RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: PDAC-T08

Your Data's Integrity: Protect & Respond to Ransomware and Critical Events

Anne Townsend

The MITRE Corporation/NCCoE

Approved for Public Release; Distribution Unlimited. Public Release Case Number 19-0447

AGENDA

- Data Integrity (DI) Programs Structure
- DI: Identify & Protect Architecture
- DI: Detect & Respond Architecture
- DI: Recover Architecture
- Additional Use Case Scenarios
- Follow On Work

RSAConference2019

Data Integrity Programs Structure

Aligned to the NIST Cybersecurity Framework & Cyberattack Life Cycle

Challenge

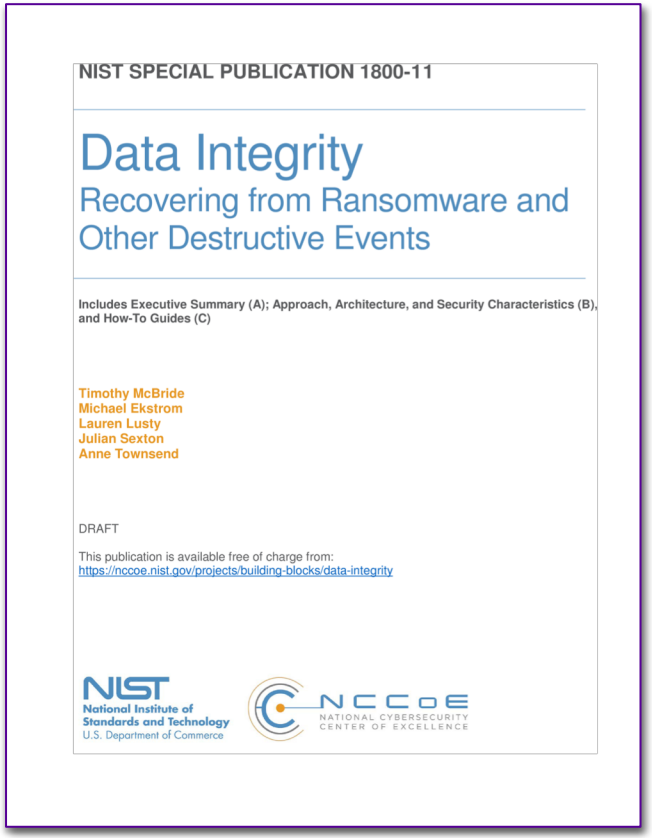
- Organizations' data -- database records, system files, configurations, user files, applications, and customer data -- all potential targets of data integrity attacks

Approach

- Effectively **identify and protect** assets against data integrity attacks
- Detail methods and potential tool sets that can **detect, mitigate, and contain** data integrity events
- Effectively **recover** from a data integrity event

Data Integrity Projects

- 1800-xx Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events (ID-PR)
- 1800-xx Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events (DE-RS)
- 1800-11 Data Integrity: Recovering from Ransomware and Other Destructive Events (REC)


NIST SPECIAL PUBLICATION 1800-11

Data Integrity
Recovering from Ransomware and Other Destructive Events

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B), and How-To Guides (C)

Timothy McBride
Michael Ekstrom
Lauren Lusty
Julian Sexton
Anne Townsend

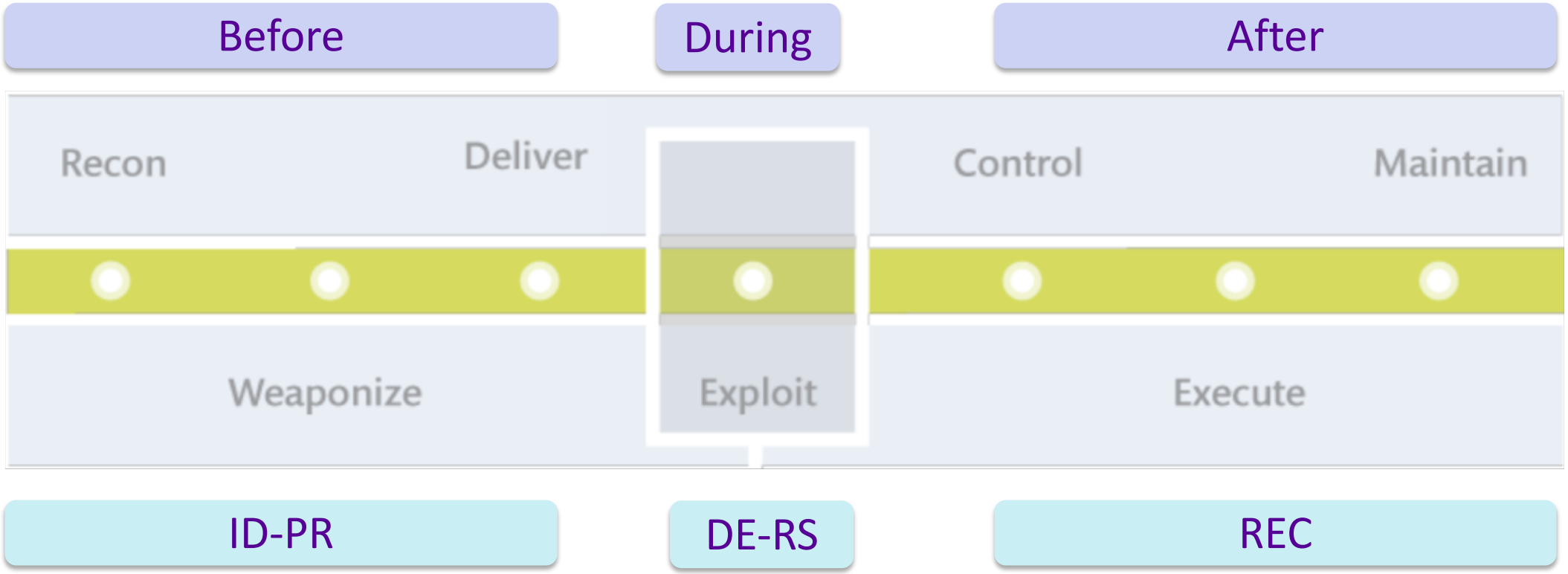
DRAFT

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

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Cyber Attack Lifecycle



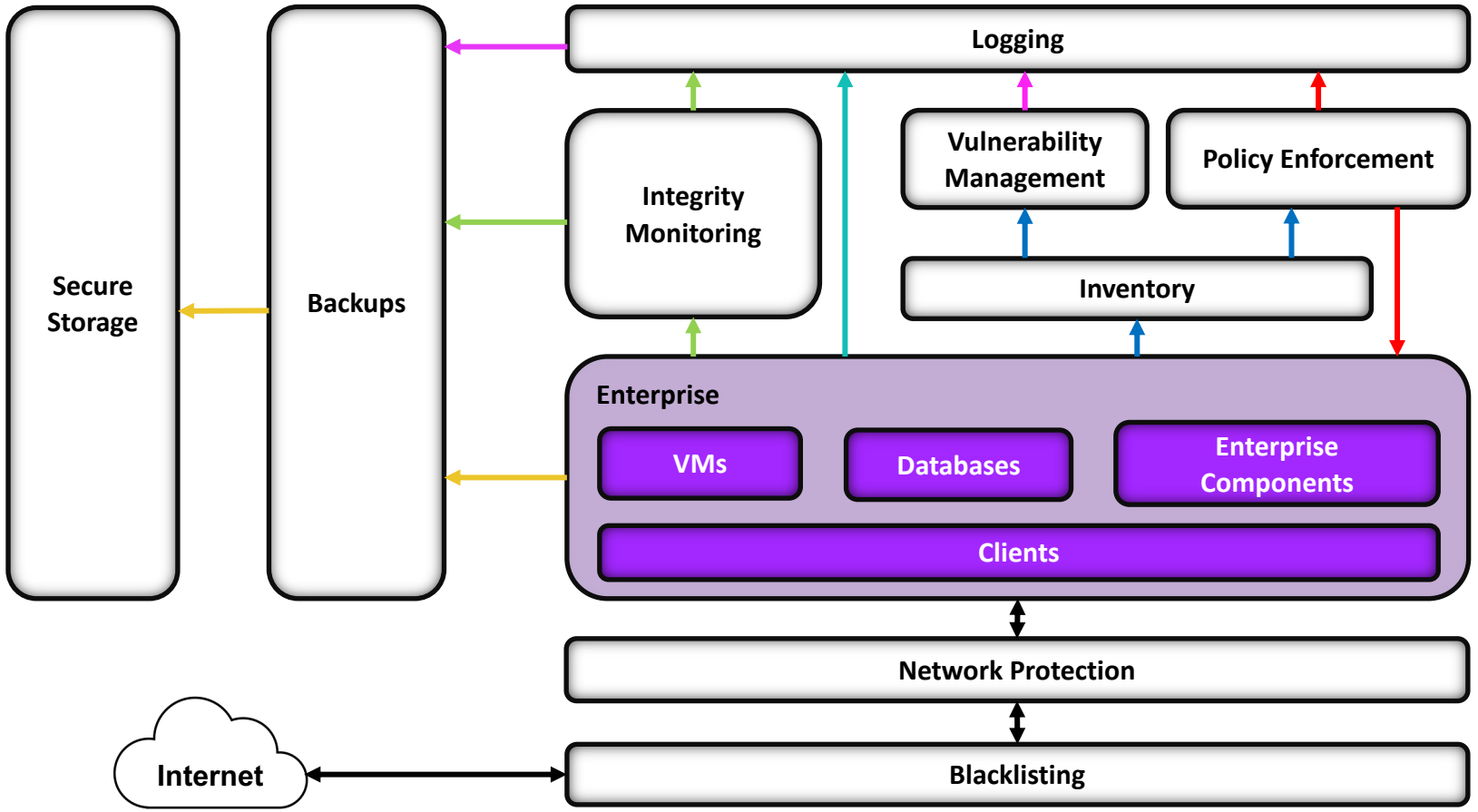
http://www2.mitre.org/public/industry-perspective/documents/lifecycle-ex.pdf

Data Integrity Project Partners

RSAConference2019

Data Integrity: The Architectures

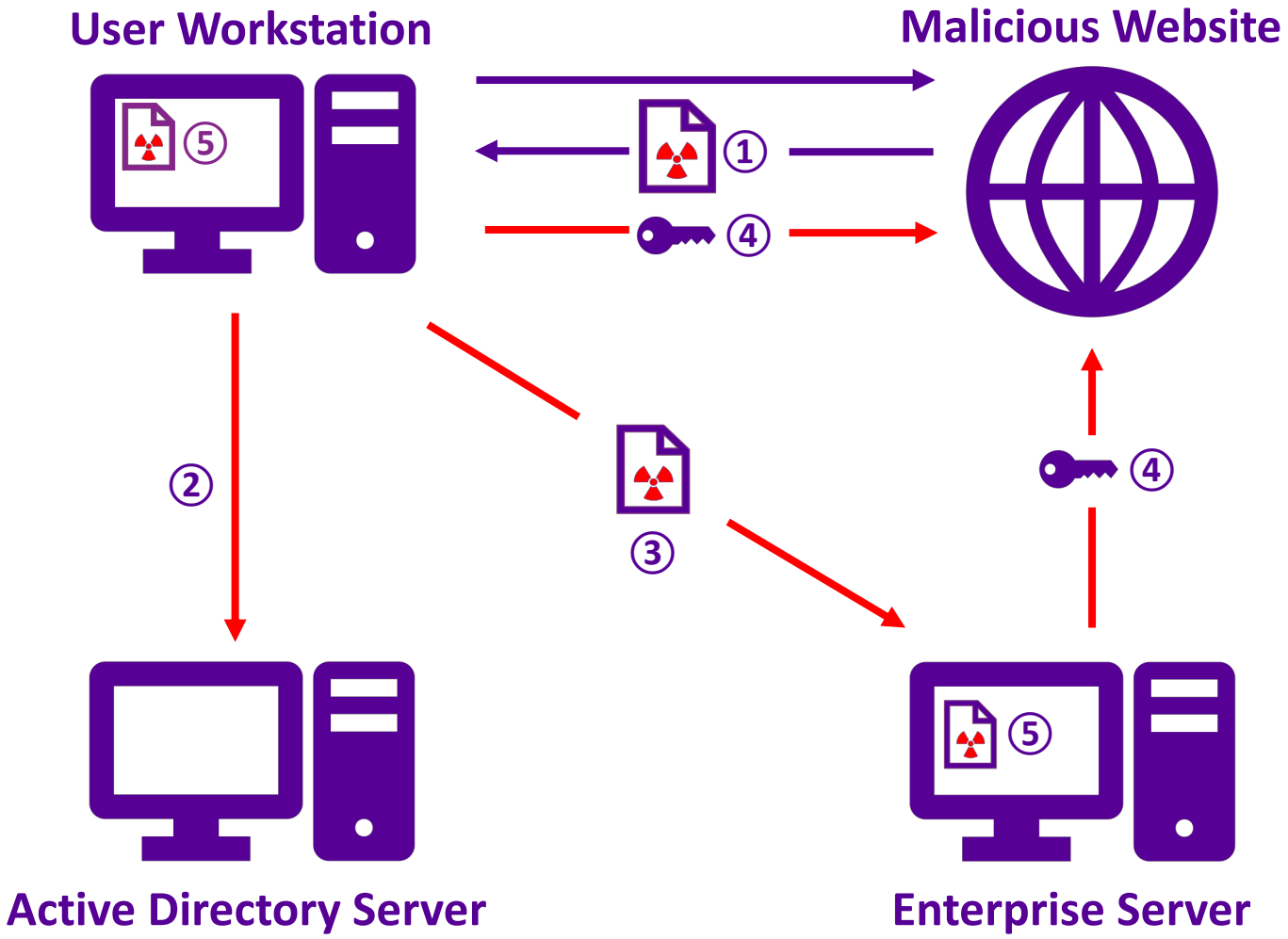
Architecture for Identify & Protect



Legend

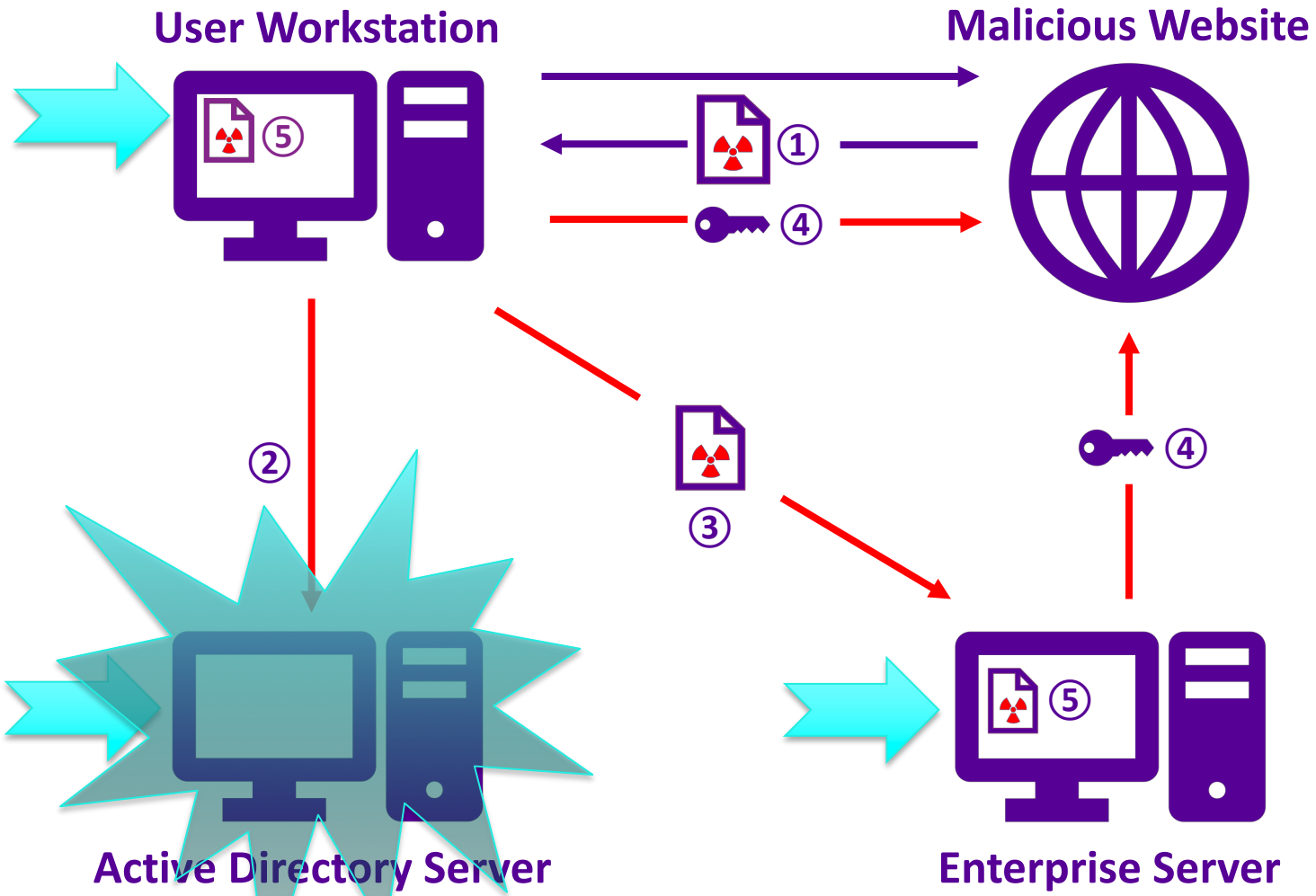
- Policy Information/operations
- Integrity Information
- Vulnerability Information
- Inventory Information
- Backup Information
- Log/Audit Information
- Organizational Data

Ransomware via Web Vector and Self-Propagation



1. User visits watering hole website and becomes infected with ransomware.
2. Ransomware exploits a vulnerable Active Directory server to obtain credentials.
3. Ransomware propagates to an enterprise server.
4. Ransomware generates encryption key and sends it to home server.
5. Ransomware executes on both machines and encrypts files.

Ransomware via Web Vector and Self-Propagation



1. [illegible] and [illegible] ransomware.

Blacklisting

2. [illegible] Active [illegible] credentials.

Vulnerability Mgmt

3. [illegible] encrypted.

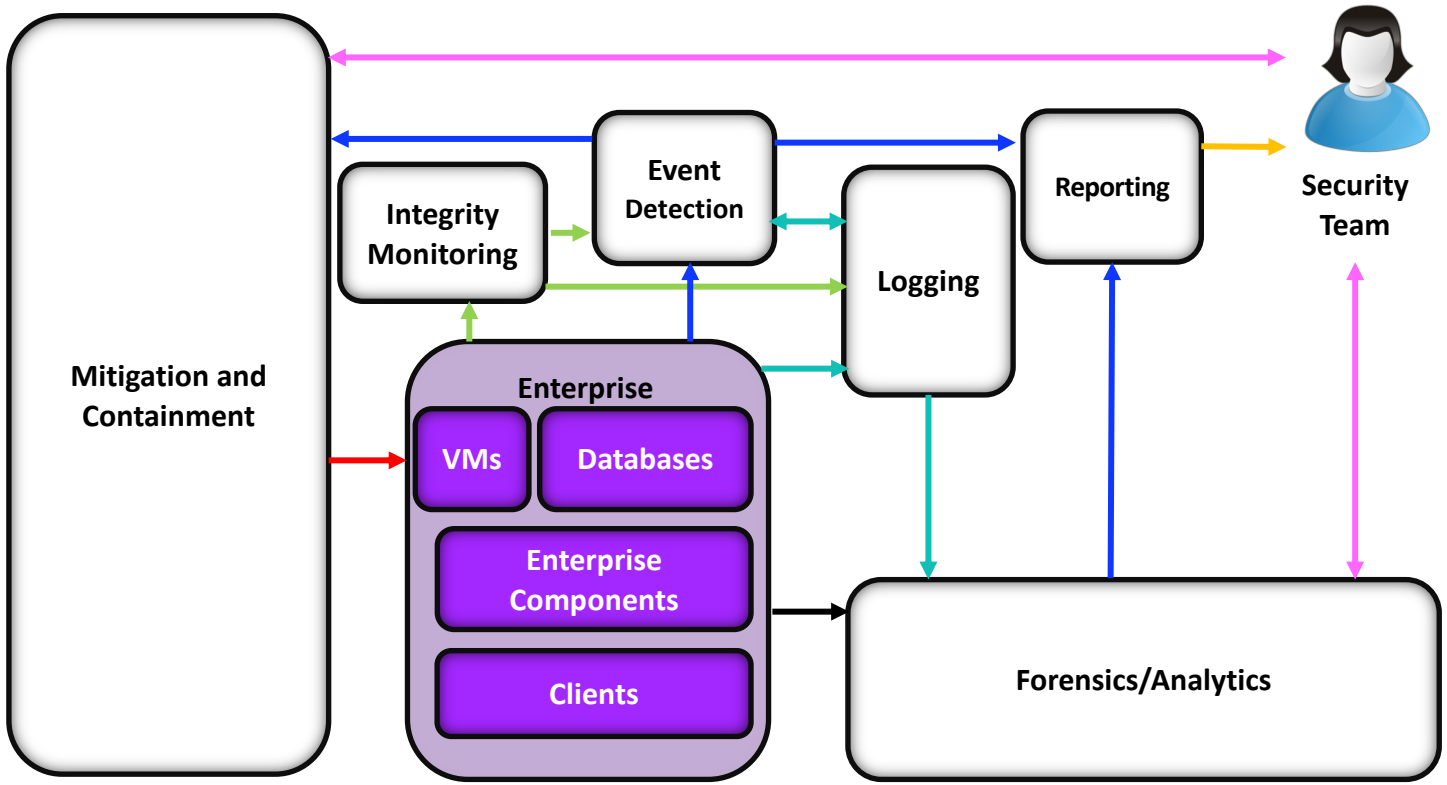
Network Protection

4. Ransomware generates encryption key

Integrity Monitoring

5. [illegible] machines and encrypts files.

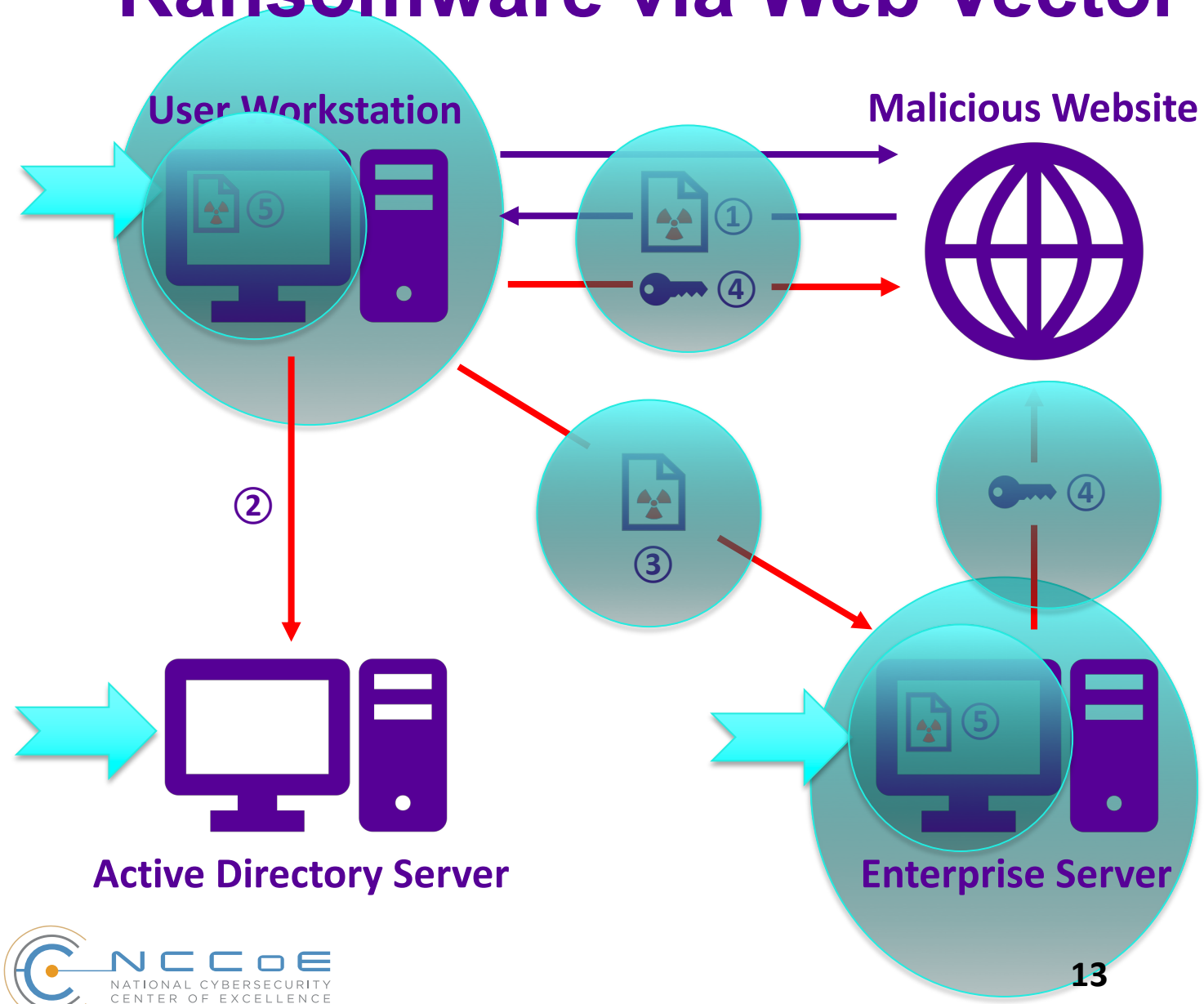
Architecture for Detect & Respond



Legend

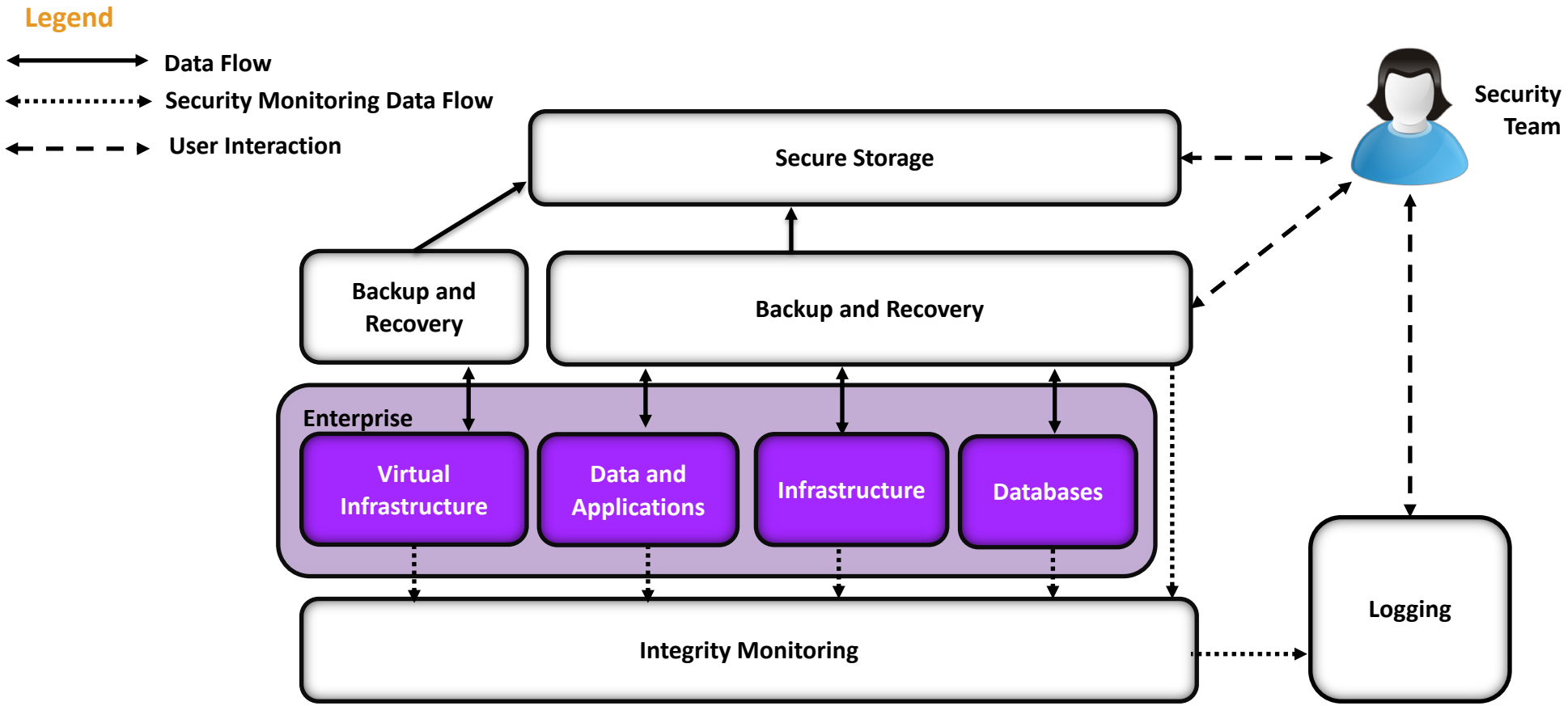
- Detected Events
- Integrity Information
- Mitigation Actions
- Log/Audit Information
- Anomaly detection
- Forensic Information
- User Interaction

Ransomware via Web Vector and Self-Propagation



1. User visits watering hole website and becomes infected with ransomware.
2. Ransomware exploits a vulnerable Active Directory server to obtain credentials.
3. Ransomware propagates to an enterprise server.
4. Ransomware generates encryption key and sends it to home server.
5. Ransomware executes on both machines and encrypts files.

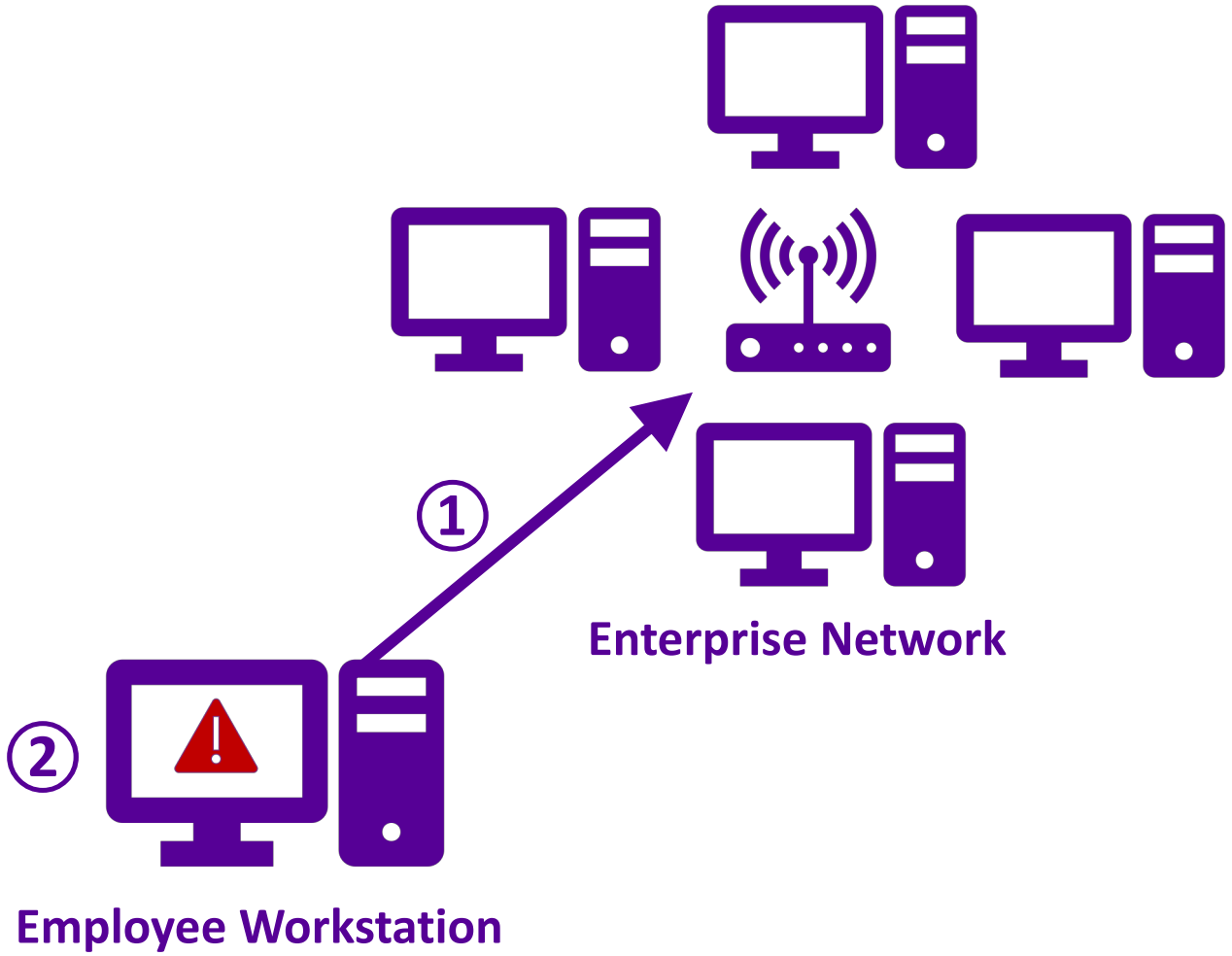
Architecture for REC



RSAConference2019

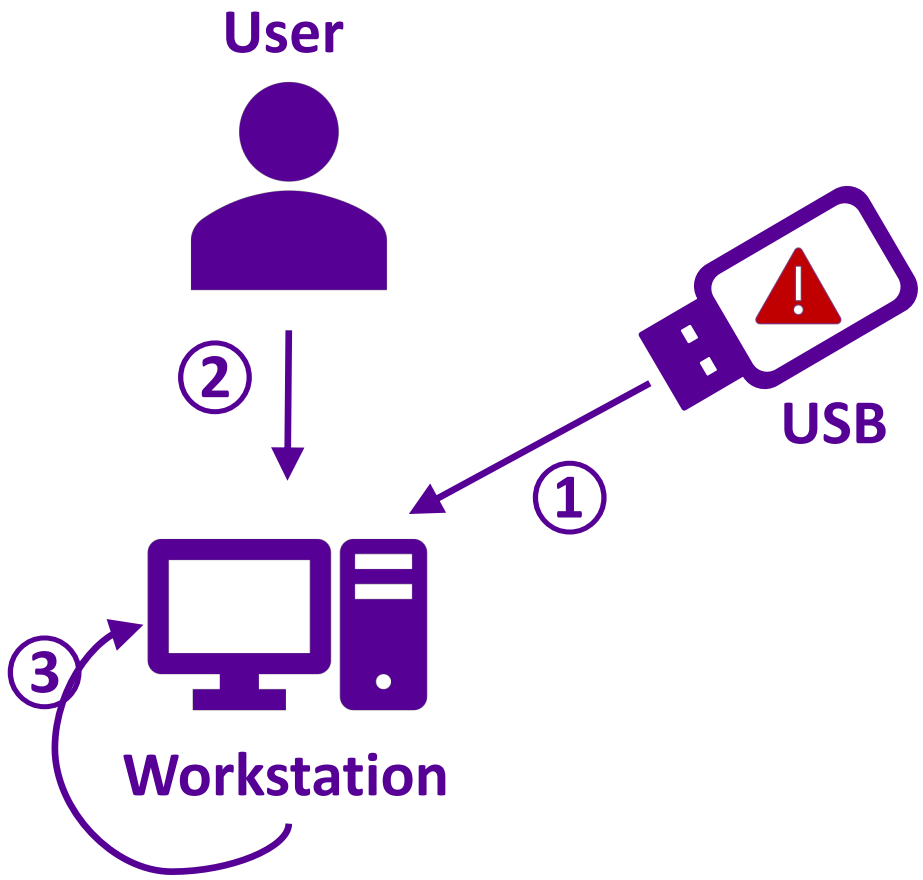
Additional Use Case Scenarios

New Employee (Unique to ID-PR)



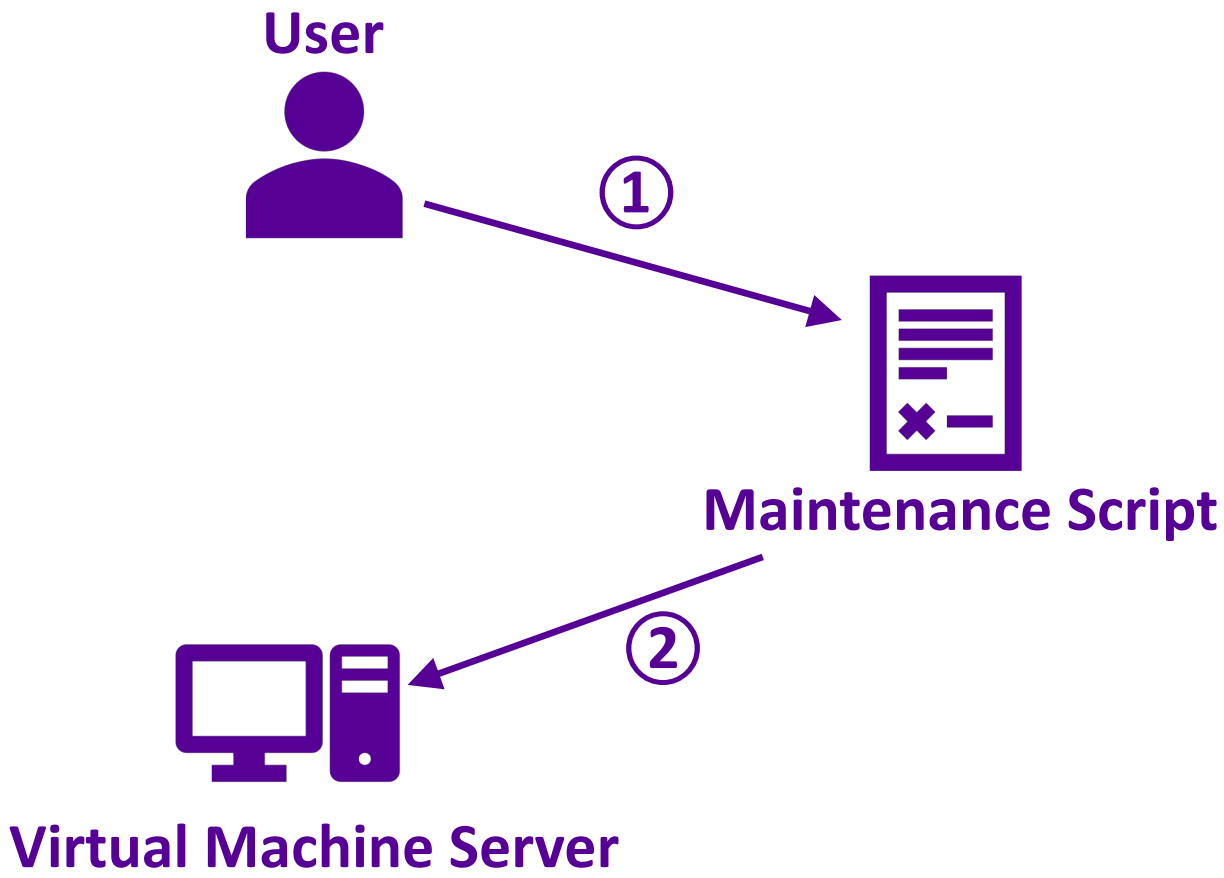
1. A new employee receives a new workstation and connects it to the network.
2. The workstation is missing critical security updates and threatens the safety of the network.

Destructive Malware via USB Vector



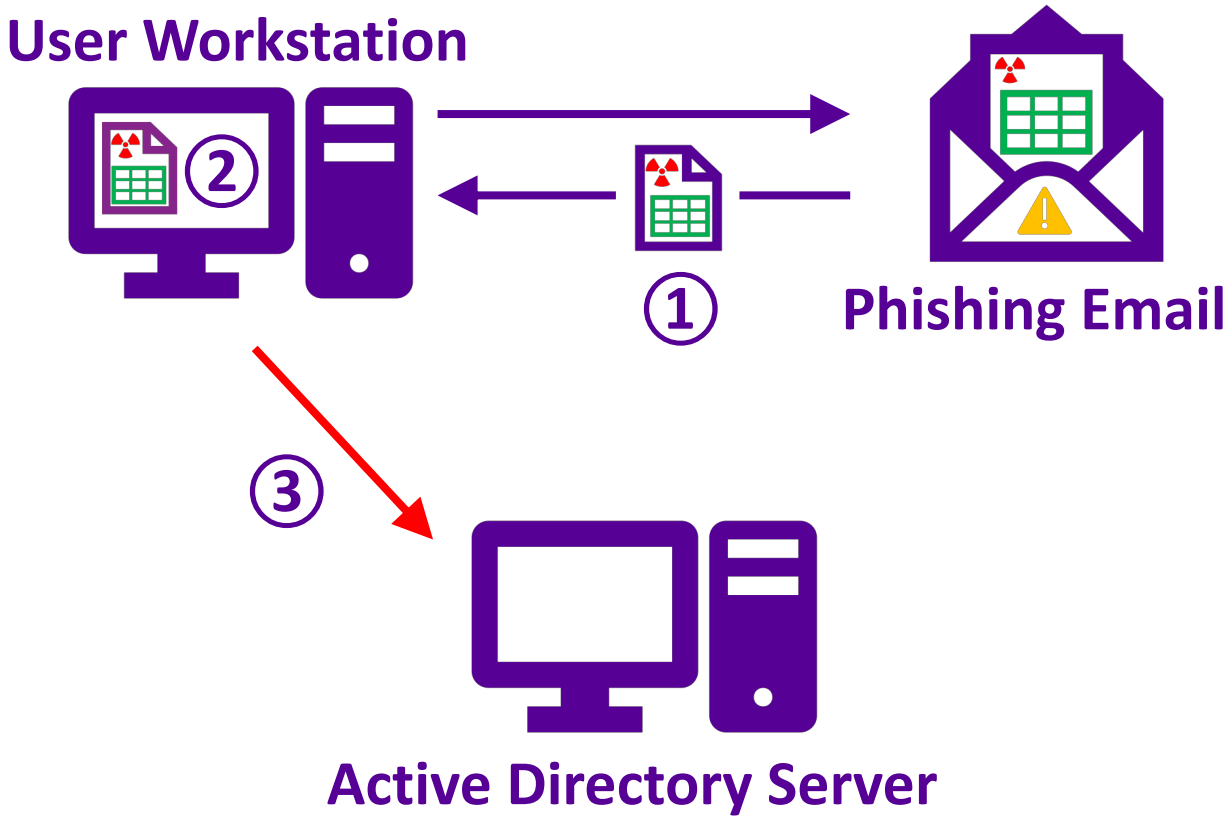
1. User finds malicious USB in parking lot and inserts it into their workstation.
2. The malicious USB has several files on it, including a README and an executable named “notepad.exe.” The user double clicks either of the files.
3. The file executes. It modifies and deletes files in the user’s Documents folder.

Accidental VM Deletion via Maintenance Script



1. A privileged user creates a maintenance script to perform maintenance on the organization's virtual machines.
2. The maintenance script contains a bug, and accidentally deletes a virtual machine.

Backdoor Creation via E-mail Vector

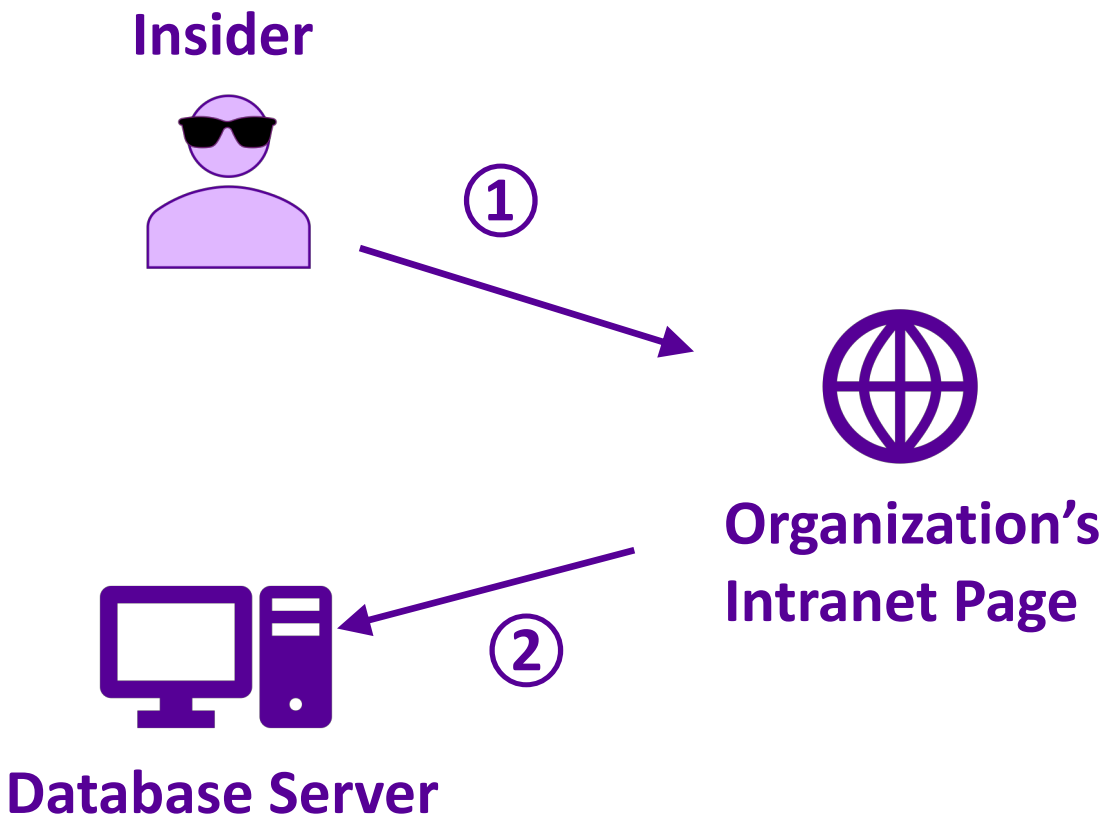


1. A privileged user receives an email as a target of a spear phishing campaign. The phishing email contains a malicious spreadsheet attachment.

2. The user opens the spreadsheet, and is prompted to run macros.

3. The spreadsheet creates backdoors in Active Directory using the user's permissions.

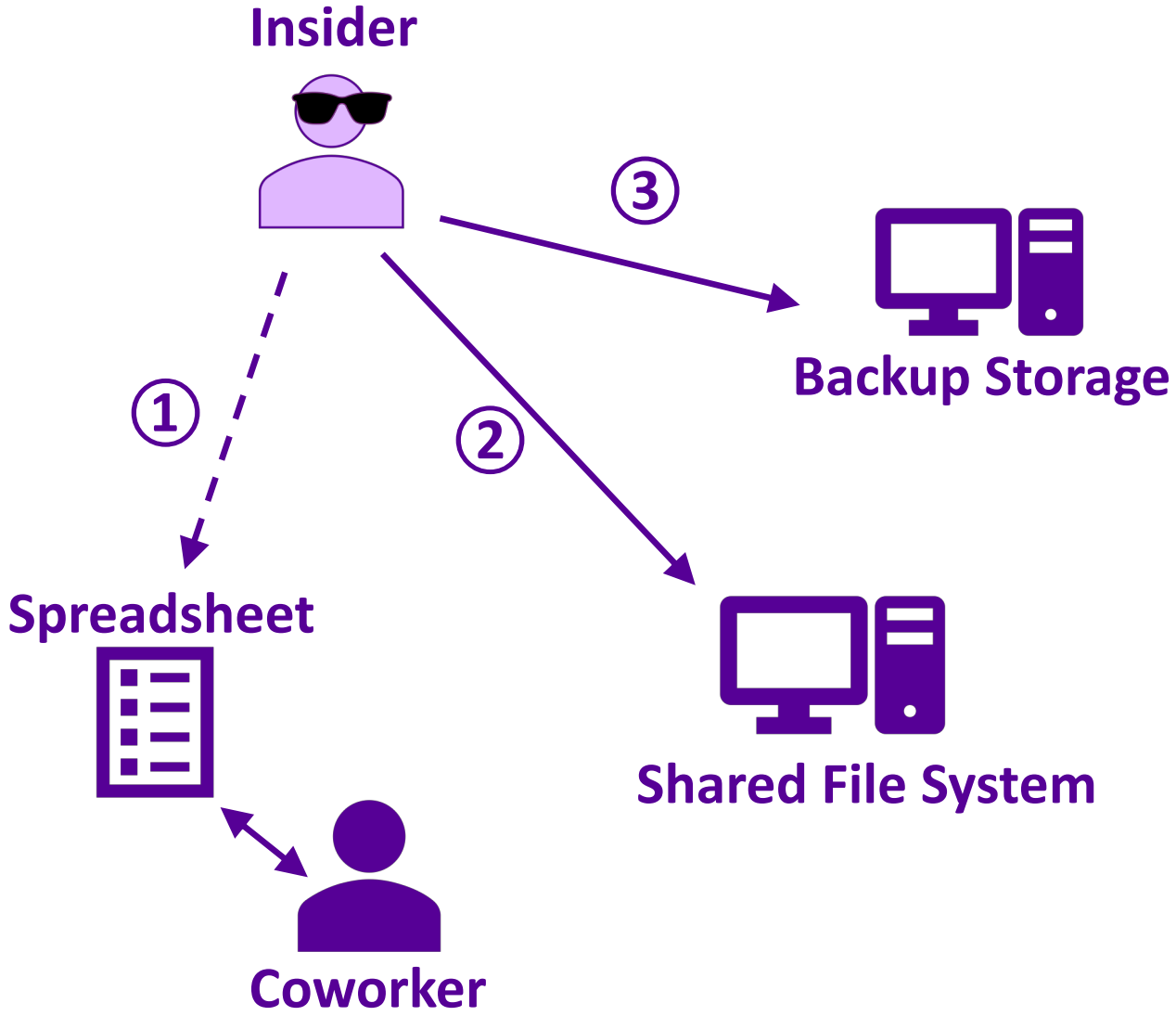
Database Modification via Malicious Insider



1. A malicious insider operating for a competing organization seeks to disrupt the organization's operations. He discovers a vulnerability on the organization's intranet page which allows him to manipulate the database.

2. Through the web page, he is able to delete data from tables in the database.

File Modification via Malicious Insider

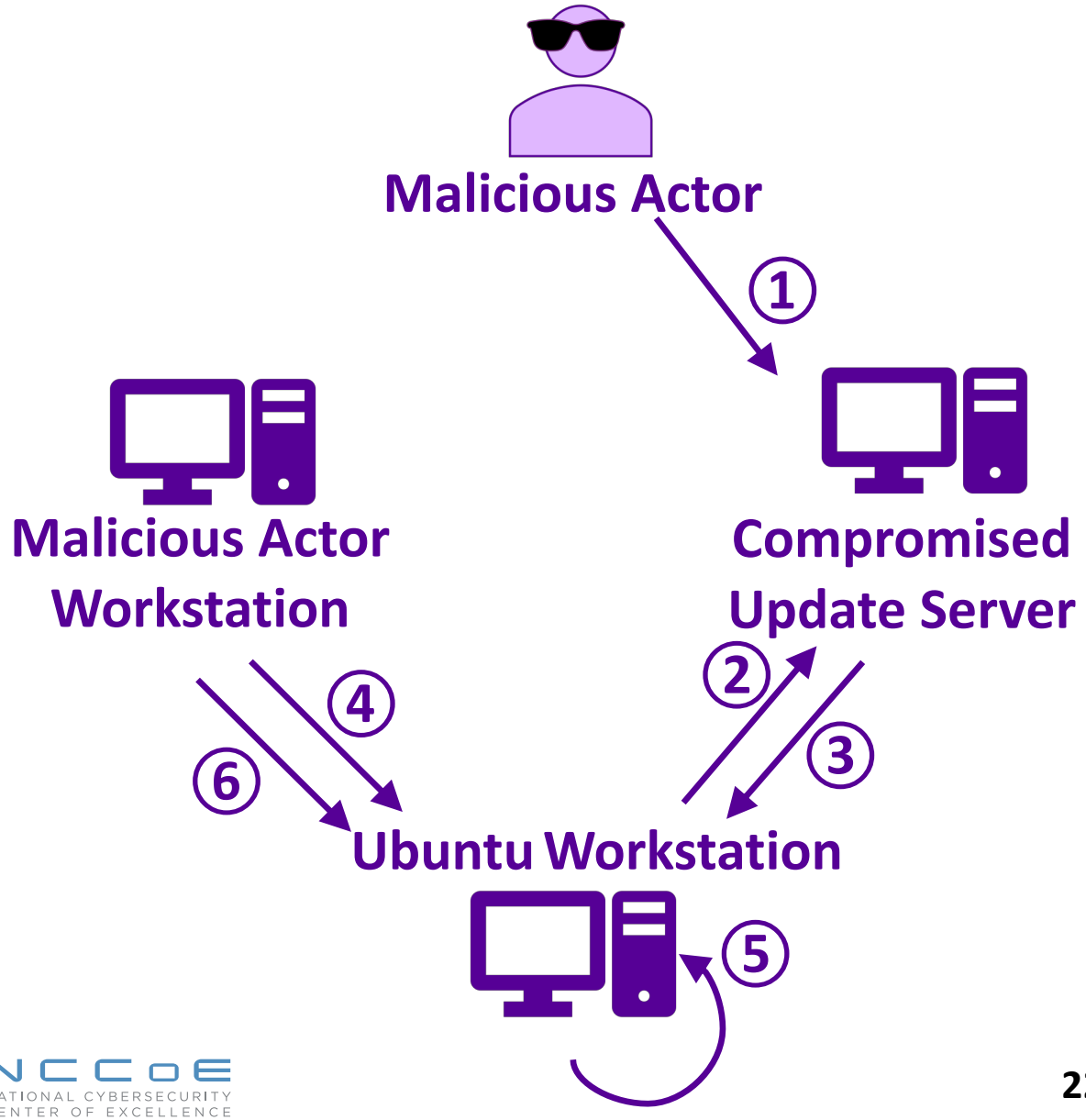


1. An employee sees an administrative coworker editing a spreadsheet that contains employee salary and stock information. He takes note of the format of the spreadsheet.

2. The employee acquires administrative credentials which were left on a sticky note. He uses these credentials to search the company files for his name in an attempt to change the number of shares he receives annually.

3. He also attempts to change any backups of the file.

Backdoor Creation via Compromised Update Server



1. A malicious actor has compromised an update server, so that the update server distributes vulnerable versions of vsftpd, an Ubuntu file sharing service.
2. An Ubuntu workstation in the enterprise requests updates from the compromised update server.
3. The update server provides the vulnerable service to the workstation.
4. The malicious actor exploits a backdoor in the vulnerable service from his workstation.
5. The service opens a port on the Ubuntu machine.
6. The malicious actor is able to acquire a root shell through this open port, from his workstation.

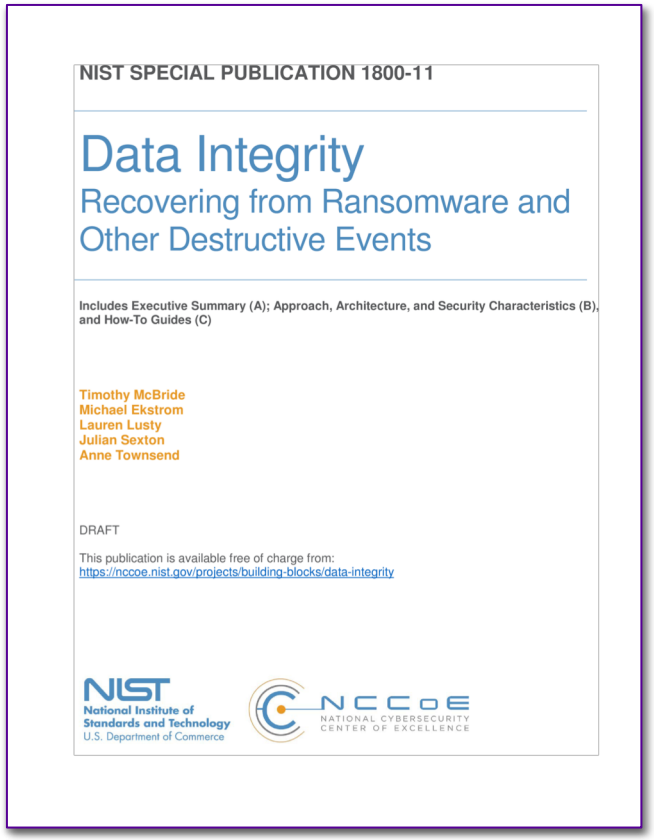
RSAConference2019

Data Integrity: Project Artifacts

Available at nccoe.nist.gov

SP 1800 Series: Volumes Overview

- Volume A: Executive Summary
  - High-level overview of the project, including a summary of the challenge, solution, and benefits
- Volume B: Approach, Architecture, and Security Characteristics
  - Deep dive into challenge and solution, including approach, architecture, and security mapping to the NIST Cybersecurity Framework and other relevant standards
- Volume C: How-To Guide
  - Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance


NIST SPECIAL PUBLICATION 1800-11

Data Integrity

Recovering from Ransomware and Other Destructive Events

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B), and How-To Guides (C)

Timothy McBride
Michael Ekstrom
Lauren Lusty
Julian Sexton
Anne Townsend

DRAFT

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

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SP 1800 Series: Mappings

Security Controls Mapping

CSF Function	CSF Subcategory	SP800-53R4[a]	IEC/ISO 27001[b]	CIS CSC[c]	NERC-CIP v5[d]
Identify	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-1	CIP-002-5.1
	ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-2	CIP-002-5.1
Protect	PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	A.11.1.1 A.11.1.2 A.11.1.4 A.11.1.6 A.11.2.3		CIP-006-6
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7	A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3		
	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	AU family	A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4 A.12.7.1	CSC-6	CIP-006-6

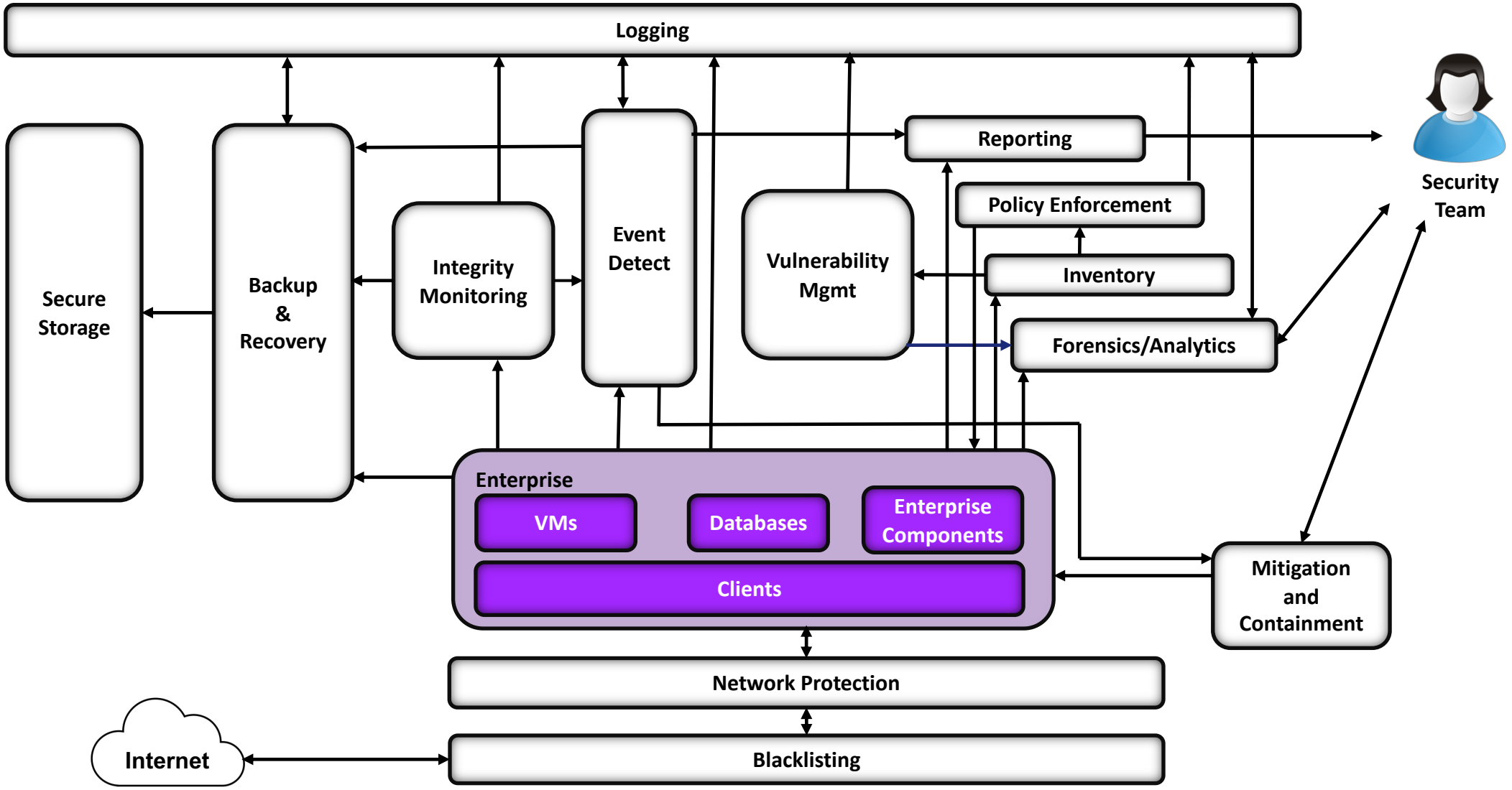
Technology Mapping

Component	Specific Product	Function	CSF Subcategories
Corruption Testing	ArcSight Enterprise Security Manager (ESM) v6.9.1 Tripwire Enterprise v8.5 Tripwire Log Center Manager v7.2.4.80	• provides monitoring for changes to data on a system • provides logs, detection, and reporting, in the event of changes to data on a system • provides audit capabilities for database metadata and content modifications • provides file hashing and integrity testing independent of file type (can include software files) • provides notifications for changes to configuration • provides file monitoring for cybersecurity events • provides analytic capabilities to determine the impact of integrity events	PR.DS-6, PR.PT-1, DE.AE-4
Secure Storage	Spectrum Protect and Backup and Replication v8.1.0 WORMdisk v151228	• provides write-once read-many file disk storage for secure backups of integrity information • provides immutability of backups • creates encrypted backups	PR.DS-1, PR.IP-4
Logging	ArcSight Enterprise Security Manager (ESM) v6.9.1	• provides auditing and logging capabilities configurable to corporate policy • provides logging of some user	PR.PT-1, DE.AE-4, DE.CM-1, DE.CM-3

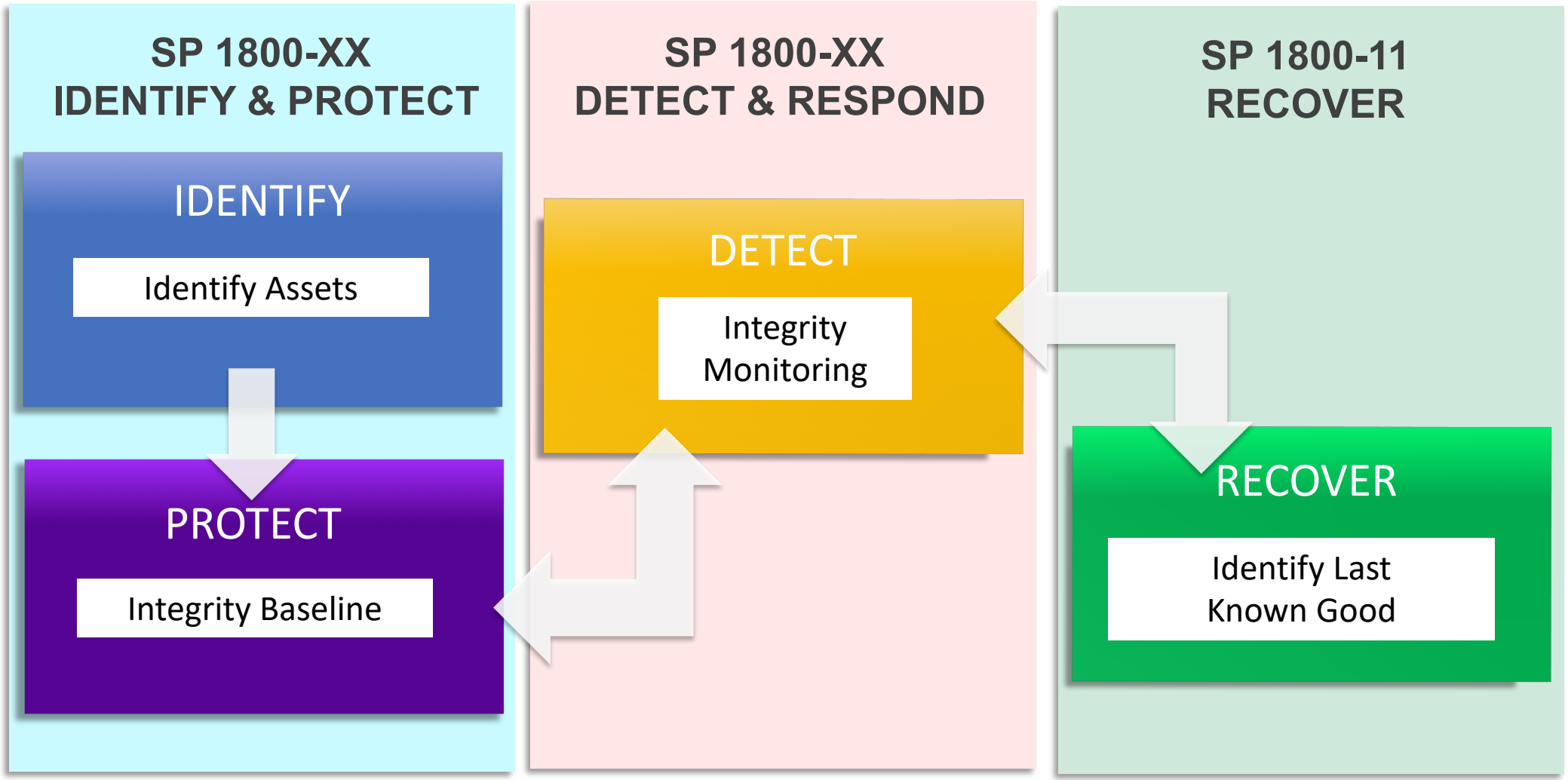
RSAConference2019

Follow on Data Security Work

One Unified Data Integrity Architecture



Tying It All Together



Next Project: Data Confidentiality

- Addressing how to identify, protect, detect, respond, and recover to a data confidentiality attack.
- Unique: User controls need to also be in place in order to ensure only authorized individuals can access to the data.
- Currently at the project beginning with the release of the project description documents available on NCCoE website

RSAConference2019

Applying What You've Learned

Applying This Work

Educate + Learn = Apply

- Provide strategies for data security
- Understand how these strategies may apply to your own organization
- Bring back to your organization new approaches to resolve data security challenges

Immediate Actions

- Investigate into your own organization if you have the capabilities presented here
- Collaborate with us!!!
- Participate in builds with us to help refine, focus, and strengthen data security capabilities.
  - Can communicate through our email address, communities of interest, meetings, or website

Future Actions

- Overlay the proposed architecture with your own organization's architecture and note differences
- Map differences to security control map; gauge what's missing
- Use technology mapping to understand if one's own organization technologies are providing the necessary capabilities

Apply What You Have Learned Today

- Next week you should:
  - Re-assess your own organization's data security capabilities
  - Join the NCCoE Data Integrity Community of Interest
- In the first three months following this presentation you should:
  - Understand what capabilities your organization's technologies are providing
  - Understand what security controls may need to still be addressed
- Within six months you should:
  - Begin to incorporate potentially new capabilities to strengthen organization's ability to provide data security

Contact Information

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

Jennifer Cawthra
Government Lead
Jennifer.Cawthra@nist.gov

Anne Townsend
MITRE
apalm@mitre.org

Data Integrity Team
di-nccoe@nist.gov

RSAConference2019

Backup Slides

Compromised Update Server

	Identify	Protect	Detect	Respond
Machine connected to network.	Machine is identified. (Cisco ISE + CryptoniteNXT)	Machine is prevented from communicating on the internet prior to authentication. (CryptoniteNXT)		
Machine is unpatched.	Vulnerabilities due to lack of updates are detected. (Tripwire IP360)			

Vendors used in Ransomware Use Case

	Identify	Protect	Detect	Respond
User visits site		Site is blacklisted. (Cisco WSA)	Site is identified as malicious. (Cisco Stealthwatch + Symantec Security Analytics)	Site is added to blacklist. (Used in Protect)
User downloads tool on A		Downloads from site are blocked. (Cisco WSA)	Tool identified as malicious. (Cisco AMP)	Download stopped or files deleted. (Cisco AMP?)
User runs tool on A			Tool identified as malicious. (Cisco AMP)	Execution stopped and analyzed. (Cisco AMP) Tools added to blacklist. (Cisco AMP?)
Tool downloads files		Downloads from site are blocked. (Cisco WSA)	Downloaded files are identified as malicious. (Cisco AMP)	Download stopped or files deleted. (Cisco AMP?) Files added to blacklist. (Cisco AMP?)
Tool exploits AD	Vulnerability is identified. (Tripwire IP360)	Vulnerability is patched or machine is quarantined. (Cisco ISE)		
Tool copies r-ware to B		Attempts to propagate are prevented. (Cryptonite NXT)	Attempts to propagate are detected. (Cisco AMP/Stealthwatch + Symantec Security Analytics)	Affected machine disconnected. (Cryptonite NXT)
R-ware runs on A and B			Execution identified as malicious. (Cisco AMP)	Execution stopped and analyzed. (Cisco AMP) R-ware added to blacklist. (Cisco AMP?)
R-ware sends key to home		Connection to site blocked. (Cisco WSA)	Communication intercepted. (Symantec Security Analytics) Site identified as malicious. (Cisco Stealthwatch + Symantec Security Analytics)	Site added to blacklist. (Used in Protect)
R-ware encrypts files	Sensitive files are inventoried. (Symantec DLP)	Backups are taken. (FileZilla + Duplicati) Integrity information baselined. (Tripwire Enterprise)	Logs of file changes are collected. (Micro Focus ArcSight)	

Destructive Malware

	Identify	Protect	Detect	Respond
User inserts USB			USB insertion detected and logged. (Micro Focus ArcSight? + Cisco AMP?) Executable is identified as malicious. (Cisco AMP)	Executable deleted. (Cisco AMP)
User runs executable			Executable is identified as malicious. (Cisco AMP)	Execution stopped. (Cisco AMP) Executable added to blacklist. (Cisco AMP?)
Executable deletes and changes files	Sensitive files are inventoried. (Symantec DLP)	Backups are taken. (FileZilla+Duplicati) Integrity information baselined. (Tripwire Enterprise)	Logs of file changes are collected. (Micro Focus ArcSight)	

VM Maintenance Error

	Identify	Protect	Detect	Respond
Maintenance script with error is executed		Error in script is patched. (Human)		
Script deletes virtual machine		Backups of virtual machines are taken. (FileZilla + Duplicati)	VM deletion is logged. (Tripwire Enterprise + Micro Focus ArcSight)	Event analyzed. (Micro Focus ArcSight)

Phishing For Backdoors

	Identify	Protect	Detect	Respond
User receives a phishing email with a malicious attachment.		Email is sorted into spam. (N/A)	Email is identified as malicious. (Glasswall)	Email is added to blacklist. (N/A)
User downloads the attachment, which is an Excel spreadsheet.			Attachment is identified as malicious. (Glasswall)	Attachment is deleted. (Glasswall)
User runs the Excel spreadsheet.			The spreadsheet is identified as malicious. (Glasswall + Cisco AMP)	Execution stopped. (Glasswall) Attachment is added to blacklist. (Glasswall?)
The Excel spreadsheet fetches malicious files.		Downloads from spreadsheets are blocked. (N/A) Downloads from site are blocked. (Cisco WSA)	Downloads from Spreadsheets are detected. (Symantec ATP?) Downloaded files are identified as malicious. (Cisco AMP)	Downloads are deleted. (Cisco AMP)
The Excel spreadsheet creates backdoors on the domain.		Configurations are baselined. (Semperis DSP) Backups of configuration are taken. (Semperis DSP + Semperis ADFR)	Downloaded executable is identified as malicious. (Cisco AMP) Account creation is logged. (Semperis DSP + Micro Focus ArcSight)	Execution stopped. (Cisco AMP) Downloads are added to blacklist. (Cisco AMP?) Download site added to blacklist.

Insider Threat – DB Change

	Identify	Protect	Detect	Respond
Malicious insider exploits vulnerability in company intranet.	Vulnerability is identified. (Human) Vulnerability is tracked. (Tripwire IP360)	Vulnerability is resolved. (Human)	Client information associated with web request is logged. (Cisco WSA + Micro Focus ArcSight + Symantec ICA)	
Database records are deleted.		Database backups are taken. (Database Software) Database is baselined. (Tripwire Enterprise + Micro Focus ArcSight)	Changes to the database are logged with appropriate information. (Tripwire Enterprise + Micro Focus ArcSight)	Information from attack reported. (Micro Focus ArcSight)

Insider Threat – File Change

	Identify	Protect	Detect	Respond
Employee searches files and backups.		Backups are encrypted. (FileZilla + Duplicati)		
Employee changes files.		Backups are taken. (FileZilla + Duplicati) Files are baselined. (Tripwire Enterprise)	Changes to files are detected. (Tripwire Enterprise + Symantec ICA)	Changes are reported. (Micro Focus ArcSight) User account is disabled/contained. (Semperis DSP + Cryptonite NXT)
Employee changes backups of files.		Backups are stored securely. (GreenTec WORMdisk)	Changes to backups are detected. (Tripwire Enterprise + Symantec ICA)	Changes are reported. (Micro Focus ArcSight) User account is disabled/contained. (Semperis DSP + Cryptonite NXT)

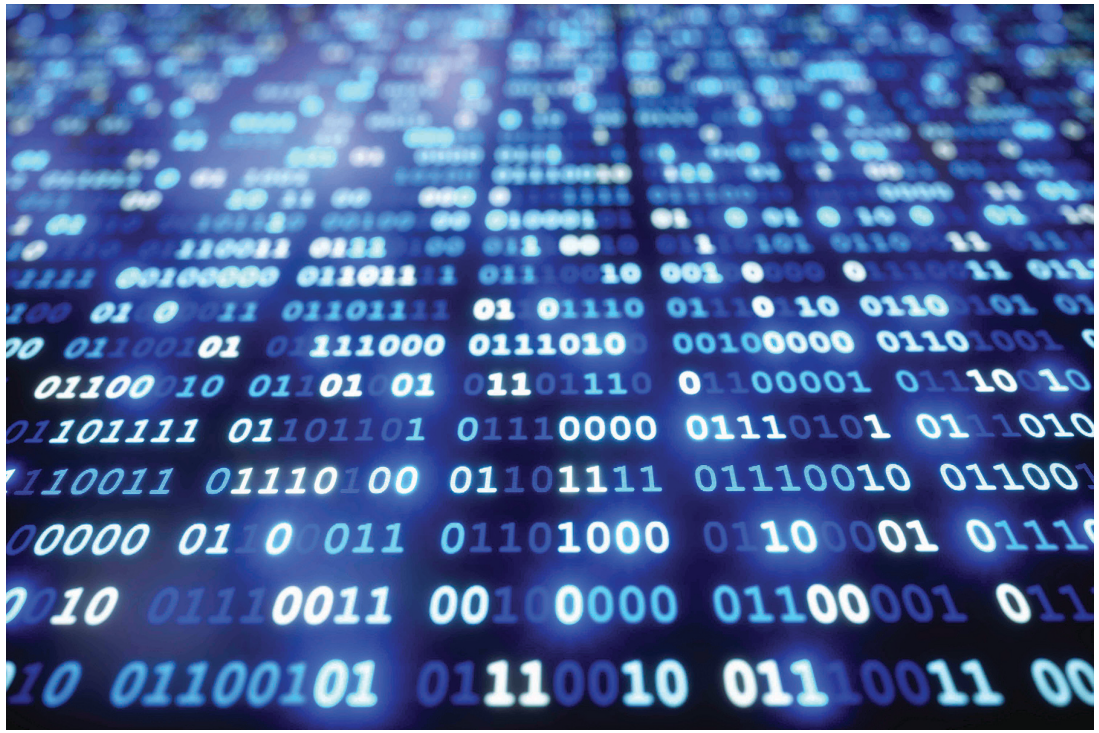
Compromised Update Server

	Identify	Protect	Detect	Respond
Vulnerable service is downloaded from server.		Downloads from site are temporarily blocked. (Cisco WSA + Cryptonite NXT)	Service is identified as malicious. (Cisco AMP)	Service is deleted/reverted. (Cisco AMP)
Vulnerable service is started.		Programs are baselined. (Tripwire Enterprise)	Service is identified as malicious. (Cisco AMP)	Service is stopped. (Cisco AMP?) Site is added to blacklist. Downloaded service is added to blacklist. (Cisco AMP?)
Malicious actor exploits a backdoor in the service.			Network traffic logged. (Symantec Analytics + Cisco Stealthwatch)	
Service opens port on machine.			Port opening detected. (Symantec Analytics + Cisco Stealthwatch)	Port closed. (CryptoniteNXT)
Malicious actor uses port to access the machine as root.		Backups are taken. (FileZilla + Duplicati) Files are baselined. (Tripwire Enterprise)	Intrusion is detected. (Cisco AMP)	Details of intrusion reported. (Micro Focus ArcSight)

Mission

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

Sector-Based Projects



- Commerce/Retail
- Energy
- Financial Services
- Healthcare
- Hospitality
- Manufacturing
- Public Safety/First Responder
- Transportation

Cross-Sector Projects

- Attribute Based Access Control (SP 1800-3)
- Data Integrity (SP 1800-11)
- Derived PIV Credentials (SP 1800-12)
- DNS-Based Secured Email (SP 1800-6)
- Mitigating IoT-Based DDoS
- Mobile Device Security (SP 1800-4)
- Privacy-Enhanced Identity Federation
- Secure Inter-Domain Routing (SP 1800-14)
- TLS Server Certificate Management (SP 1800-16)
- Trusted Geolocation in the Cloud (NISTIR 7904)