RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: SEM-M03

RECOVER QUICKLY & SAFELY FROM RANSOMWARE

Brian Abe

Department Head, National Cybersecurity FFRDC
National Cybersecurity Center of Excellence (NCCoE)
MITRE

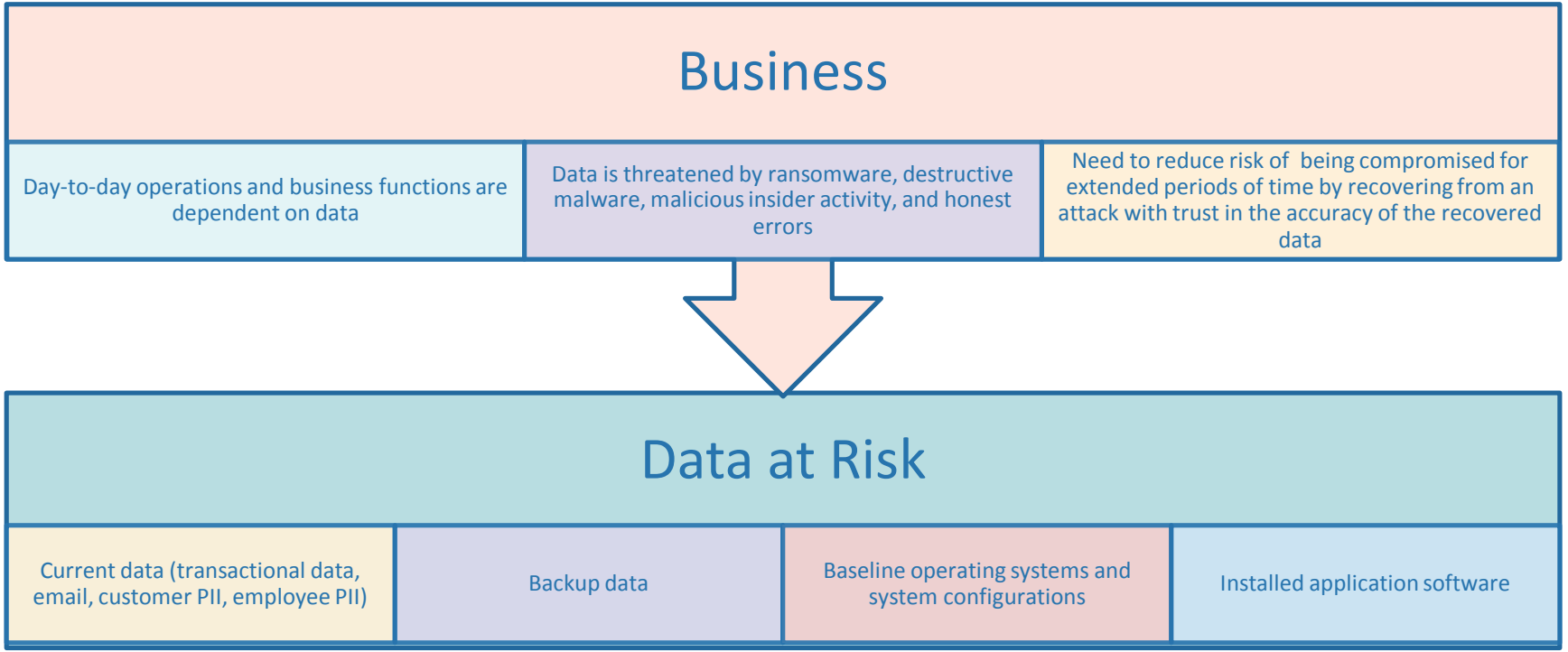
Anne Townsend

Lead Cybersecurity Engineer
National Cybersecurity Center of Excellence (NCCoE)
MITRE

Evolution of the Data Integrity Project

- Initially identified in NISTIR 8050, Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy (12 Feb 15, draft published on 2 Apr 15)
- Coordinated with FS-ISAC Destructive Malware Task Force
- Project Description released on 23 Nov 15 for 60-day public comment period

Challenges


Business
Day-to-day operations and business functions are dependent on data
Data is threatened by ransomware, destructive malware, malicious insider activity, and honest errors
Need to reduce risk of being compromised for extended periods of time by recovering from an attack with trust in the accuracy of the recovered data
Data at Risk
Current data (transactional data, email, customer PII, employee PII)
Backup data
Baseline operating systems and system configurations
Installed application software

SP 1800-11: RECOVERING FROM RANSOMWARE AND OTHER DESTRUCTIVE EVENTS PRACTICE GUIDE

Volume A: Executive Summary

- High-level overview of the project, including summaries of the challenge, solution, and benefits

NIST SPECIAL PUBLICATION 1800-11A

Data Integrity

Recovering from Ransomware and Other Destructive Events

Volume A:
Executive Summary

Timothy McBride
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Michael Ekstrom
Lauren Lusty
Julian Sexton
Anne Townsend
The MITRE Corporation
McLean, VA

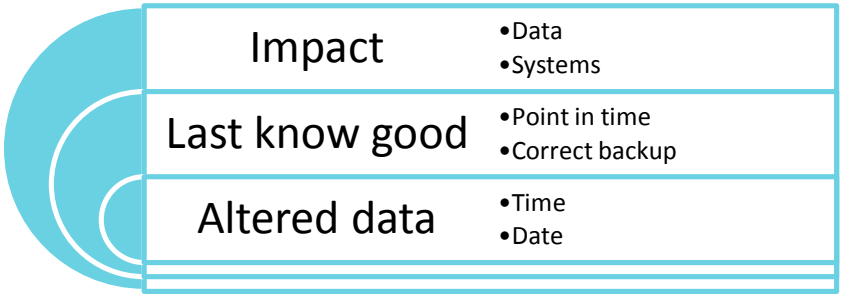
September 2017

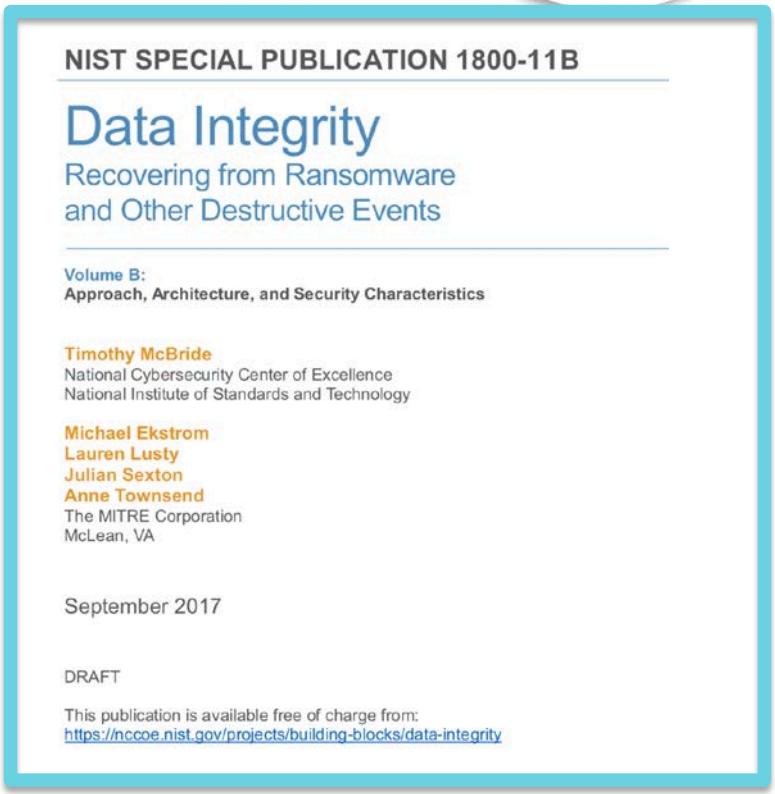
DRAFT

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

Volume B: Approach, Architecture, and Security Characteristics

- Deep dive into challenge and solution, including approach, architecture, and security mapping to NIST Cyber Security Framework (CSF) and other relevant standards





NIST SPECIAL PUBLICATION 1800-11B

Data Integrity

Recovering from Ransomware and Other Destructive Events

Volume B:
Approach, Architecture, and Security Characteristics

Timothy McBride
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Michael Ekstrom
Lauren Lusty
Julian Sexton
Anne Townsend
The MITRE Corporation
McLean, VA

September 2017

DRAFT

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

Volume C: How-To Guide

- Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance

NIST SPECIAL PUBLICATION 1800-11C

Data Integrity

Recovering from Ransomware and Other Destructive Events

Volume C:
How-to Guides

Timothy McBride
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

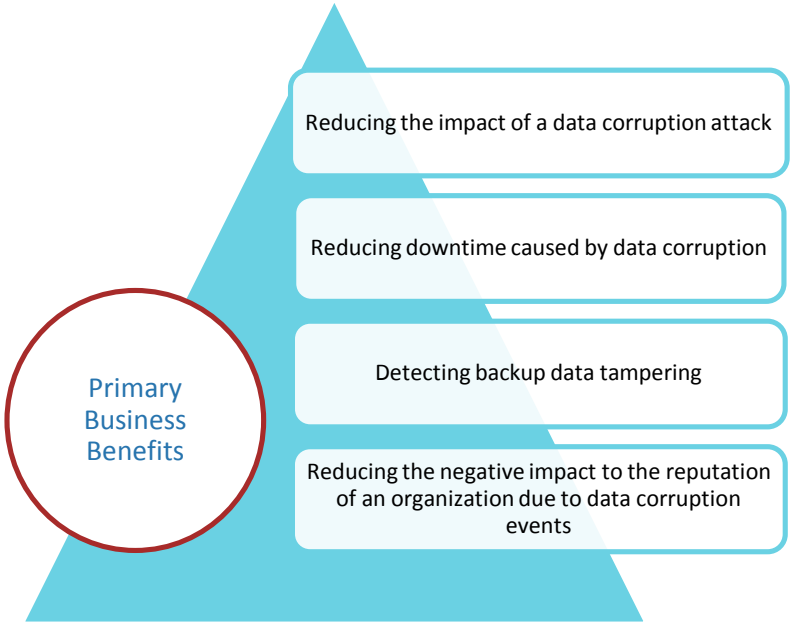
Michael Ekstrom
Lauren Lusty
Julian Sexton
Anne Townsend
The MITRE Corporation
McLean, VA

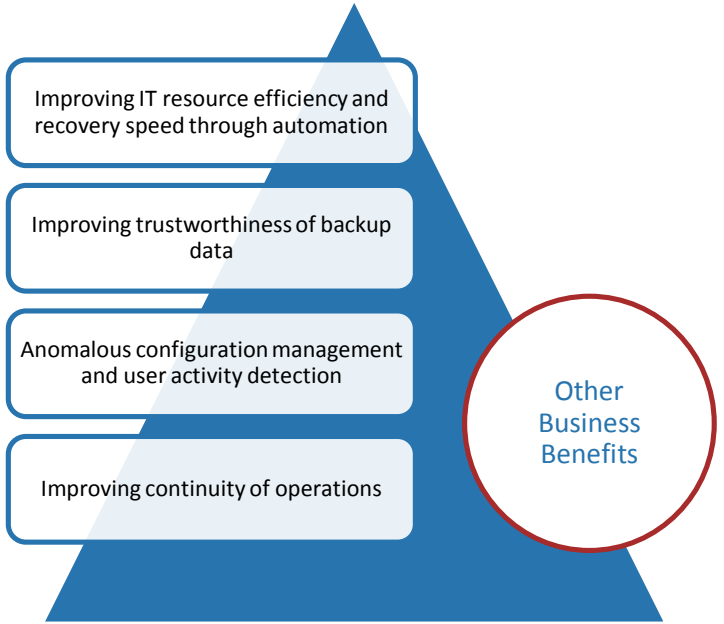
September 2017

DRAFT

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

Benefits


Primary Business Benefits
Reducing the impact of a data corruption attack
Reducing downtime caused by data corruption
Detecting backup data tampering
Reducing the negative impact to the reputation of an organization due to data corruption events


Other Business Benefits
Improving IT resource efficiency and recovery speed through automation
Improving trustworthiness of backup data
Anomalous configuration management and user activity detection
Improving continuity of operations

Scenarios

Scenario 1: Ransomware

- Malware encrypts files and displays notice demanding payment for decryption

Scenario 2: Data Deletion

- Spear-phishing campaign with link/attachment containing malware that destroys data on user machine

Scenario 3: VM Deletion

- End user with privileges mistakenly deletes a virtual machine

Scenario 4: Permission Change on a Server

- Insider creates backdoor accounts to allow outside access to internal network

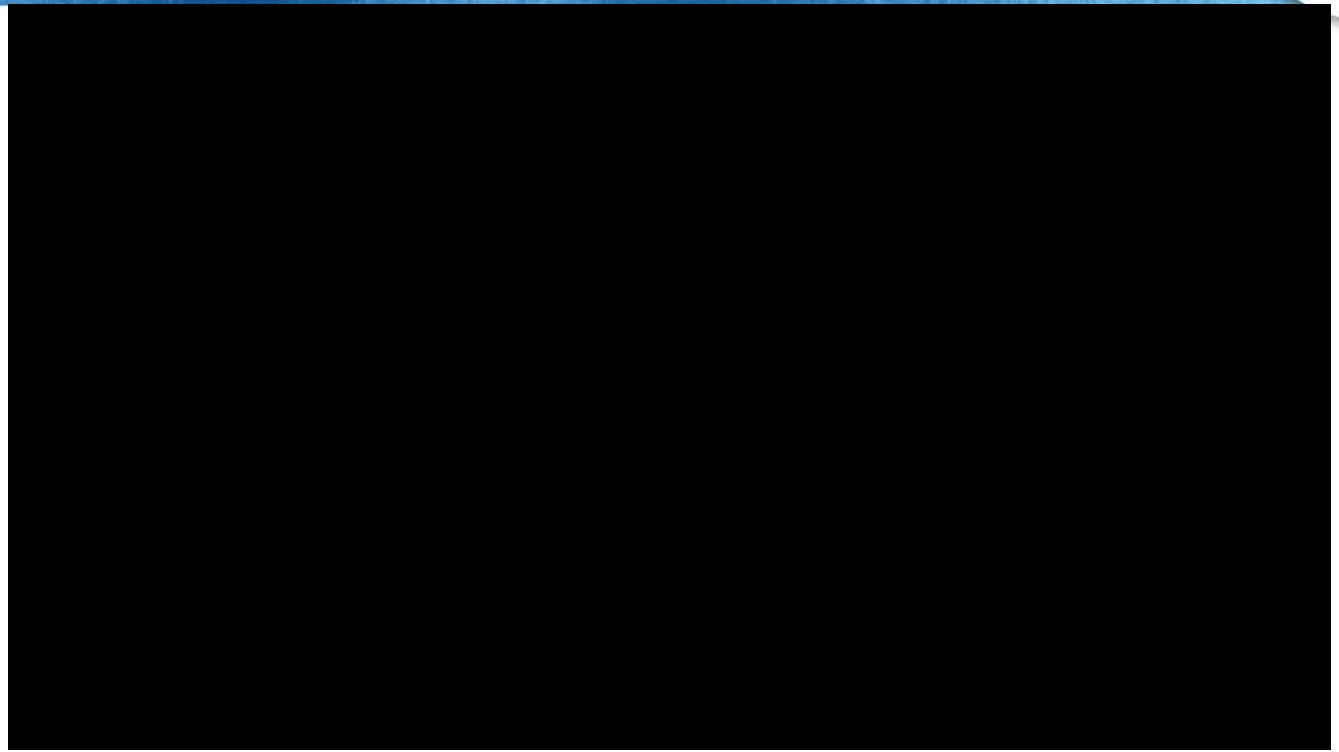
Scenario 5: Move of Database Table

- User accidentally moves a database rendering a system inoperable

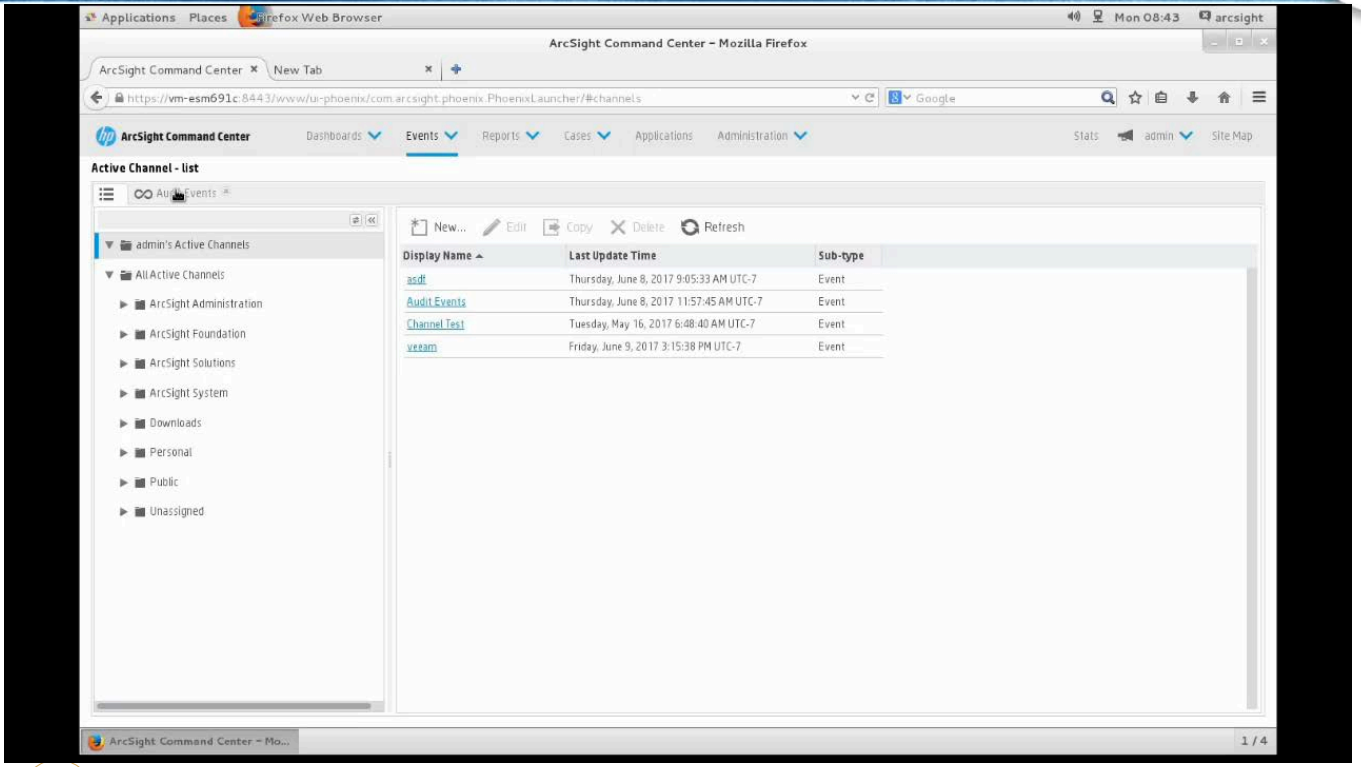
Scenario 6: Database Error

- An unwanted query adds/modifies/deletes data in a database and queries have been performed since last backup

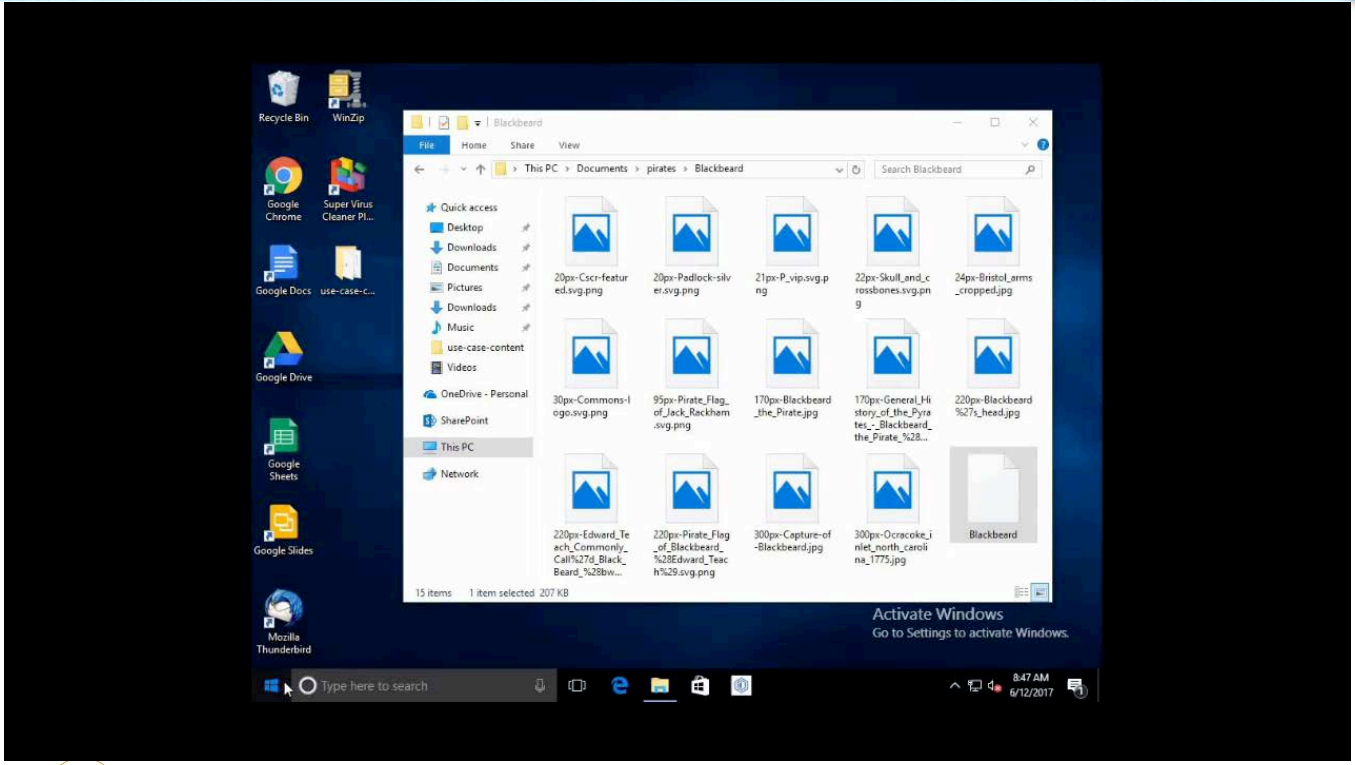
Demo – Ransomware Attack



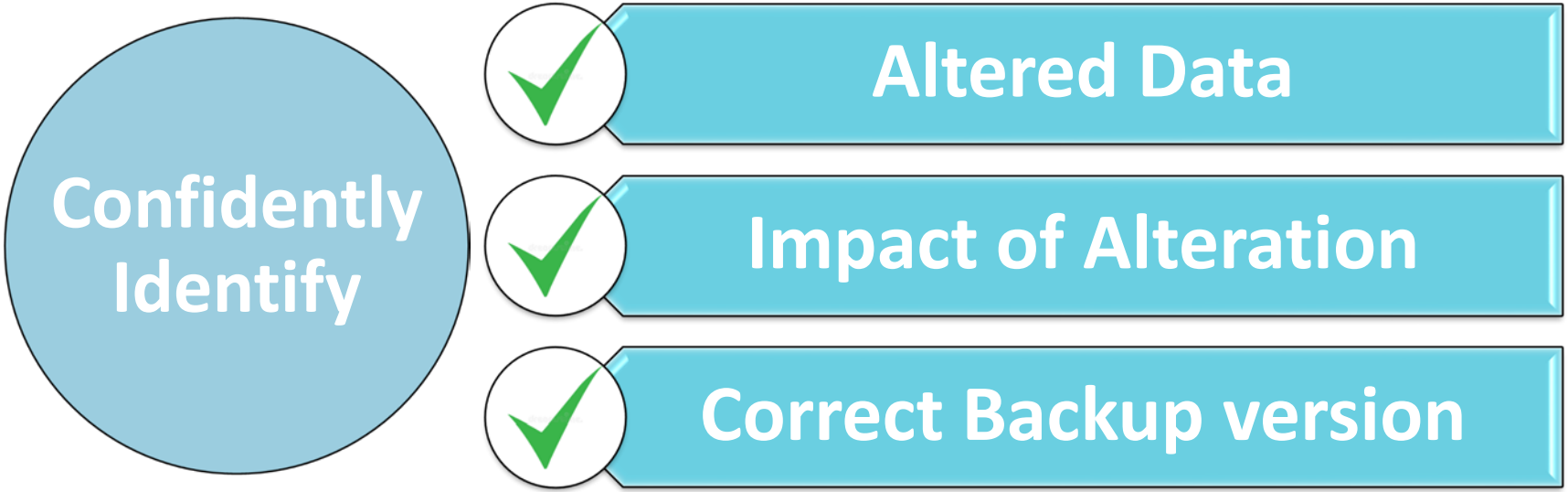
Demo – Ransomware Identification



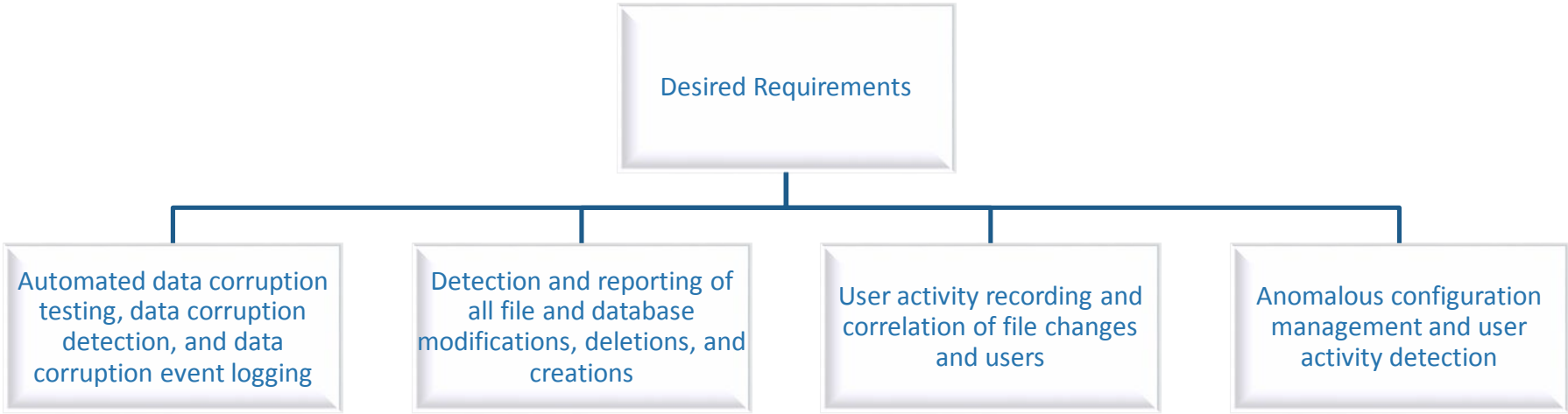
Demo – Ransomware Recover



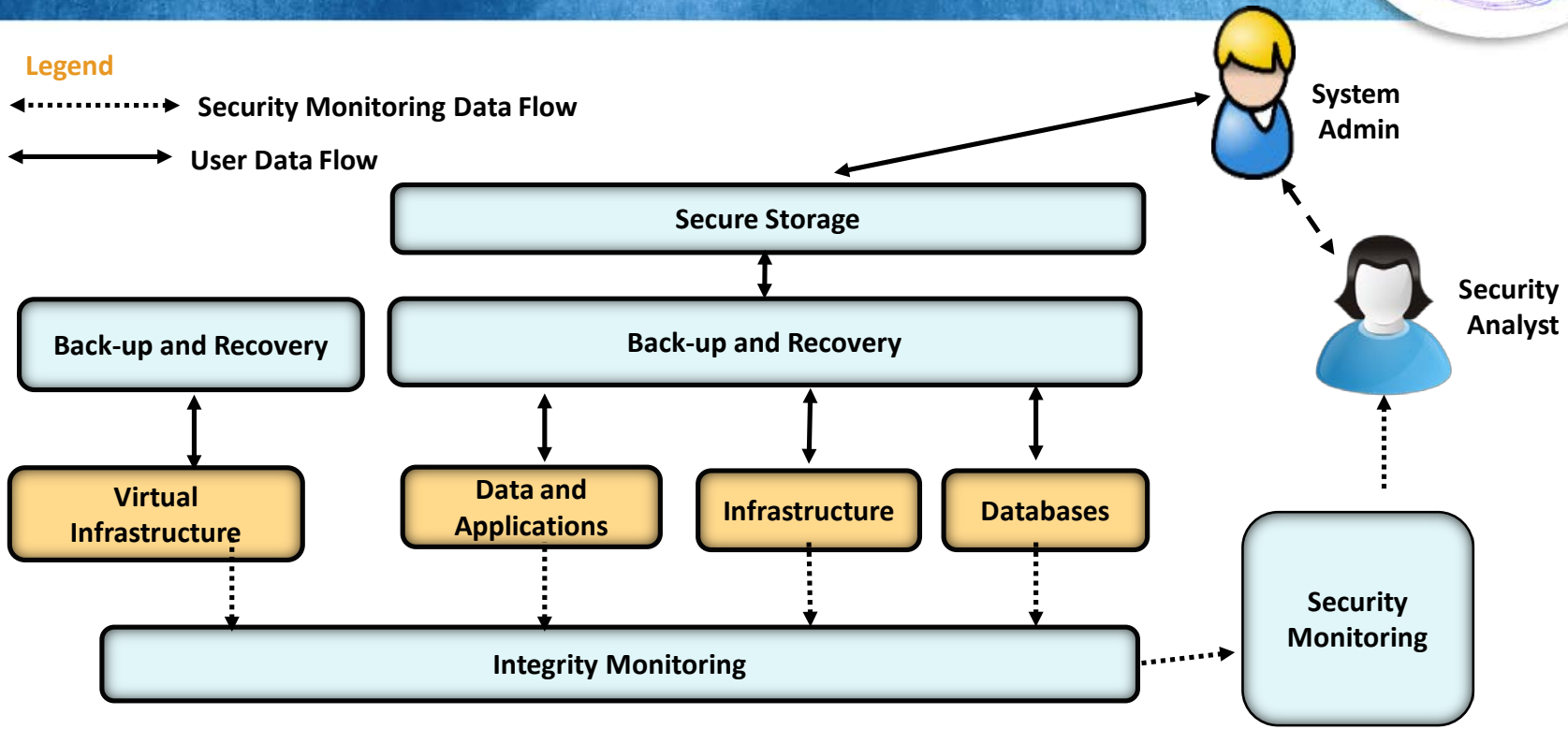
Recovery


Confidently Identify
Altered Data
Impact of Alteration
Correct Backup version

Recovery Continued



Solution


Legend
Security Monitoring Data Flow
User Data Flow
System Admin
Security Analyst
Secure Storage
Back-up and Recovery
Back-up and Recovery
Virtual Infrastructure
Data and Applications
Infrastructure
Databases
Integrity Monitoring
Security Monitoring

Data Integrity Projects

Special Publication 1800-11 Released September 2017	• Data Integrity: Recovering from Ransomware and Other Destructive Events
Project Descriptions Both Released November 2017	• Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events • Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events
Additional Publication Release Date Pending	• Implementation document to address the cohesion of all above listed projects

Apply What You Have Learned Today

- Next week you should:
  - Have the appropriate informational materials in order to understand this challenge space and how to address it
- In the first three months following this presentation you should:
  - Understand what components are needed for your infrastructure in order to recover from data integrity attacks
  - Define what specific configurations will be necessary for your organization
- Within six months you should:
  - Select the security components required for your infrastructure
  - Begin to form and develop an implementation that will provide the ability to recover

Contact Information

- Phone: 301.975.0200
- Website: http://nccoe.nist.gov
- Email: di-nccoe@nist.gov
- Address: 9700 Great Seneca Hwy, Rockville, MD 20850