Securing Data Integrity Against Ransomware Attacks:

Using the NIST Cybersecurity Framework and NIST Cybersecurity Practice Guides

Jennifer Cawthra
National Cybersecurity Center of Excellence
Gaithersburg, MD

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

October 1, 2020

ds-nccoe@nist.gov

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.10012020-draft

DRAFT

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

Abstract

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) is actively engaged in helping organizations address the challenge of ransomware and other data integrity events through the Data Integrity projects. These projects help organizations implement technical capabilities that address data integrity issues. The objective of this document is to provide an overview of these Data Integrity projects; provide a high-level explanation of the architecture and capabilities; and explain how these projects can be brought together into one comprehensive data integrity solution.

Keywords

data integrity; data security; malware; ransomware; security architecture.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Additional Information

For additional information on NIST's Cybersecurity programs, projects and publications, visit the Computer Security Resource Center. Information on other efforts at NIST and in the Information Technology Laboratory (ITL) is also available.

Public Comment Period: *October 1, 2020 through November 13, 2020*

National Institute of Standards and Technology
Attn: Applied CyberSecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2002) Gaithersburg, MD 20899-2002
Email: ds-nccoe@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA)

Table of Contents

1 Ransomware and Data Integrity 1
1.1 Purpose 1
1.2 Introduction 1
1.3 NCCoE Efforts in Data Integrity 2
***2 Special Publication (SP) 1800-25 Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events* 4**
***3 SP 1800-26 Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events* 6**
***4 SP 1800-11 Data Integrity: Recovering from Ransomware and Other Destructive Events* . 8**
5 Project Integration 10
5.1 Combined Architecture 10
6 Cross Function Interactions 12
6.1 Backup and Restoration 12
7 Additional Considerations 14
8 Summary 15
References 16

List of Appendices

Appendix A— Acronyms 18
Appendix B— Glossary 19
Appendix C— Cross Function Interactions 21
C.1 Integrity Monitoring 21
C.2 Detection 22
C.3 Denylist 23
C.4 Vulnerability Response 24
C.5 Policy Updates and User Privileges 24
Appendix D— Additional Data Security Capabilities 25
D.1 Data Tokenization and Data Masking 25
D.2 Content Filtering 25
D.3 Additional Capabilities 26

D.4 Additional Sources for Information 26

List of Figures

Figure 1-1 Data Security Projects 2
Figure 1-2 Framework Core Functions 2
Figure 1-3 Division of CSF Functions Across Data Integrity Projects 3
Figure 2-1 SP 1800-25 Architecture 4
Figure 3-1 SP 1800-26 Architecture 6
Figure 4-1 SP 1800-11 Architecture 8
Figure 5-1 Overarching Architecture 11
Figure 6-1 Backup and Restoration Cross Function Diagram 13

Figure C-1 Integrity Monitoring Cross Function Diagram 22
Figure C-2 Detection Cross Function Diagram 23
Figure C-3 Denylist Cross Function Diagram 24
Figure C-4 Vulnerability Response Cross Function Diagram 24

1 Ransomware and Data Integrity

1.1 Purpose

This guide is designed for organizations that are not currently experiencing a loss of data integrity event (ransomware or otherwise). This document prepares an organization to adequately address future data integrity events. For information on dealing with a current attack, please explore guidance from organizations like the Federal Bureau of Investigation [1], the United States Secret Service [2], or other pertinent groups or government bodies.

1.2 Introduction

Successful ransomware impacts data's integrity, yet ransomware is just one of many potential vectors through which an organization could suffer a loss of data integrity. Integrity is part of the CIA security triad [5] which encompasses Confidentiality, Integrity, and Availability. As the CIA triad is applied to data security, data integrity is defined [6] as "the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner." An attack against data integrity can cause corruption, modification, and/or destruction of the data which ultimately results in a loss in trust in the data.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) is actively engaged in helping organizations address the challenge of ransomware and other data integrity events through the Data Integrity projects. These projects help organizations implement technical capabilities that address data integrity issues. Ransomware is one of the many use-case examples in these projects.

This document provides an overview of these Data Integrity projects; providing a high-level explanation of the architecture and capabilities, and how these projects can be brought together into one comprehensive data integrity solution. This comprehensive data integrity solution can then be integrated into a larger security picture to address all of an organization's data security needs.

To continue its work with the security triad, the NCCoE, at the time of this publication is developing data confidentiality projects through the publications of SP 1800-28 and SP 1800-29. Data availability has not been pursued yet as an SP 1800-series publication, but research is being conducted to determine how NIST, through the NCCoE, can best address this subject as well.

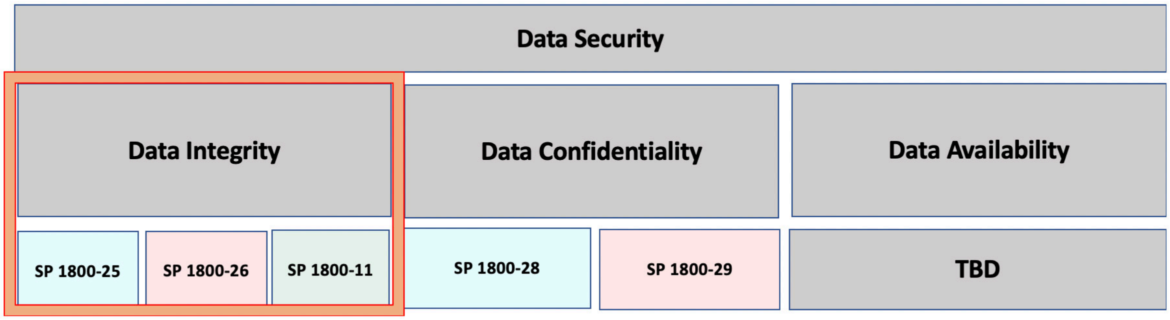

Figure 1-1 Data Security Projects

1.3 NCCoE Efforts in Data Integrity

Ransomware, destructive malware, insider threats, and even honest user mistakes present ongoing threats to organizations. Organizations' data, such as database records, system files, configurations, user files, applications, and customer data, are all potential targets of data corruption, modification, and destruction. This document provides an overview of three data integrity projects that are aligned with the functions in the NIST Cybersecurity Framework with the goal of formulating a defense against data integrity challenges. NIST published version 1.1 of the Cybersecurity Framework [7] in April 2018 to provide guidance on protecting and developing resiliency for critical infrastructure and other sectors. In this document, the framework core contains five functions:

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.

Figure 1-2 Framework Core Functions

When applying the Cybersecurity Framework to data integrity, a natural separation into three distinct projects based on the lifecycle of a data integrity attack was apparent. Before an attack, one must identify all assets and potential vulnerabilities and protect these assets including remedying the discovered vulnerabilities. This concept is described in the practice guide *SP*

1800-25 Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events. To plan for how an organization can handle when an attack occurs, one needs to have the capabilities to detect and respond to destructive events. *SP 1800-26 Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events* addresses this challenge. Lastly, should a data integrity attack be successful, an organization must have the capability to recover which is described in *SP 1800-11 Data Integrity: Recovering from Ransomware and Other Destructive Events.*

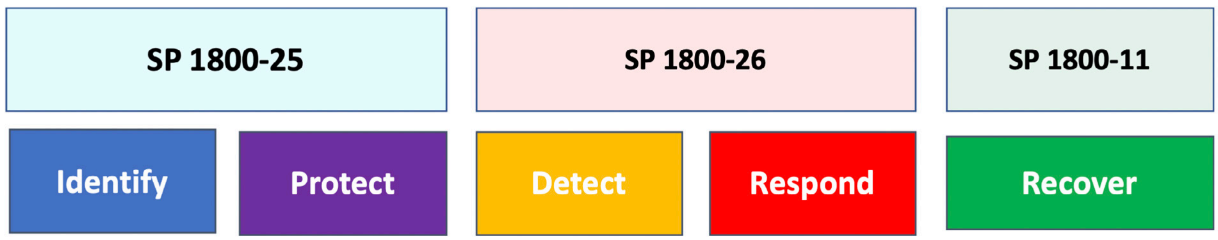

Figure 1-3 Division of CSF Functions Across Data Integrity Projects

The next three sections will summarize each of the three projects' architecture and capabilities. For more in-depth understanding of the projects, the associated SP 1800 document should be referenced.

2 Special Publication (SP) 1800-25 Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events

SP 1800-25 Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events addresses data integrity before a potential attack. It details the need for a thorough knowledge of the assets within the enterprise and the protection of these assets against the threat of data corruption and destruction. This project proposes an architecture with multiple systems that work together to identify and protect an organization's assets against the threat of corruption, modification, and destruction. The purpose of this project is to help guide organizations to effectively identify assets (devices, data, and applications) that may become targets that enable a data integrity attack, as well as the vulnerabilities that facilitate these attacks. It also explores methods to protect these assets against data integrity attacks.

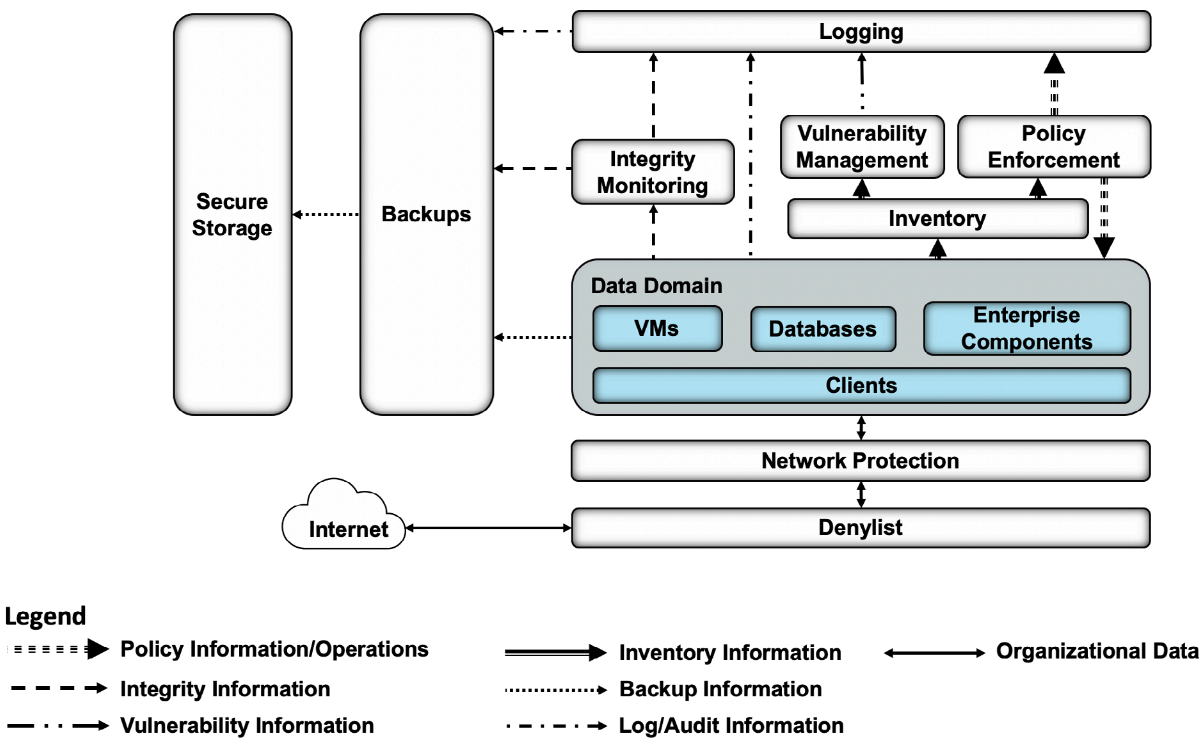

Figure 2-1 SP 1800-25 Architecture

The following is a brief description of the capabilities. For more information, visit *SP 1800-25 Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*.

In order to identify and protect data against destructive events, it is necessary to understand the systems and devices on which an organization's data resides. The capability to inventory allows for discovery, and tracking devices connected to the enterprise. Once an organization has awareness of its networks and devices, more capabilities can be thoroughly applied. Vulnerability Management provides a mechanism for analyzing these various network components. This capability provides for a better understanding of resolved and unresolved vulnerabilities in the enterprise, and allows an organization to make informed decisions about handling known vulnerabilities to best protect prioritized data. The Logging capability records and stores all the log files produced by these components within the enterprise. Together the Vulnerability Management and logs contribute to the Policy Enforcement capability. Policy Enforcement targets machines with unresolved vulnerabilities and helps maintain overall enterprise health.

The Integrity Monitoring capability establishes baselines of files and systems, which is essential in determining information about any integrity changes that occur to the data within those files and systems. At the same time, the Backup capabilities allow components within the enterprise to produce backup files of data. Some stored data, including backup files, may benefit from a Secure Storage capability. Secure Storage allows data storage with additional data protection measures, such as write once read many technologies.

In addition to file-level protections, a Network Protection capability can defend an enterprise network against both intrusion and lateral movement of malicious actors and programs. Network protections can be supplemented by Denylist[1] capabilities which can filter allowed programs or network communications. Often, this may be provided in the form of a firewall or even an allowlist, but products exist that allow finer-grained control over these filters.

Through the use and integration of these technologies, an organization can prepare for a potential loss of data integrity before such an event occurs by identifying their assets and protecting them against attacks.

[1] Some past documents for the Data Integrity projects, such as the project descriptions and practice guide drafts, are still available for archival purposes. These documents used alternative terms for denylists and allowlists. These terms do not reflect current NIST practices.

3 SP 1800-26 Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events

SP 1800-26 Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events focuses on when a data integrity attack is occurring. The architecture from this project demonstrates that policies and tools must be in place that detect and respond to data integrity events. Prior to an event, information must be gathered to understand the range of normal activity. Tools must be in place to detect any deviation from normal that might be a data integrity event. Policies must be established to respond efficiently and effectively. The purpose of this project is to help guide organizations in establishing the tools and procedures to detect data integrity events and respond in an appropriate and timely fashion.

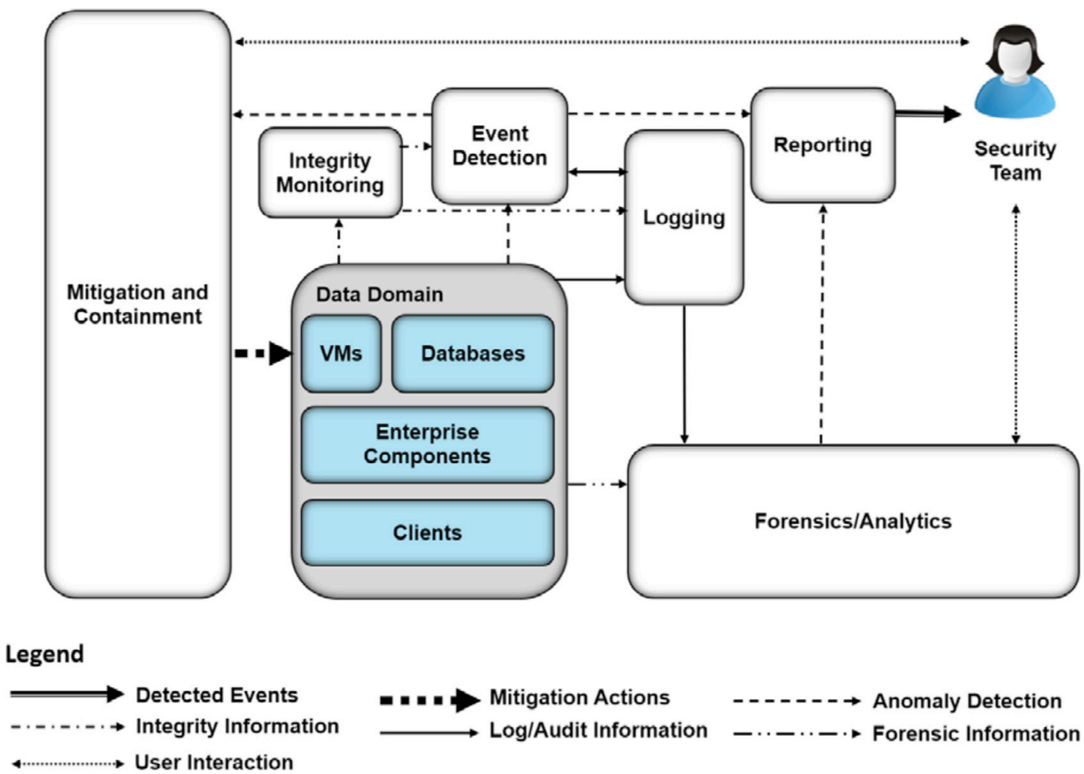

Figure 3-1 SP 1800-26 Architecture

The following is a brief description of the capabilities. For more information, visit *SP 1800-26 Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*.

An Integrity Monitoring capability continues to be used in this architecture as it was in the above project. However, the focus shifts from establishing baselines for assets and their data to monitoring them for unauthorized changes. The Logging capability, also from the above project, provides the ability to aggregate logs from many sources, including the Integrity capability. These logs are fed into an Event Detection capability which provides analysis of activity that indicates events such as malware, intrusions, and other anomalies which may have an undesirable impact on the integrity of an organization's data. The Event Detection capability turns logs into information that is more readily digested by security professionals. The Forensics/Analytics capability also uses the aggregated logs to discover the source and effects of any destructive event on data and enables security teams to make the changes necessary to prevent similar events in the future.

A Mitigation and Containment capability provides the ability to limit a destructive event's affect on the enterprise and its data. This response, which can be automated or integrated with activity by a security team, can involve stopping execution of associated programs, disabling user accounts, disconnecting a system from the network, or more, depending on the threat.

The reporting component is primarily an interface between various components of the architecture and the security team. It allows alerting through email and dashboards based on predetermined events, depending on the organization's need. The reporting capabilities are best used for the duration of an event. They can be used to alert the security team when an event starts, as well as to provide regular status updates when events are not happening or have just finished.

When these components work together, security teams and their tools are enabled to detect a loss of data integrity and respond to the event.

4 SP 1800-11 Data Integrity: Recovering from Ransomware and Other Destructive Events

SP 1800-11 Data Integrity: Recovering from Ransomware and Other Destructive Events, demonstrates that if data integrity has been jeopardized, multiple systems work in concert to recover from the event. The solution recommends capabilities and explores issues around auditing and reporting to support recovery and investigations. The purpose of this project is to help guide organizations in establishing the tools and procedures to recover to a last known good dataset.

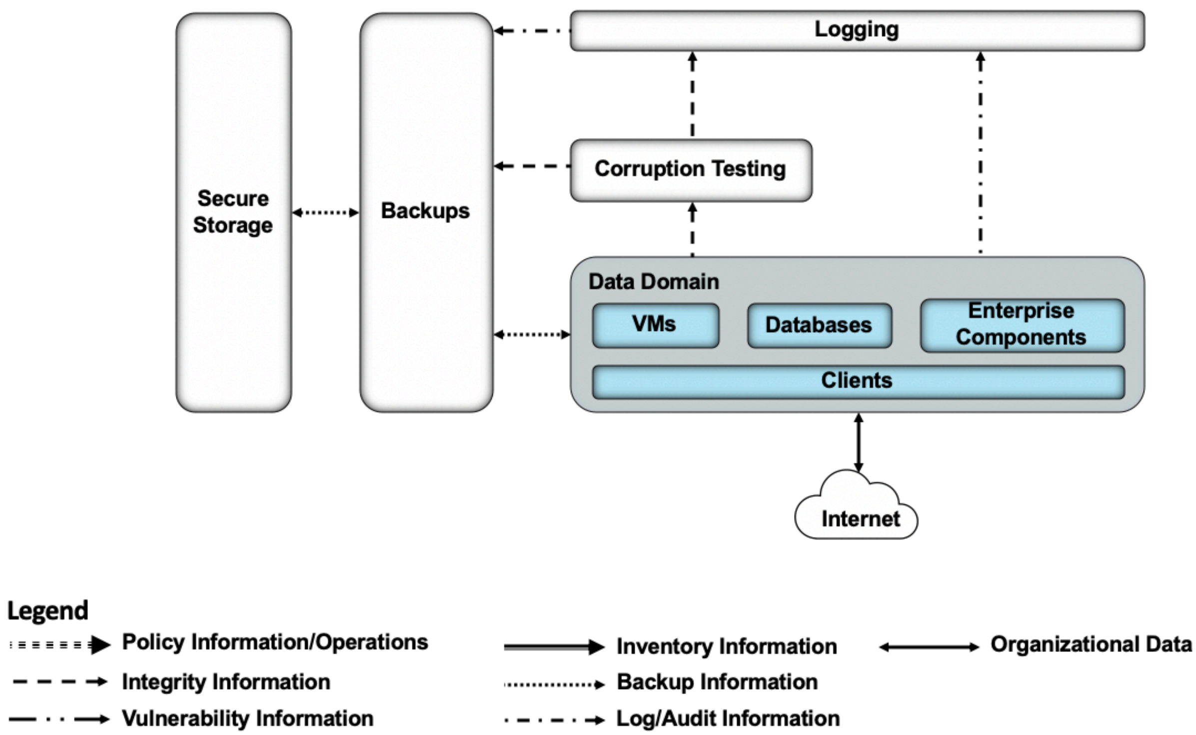

Figure 4-1 SP 1800-11 Architecture

In order to recover from a loss of data integrity, an organization must have taken action before the destructive event occurred. While the focus of this project is on recovery processes, it also documents those capabilities that must have already been in place to facilitate a recovery.

One crucial capability to have in place is the ability to backup data, in order to store copies that an organization has prioritized. Within this project, compromised data is restored from non-compromised previous versions in existing backup files. One method of ensuring that these backup files remain unaltered until they are needed is by storing them using a secure storage capability, which reduces or eliminates the risk to stored data.

In order to understand what data needs to be restored, a corruption testing capability is utilized. This tool is able to identify the last known good status and oversee restoration of data to that state. As with the above projects, a logging capability is important to record relevant information and provide that information to decision-makers.

These capabilities, combined with their roles before an event has occurred, allow an organization to appropriately recover from a loss of data integrity.

5 Project Integration

Building a comprehensive data integrity suite that addresses all functions of the Cybersecurity Framework requires adoption of all the aforementioned projects. Each project though, has components of the architecture that overlap. Thus, adoption of all architectures is not merely a build of three architectures but rather an integration and overlay of the three.

This section describes how to integrate and overlap the three architectures. It also provides guidance on considerations and limitations that an organization should address when using the architectures.

5.1 Combined Architecture

A combined DI solution is designed to implement the technologies from all three practice guides. It seeks to implement the security controls highlighted in the three practice guides through a combined security architecture. Figure 5-1provides a high-level view of the necessary components and the data flows that exist between them.

Components that contain gray coloring can be found in SP 1800-25 and focus on identify and protect functionality. Components that contain blue coloring can be found in SP 1800-26 and focus on detect and respond functionality. Components that contain green coloring can be found in SP 1800-11 and focus on recover functionality. Any component with multiple colors occurs in multiple practice guides and represents key points of integration between them.

The capabilities of Integrity Monitoring and Corruption Testing have been combined in Figure 5-1 due to their similar roles and data flows in their respective data integrity solutions. The capability's terminology evolved in the time elapsed between projects, and the consolidation of the terms in the combined architecture diagram are intended to reflect that consolidation.

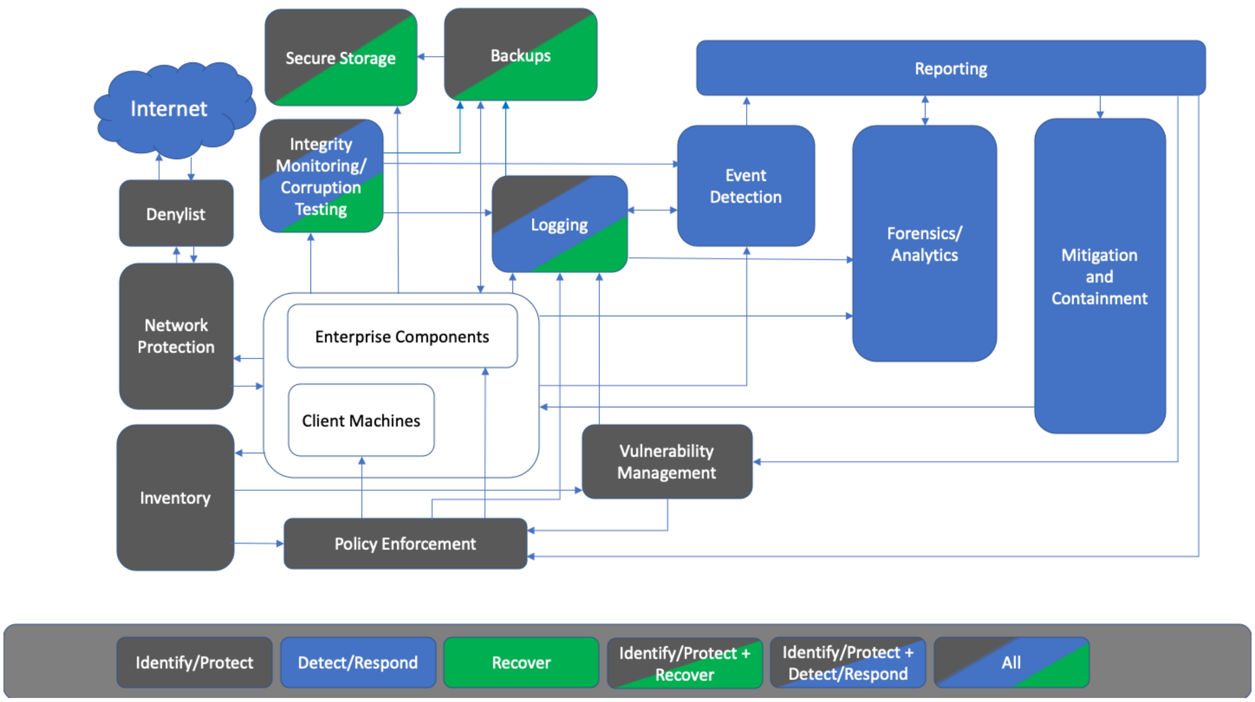

Figure 5-1 Overarching Architecture

If choosing to implement the combined architecture, all three practice guides will provide the details; yet, there may be additional considerations including duplicative instructions, additional setup, and integration steps. Reach out to the NCCoE Data Security team at ds-nccoe@nist.gov for additional integration guidance.

6 Cross Function Interactions

Each of these projects produced a unique architecture that addressed the requirements and capabilities necessary to achieve the desired end state. Each project was comprised of specific components that worked in unison for their specific objective; but information gained during use case scenario testing and functions performed within one project actually provides valuable information to functions in other data integrity projects. For the purpose of this document, this type of information that is shared between functions will be termed cross-function exchange.

When applying the Cybersecurity Framework to the principle of data integrity, it is important to consider the effect various functions have on each other. For example, backup files, though a subcategory of Protect in SP 1800-25, do not actually mitigate damage until they are applied in the Recover function of SP 1800-11. Conversely, the Recover function of SP 1800-11 is ill-prepared without successful backup files being taken during the protect function in SP 1800-25. Similarly, information about a zero-day vulnerability is, by definition, unknown until the vulnerability has been exploited. Even though this information is not available until the Respond function of SP 1800-26, the information can be applied in the Identify function of SP 1800-25 to mitigate future exploits of the same vulnerability. In this section, we discuss various ways the presented capabilities for the Data Integrity projects distribute information in order to strengthen each function.

6.1 Backup and Restoration

Perhaps the most obvious example of cross-function interaction lies within the action of recovering in the SP 1800-11 architecture. Certain assets within an organization are identified as critical (IDENTIFY). Backup files of these assets are created as a preemptive measure taken to protect data from modification (PROTECT). Once data has been modified undesirably, to the degree that the modification constitutes a loss of integrity, a restoration capability uses the information stored in these backup files to return the data to its pre-modification state (RECOVER).

In practice, backup and restoration are typically part of the same product, because one is useless without the other. Asset identification is sometimes a separate product which facilitates human identification of assets, depending on the needs of the organization.

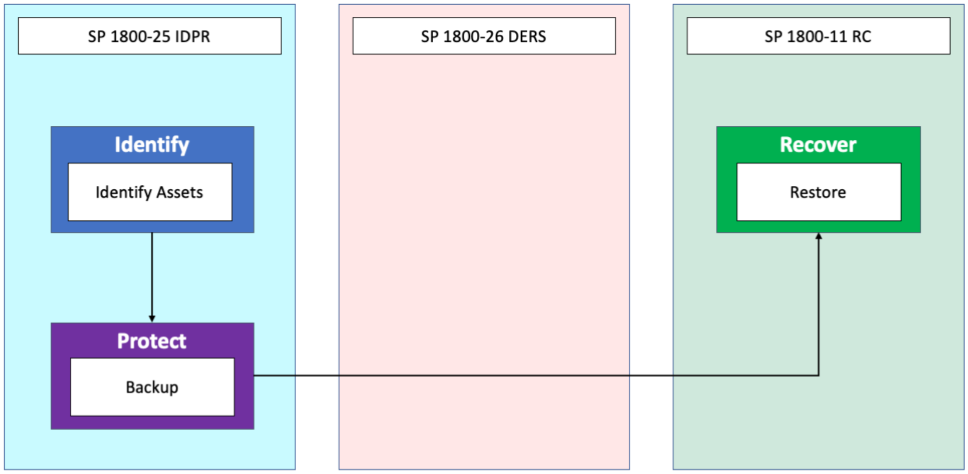

Figure 6-1 Backup and Restoration Cross Function Diagram

To understand how other functions interoperate in situations such as:

- Integrity monitoring
- Malware detection
- Denylists
- Vulnerability response
- Policy updates and user privileges

See Appendix C— Cross Function Interactions.

7 Additional Considerations

As previously stated in the document, the capabilities listed are derived from the architectures proposed in the 1800-series documentation. These capabilities and exemplar technologies are not the only capabilities that can provide data security. Should an organization wish to implement other data security technologies, substitution for capabilities can easily occur and achieve the same architectural goals from the 1800-series documents, so long as the substituted technologies provide the same framework functions and subcategories. Thus, in each of the 1800-series documents, a mapping to the Cybersecurity Framework is provided as a tool to enable this substitution. This capability of using the mapping as a guide to use other technologies demonstrates NCCoE's tenet of proposing flexible and adaptable solutions.

As an example of differing capabilities that provide data security, Appendix D— Additional Data Security Capabilities discusses other relevant technologies that address elements of data security and additional sources of information about them.

8 Summary

Using the guidance in this document, an organization can cohesively integrate and apply the guidance in the Data Integrity suite of practices guides: SP 1800-11, SP 1800-25, SP 1800-26. Implementing this guidance will allow an organization to address security needs with respect to the integrity of their data across all five functions of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. Once all necessary tools and systems are integrated, this document also provides guidance on how to constantly improve an enterprise cybersecurity posture by effectively applying information gathered from each of the steps to the other areas. In the end, organizations will be better prepared to handle the impact of a data integrity event within their enterprise.

References

[1] Federal Bureau of Investigations, *How to Protect Your Networks from Ransomware,* available: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

[2] United States Secret Service, *United States Secret Service & Homeland Security Investigations,* May 10, 2016, available: https://www.secretservice.gov/data/investigation/Cybersecurity_Joint_USSS_ECTF_HSI_Ransomware_Advisory.pdf

[3] D. K. Zafra, K. Lunden, N. Brubaker, and J. Kennelly. “Ransomware Against the Machine: How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT.” Fireeye.com. https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html (accessed Jun. 2, 2020).

[4] Federal Bureau of Investigation. (2019, October). *HIGH-IMPACT RANSOMWARE ATTACKS THREATEN U.S. BUSINESSES AND ORGANIZATIONS* [Brochure]. Washington, DC: Author.

[5] Cryptographic Key Management Workshop Summary—June 8-9, 2009, NIST Interagency Report 7609, June 2009. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7609.pdf

[6] Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009, April 2015. [Online]. Available: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

[7] NIST. Cybersecurity Framework. Available: http://www.nist.gov/cyberframework

[8] NIST/NCCoE. Attribute Based Access Control. Available: https://www.nccoe.nist.gov/projects/building-blocks/attribute-based-access-control

[9] NIST/NCCoE. Identity and Access Management (IdAM). Availble: https://www.nccoe.nist.gov/projects/use-cases/idam

[10] Newhouse, William and Weeks, Sarah, *Securing Non-Credit Card, Sensitive Consumer Data Consumer Data Security for the Retail Sector,* NCCoE/NIST, May 5, 2016. Available: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/cr-securing-consumer-data-project-description-draft.pdf

[11] FirstData, *EMV and Encryption + Tokenization: A Layered Approach to Security,* 2020. Available: https://www.firstdata.com/downloads/thought-leadership/EMV-Encrypt-Tokenization-WP.PDF

[12] Maji, Biswajit, *Implement Data Masking to Protect Sensitive Data: Part 1,* IBM, January 5, 2015. Available: http://www.ibmbigdatahub.com/blog/implement-data-masking-protect-sensitive-data-part-1

Appendix A—Acronyms

CSF	Cybersecurity Framework
CPU	Central Processing Unit
DI	Data Integrity
DERS	Detect/Respond [CSF Categories]
IDPR	Identify/Protect [CSF Categories]
NCCoE	National Cybersecurity Center of Excellence
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
SP	Special Publication
RC	Recover [CSF Category]

Appendix B—Glossary

Architecture

A highly structured specification of an acceptable approach within a framework for solving a specific problem. An architecture contains descriptions of all the components of a selected, acceptable solution while allowing certain details of specific components to be variable to satisfy related constraints (e.g., costs, local environment, user acceptability).

SOURCE: FIPS 201-2

Asset

A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

SOURCE: CNSSI 4009-2015

Backup

Duplicating data onto another medium

SOURCE: NIST SP 800-69

Backup files

A copy of files and programs made to facilitate recovery if necessary.

SOURCE: NIST SP 800-34 Rev. 1

Denylist

A list of discrete entities, such as hosts or applications, that have been previously determined to be associated with malicious activity.

SOURCE: NIST SP 800-94

Cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to

	ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. **SOURCE:** CNSSI 4009-2015 (NSPD-54/HSPD-23)
Data	A subset of information in an electronic format that allows it to be retrieved or transmitted. SOURCE: CNSSI-4009
Data Integrity	The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. SOURCE: CNSSI-4009
Event	Any observable occurrence in an information system. **SOURCE:** NIST SP 800-53 Rev. 4 (Adapted from CNSSI 4009)
Firewall	A gateway that limits access between networks in accordance with local security policy. **SOURCE:** CNSSI 4009-2015 (NIST SP 800-32)
Maintenance	Any act that either prevents the failure or malfunction of equipment or restores its operating capability. **SOURCE:** NIST SP 800-82 Rev. 2
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system. SOURCE: NIST SP 800-111
Policy	Statements, rules or assertions that specify the correct or expected behavior of an entity. For example, an authorization

policy might specify the correct access control rules for a software component.

SOURCE: NIST SP 800-95

Privilege A right granted to an individual, a program, or a process.

SOURCE: CNSSI 4009-201

Reporting The final phase of the computer and network forensic process, which involves reporting the results of the analysis; this may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process. The formality of the reporting step varies greatly depending on the situation.

SOURCE: NIST SP 800-86

Vulnerability Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

SOURCE: FIPS 200 (Adapted from CNSSI 4009)

Appendix C—Cross Function Interactions

C.1 Integrity Monitoring

Monitoring the integrity of files, programs, and systems in an enterprise is a process that takes place across multiple functions of the Cybersecurity Framework. Again, a prerequisite to Integrity Monitoring, similar to backups, is that critical assets in an enterprise have been identified (IDENTIFY). An initial baseline is typically performed before an attack ever occurs. This essentially means assuming the system is in a “good” state and recording integrity information for relevant assets while in this state (PROTECT).

The primary purpose of the baseline is to be used in comparison with the current state of operations. Whenever assets such as programs, files, and systems, are changed, these changes are logged. From there, they can be used as indicators of destructive data integrity events

(DETECT), and to inform decisions made when restoring to the last known good (RECOVER). As integrity monitoring software typically provides information such as the user, program, and time associated with any changes, it can aid administrators in deciding which backup constitutes the “last known good”.

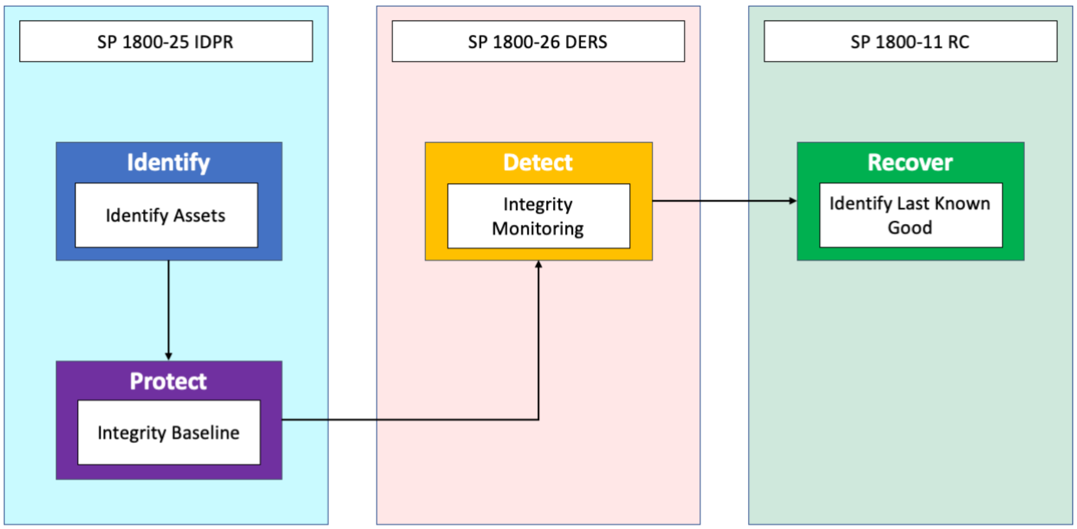

Figure C-1 Integrity Monitoring Cross Function Diagram

C.2 Detection

In the SP 1800-26 architecture, event detection can be significantly enhanced through iterations of functions in the Cybersecurity Framework. Either through use of signatures or recognition of behaviors, information is gained enabling an appropriate response. The more quickly information is gained from an attack and applied, the earlier in the cycle the executable can be stopped (RESPOND). The information about the malware can be used to prevent the next attack and detect the attack if it spreads to other systems (DETECT).

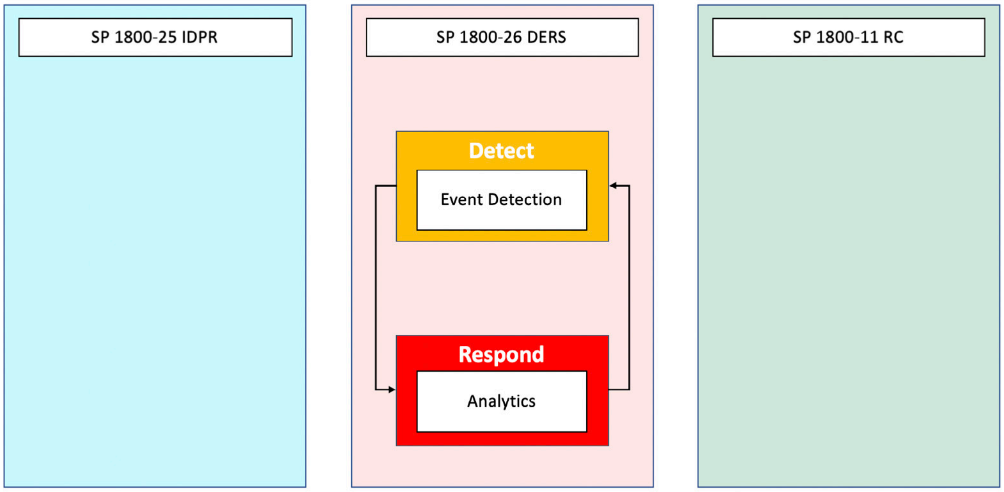

Figure C-2 Detection Cross Function Diagram

C.3 Denylist

Denylists, though typically a measure taken before an attack happens to prevent communication between workstations and potentially malicious servers, rely on their ability to adapt to new information. Denylists are a simple way of enhancing an organization's Respond capabilities and Protecting from future attacks. An organization with sufficient detection capabilities can learn from an attack by observing where the attack originated from, and the servers the attack communicated with (RESPOND). After review to ensure that the servers involved are indeed malicious, the servers can simply be added to the denylist. Furthermore, future malware which originates from these servers would be prevented before the attack happens (PROTECT).

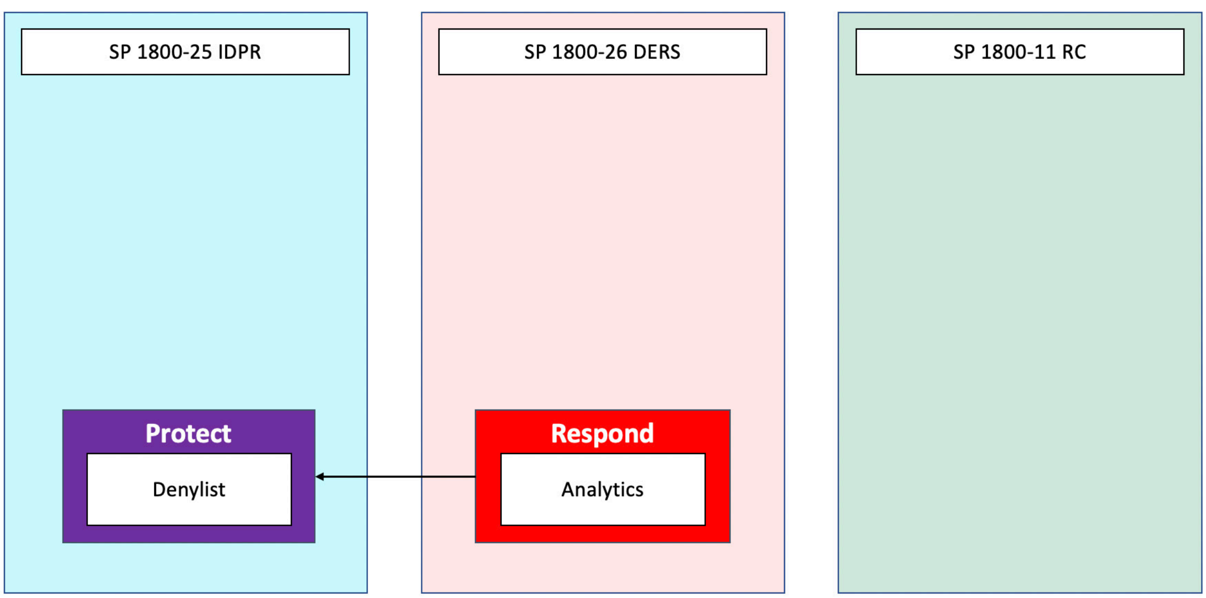

Figure C-3 Denylist Cross Function Diagram

C.4 Vulnerability Response

Exploitations resulting from zero-day vulnerabilities are difficult to protect against. They are typically attacks on previously undiscovered or unknown vulnerabilities. Products may have varying success detecting these zero-days before they happen. If these products fail to detect an exploitation attempt, the information gathered from the attack after it has started (RESPOND) can be applied to discover (IDENTIFY) and fix (PROTECT) vulnerabilities.

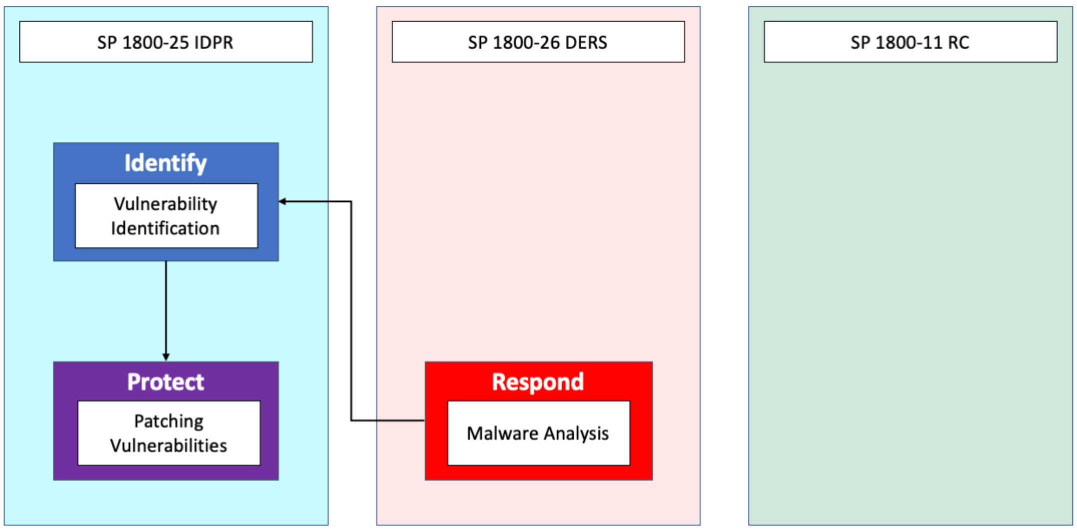

Figure C-4 Vulnerability Response Cross Function Diagram

C.5 Policy Updates and User Privileges

There are other ways to mitigate destructive data integrity attacks. Information about malicious insiders gained from logs (RESPOND) can be used to restrict privileges and inform policy changes within the organization (PROTECT). Policy changes can be anything from restricting downloads of certain file types to reforming the organization's password policies to better thwart attacks. These policy changes typically would require some sort of human element, and they are specific to the software and construction of the enterprise in question – but they can be informed by studying the data made available after an attack has occurred.

Restricting user privileges is an access control function and can be a reaction to the discovery of a malicious insider, or something less straightforward, such as a web server system account being able to access resources that shouldn't be available to clients. Access control is discussed in other projects at the NCCoE [8, 9] , but the information which informs these changes is aggregated in the Logging capability in SP 1800-26 and SP 1800-11.

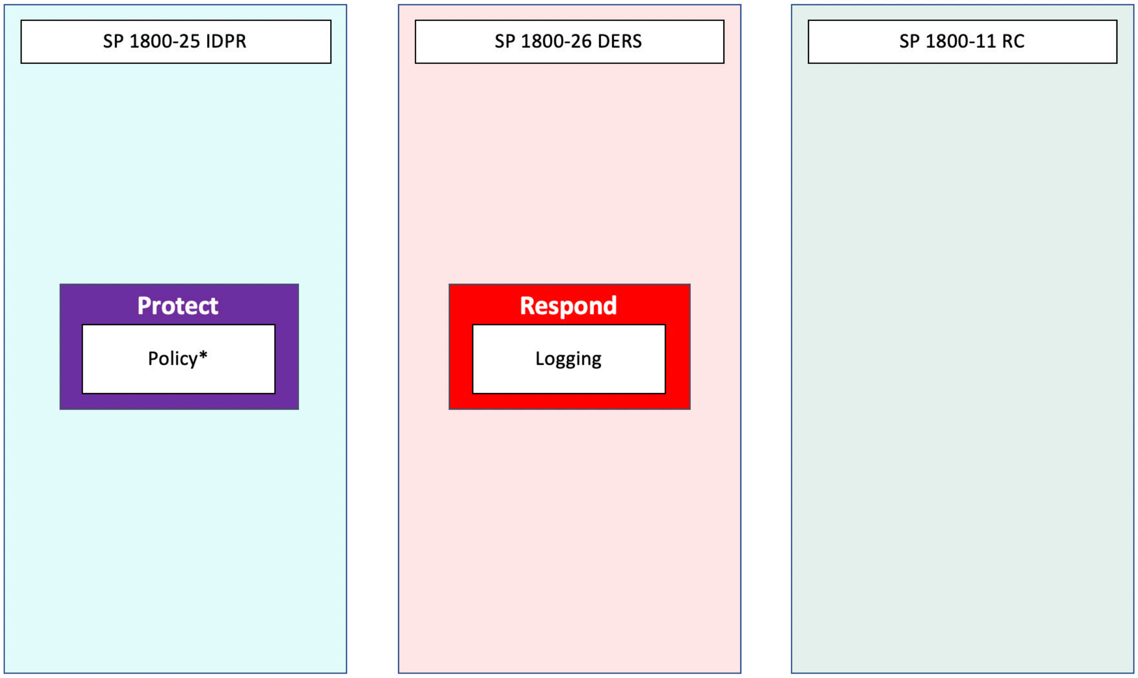

Figure C-5 Policy Updates and User Privileges Diagram

Appendix D—Additional Data Security Capabilities

D.1 Data Tokenization and Data Masking

Data tokenization “is the process of replacing sensitive data with surrogate values that remove risk but preserve value to the business” [11]. The concept aims to remove valuable data from use in order to reduce the risk of comprise or corruption to the data. Data masking is a type of data obfuscation that implements a process of “de-identifying or scrambling specific data elements to protect them from unauthorized access by specific groups of end users” [12], again, aiming to reduce the risk of compromise or corruption.

Both of these concepts are in utilized in the NCCoE publication entitled “Securing Non-Credit Card, Sensitive Consumer Data: Consumer Data Security for the Retail Sector” [10]. This document provides a high-level architecture and example scenarios where these types of data security techniques may be impactful.

D.2 Content Filtering

The Committee on Nation Security Systems defines in CNSSI No. 4009 a security filter as “a secure subsystem of an information system that enforces security policy on the data passing through it.” [6] Content filtering is a type of security filter that is designed to explicitly enforce a security policy on data. This technology can be applied in many different places throughout an organization including at the network layer, the application layer, or in a specialized appliance. As an example, in SP 1800-26 a content filtering device was incorporated in a specialized email sanitization device to enforce both event detection and mitigation capabilities. In event detection, the content filtering device is enforcing the security policy and in the mitigation capability the device can sanitize any malicious data before it ever reaches an end user device.

Although the SP 1800-26 document does use content filtering, it was referenced by the capabilities it provided, event detection and mitigation, through a specialized device. This content filtering technology, as stated above, could be applied to more places within the infrastructure should an adopting organization desire.

D.3 Additional Capabilities

Many long-standing capabilities (e.g., anti-virus, denylisting, browser-blockers) and more newly developing technologies (e.g., block-chain) will continue to be options to build into a data security strategy. It is not the intention of NCCoE documents to represent one specific capability over another or advocate for one specific vendor. Instead, through a series of architectural builds, the projects aim to provide technical guidance and reference architectures that address the challenge of data integrity. These architectures implement commercial and open-source products, standards, and best practices that align to the Cybersecurity Framework and illustrate how to implement the functions and subcategories of the framework.

D.4 Additional Sources for Information

In recent publications FireEye [3] assesses that ransomware attacks “have cost victims across a variety of industry verticals many millions of dollars in ransom and collateral costs….[and] significant disruptions and delays to the physical processes that enable organizations to produce and deliver goods and services.” The publication continues by explaining that across industries there exists “multiple disclosures of ransomware infections in both IT [(information technology)] and OT [(operational technology)] networks. Infections result in the same outcome: insufficient or late supply of end products or services.”

Ransomware maintains its success by continuing to be able to evolve and adapt to remediation attempts that organizations implement. The Federal Bureau of Investigation (FBI) Cyber Division has engaged in this battle against ransomware by also producing publications to help explain this type of malware and considerations that organizations should enact. As an example, FBI publications [4] explain “ransomware is a form of malware that targets both human and technical weakness in organizations and individual networks in an effort to deny the availability of critical data and systems. […] Recent iterations target enterprise end users, making awareness and training a critical preventative measure.” The literature provides high level consideration focused on prevention, business continuity, and other technical considerations.