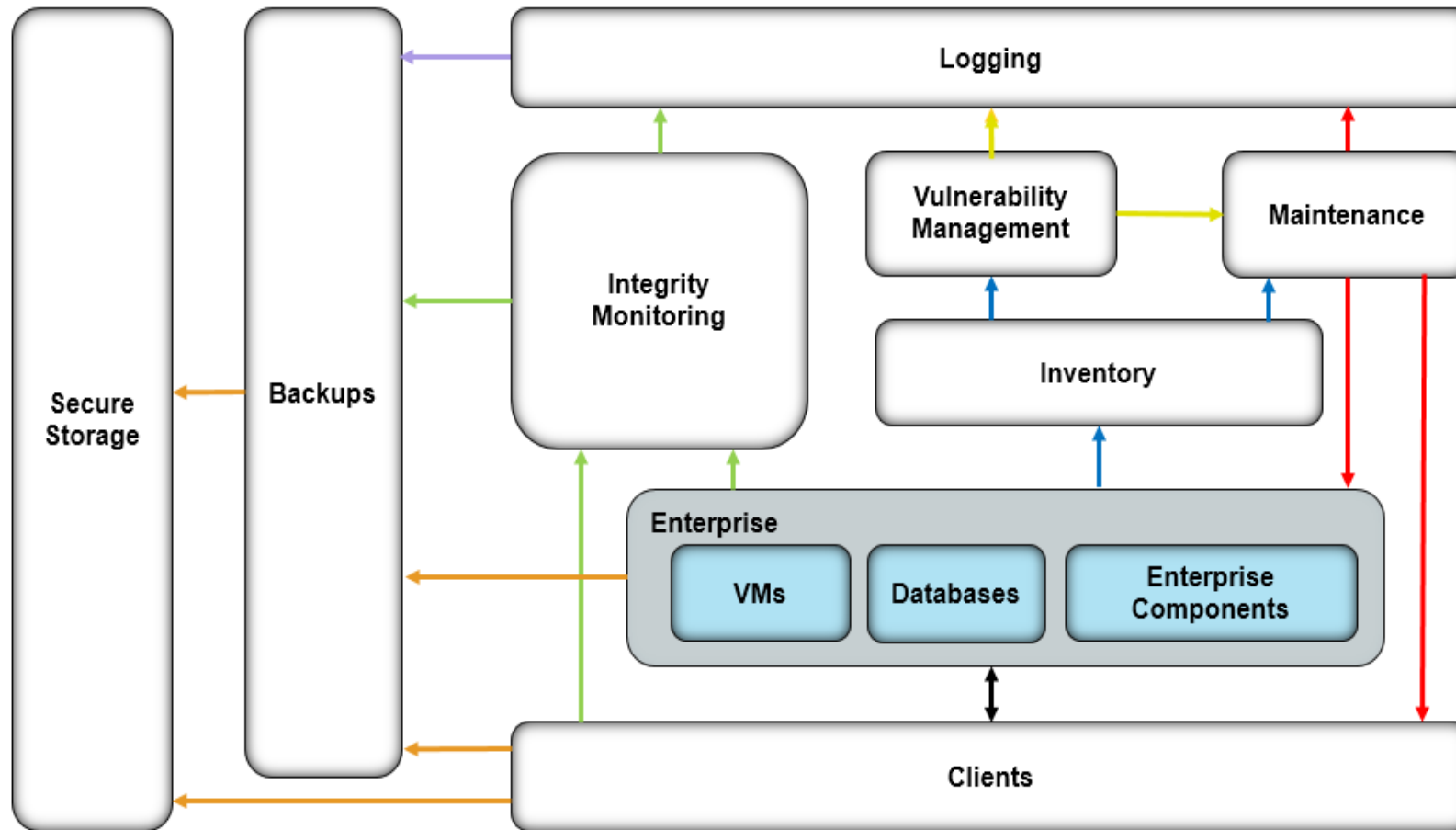
---

- An insider seeking to disrupt the organization's operations for financial gain in the stock market makes changes to the database structure. These changes leave the applications relying on the affected database tables unable to function properly.

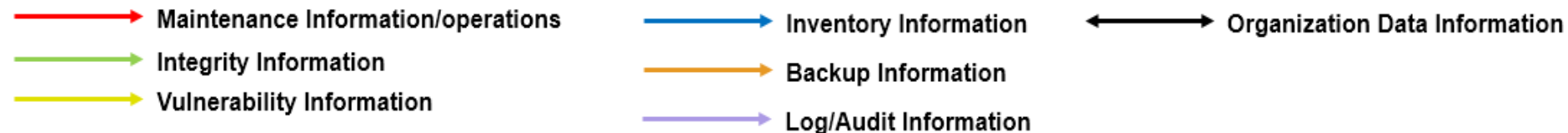




# > Scope for Identify & Protect

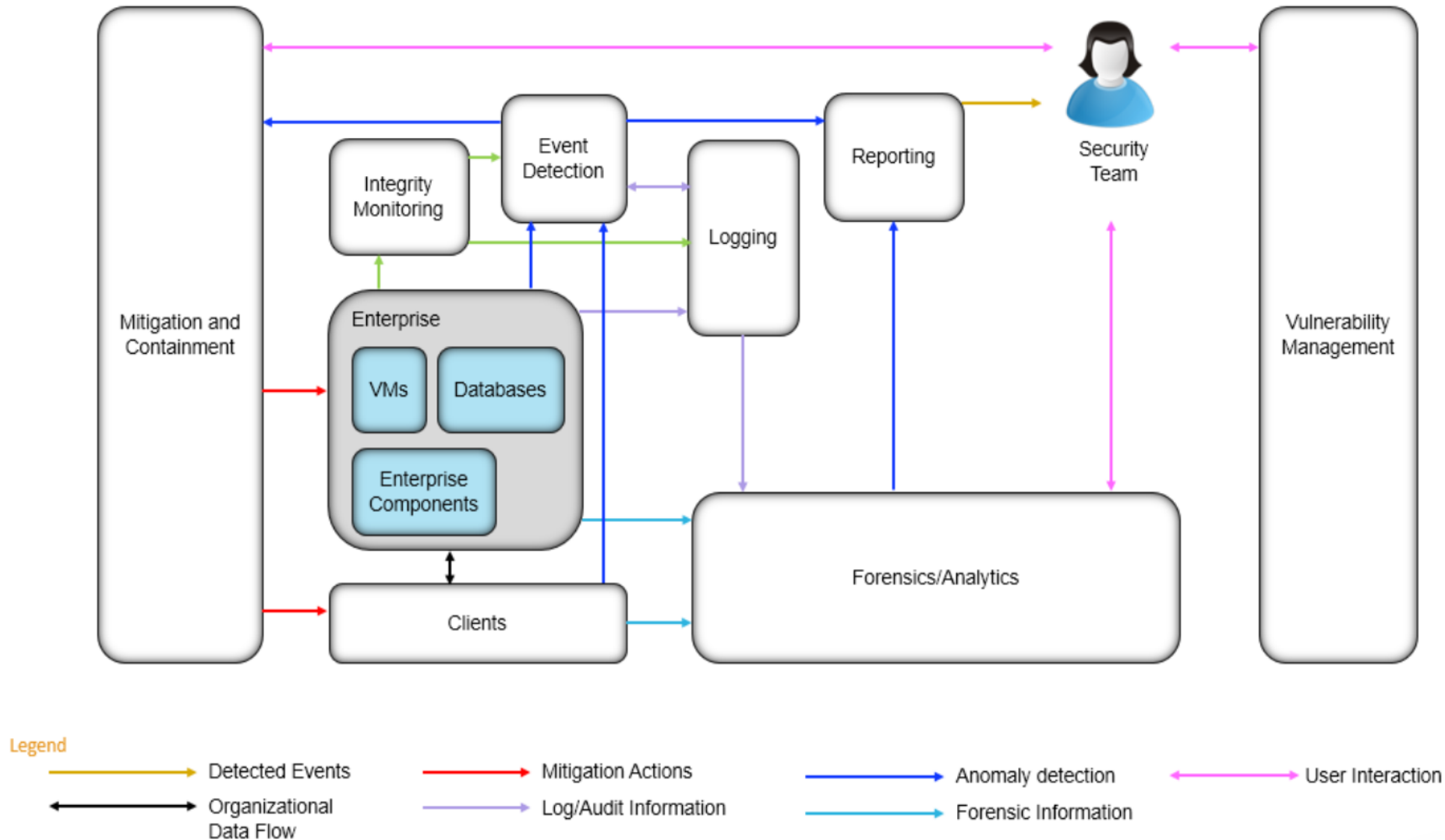


## Legend





# > Scope for Detect & Respond



# > Component List

Identify & Protect	Detect & Respond
Secure storage	Baseline capability
File integrity checking mechanisms	Event detection
Backup capability for databases, VMs, and filesystems	Malicious software detection
Vulnerability management and identification software	Unauthorized activity detection
Log collection software	Anomalous activity detection
Asset inventory software	Data aggregation and correlation
Maintenance software (including software versioning and distribution technology)	Vulnerability scanning
	Forensic tools

# > Desired Requirements

## Identify & Protect

Inventory assets both part of the enterprise and the solution itself

Be secure against integrity attacks against hosts

Be secure against integrity attacks that occur on the network

Support secure backups

Provide protected network and remote access

Provide audit capabilities

## Detect & Respond

Detect/report/analyze the impact of/mitigate the impact of/contain unauthorized or malicious activity on the network

Detect/report/analyze the impact of/mitigate the impact of/contain unauthorized or malicious mobile code events

Detect/report/analyze the impact of/mitigate the impact of/contain unauthorized or malicious executables

Detect/report/analyze the impact of/mitigate the impact of/contain unauthorized or malicious behavior

# › Project Descriptions

<https://nccoe.nist.gov/projects/building-blocks/data-integrity>

- <https://nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect>
- <https://nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond>
- Comment period closed Dec 12, 2017
- Next steps

Complete FRN and receiving LOIs from interested collaborators

# > Questions?

**Tim McBride, Deputy Director NCCoE**

**Anne Townsend, Lead Cybersecurity Engineer**

Timothy.McBride@nist.gov

Anne.Townsend@nist.gov

301.975.0214

703.983.1618



<http://nccoe.nist.gov>



301-975-0200



[nccoe@nist.gov](mailto:nccoe@nist.gov)