National Cybersecurity Center of Excellence

A Resource and Partner for Securing FinTech

AUSTCyber National FinTech Cyber Security Summit
September 28, 2017
Agenda

• NCCoE Overview
• Projects and Publications
• Engaging with the NCCoE
NCCoE Mission

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

**DEFINE**

OUTCOME: Define a scope of work with industry to solve a pressing cybersecurity challenge

**ASSEMBLE**

OUTCOME: Assemble teams of industry organizations, government agencies, and academic institutions to address all aspects of the cybersecurity challenge

**BUILD**

OUTCOME: Build a practical, usable, repeatable implementation to address the cybersecurity challenge

**ADVOCATE**

OUTCOME: Advocate adoption of the example implementation using the practice guide
Practice Guide
Volume A: Executive Summary
• High-level overview of the project, including summaries 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 NIST Cyber Security Framework (CSF) and other relevant standards

Volume C: How-To Guide
• Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance
## Example: ARM Map to Financial Industry

<table>
<thead>
<tr>
<th>CSF Subcategory</th>
<th>NIST 800-53 rev4&lt;sup&gt;a&lt;/sup&gt;</th>
<th>IEC/ISO 27001&lt;sup&gt;b&lt;/sup&gt;</th>
<th>FFIEC CAT v1&lt;sup&gt;c&lt;/sup&gt;</th>
<th>FFIEC IT Exam Handbook Information Security&lt;sup&gt;d&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established.</strong></td>
<td>CP-2, PS-7, PM-11</td>
<td>A.6.1.1</td>
<td>D1.R.St.B.1: Information security roles and responsibilities have been identified.</td>
<td>IS.B.7: Employees should know, understand, and be held accountable for fulfilling their security responsibilities. Financial institutions should define these responsibilities in their security policy.</td>
</tr>
<tr>
<td><strong>ID.BE-4: Dependencies and critical functions for delivery of critical services are established.</strong></td>
<td>SA-14, CP-8, PE-9, PE-11, PM-8, SA-14</td>
<td>A.11.2.2, A.11.2.3, A.12.1.3</td>
<td>D1.G.IT.B.2: Organizational assets (e.g., hardware, systems, data, and applications) are ....</td>
<td>IS.WP.I.4.1: Review and evaluate ...</td>
</tr>
<tr>
<td><strong>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.</strong></td>
<td>AU Family IR-5, IR-6</td>
<td>A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1</td>
<td>D2.MA.Ma.B.1: Audit log records and other security event logs are reviewed and retained in a secure manner.</td>
<td>IS.B.79: Institutions should strictly control and monitor access to log files whether on the host or in a centralized logging facility. IS.WP.II.B.13: Determine ... IS.B.83: Because the identification ....</td>
</tr>
</tbody>
</table>
Projects and Publications

⭐ • Attribute Based Access Control (SP 1800-3)
• Consumer/Retail: Multifactor Authentication for e-Commerce
⭐ • Data Integrity: Recovering from a Destructive Malware Attack
• Derived Personal Identity Verification Credentials
⭐ • DNS-Based Email Security (SP 1800-6)
• Energy: Identity and Access Management (SP 1800-2)
• Energy: Situational Awareness (SP 1800-7)
• Financial Services: Access Rights Management (SP 1800-9)
• Financial Services: IT Asset Management (SP 1800-5)

⭐ • Healthcare: Securing Electronic Health Records on Mobile Devices (SP 1800-1)
• Healthcare: Securing Wireless Infusion Pumps (SP 1800-8)
• Hospitality: Securing Property Management Systems
• Manufacturing: Capabilities Assessment for Securing Manufacturing Industrial Control Systems
• Mobile Device Security (SP 1800-4)
• Privacy-Enhanced Identity Federation
• Public Safety/First Responder: Mobile Application Single Sign-On
• Secure Inter-Domain Routing
• Transportation: Maritime: Oil & Natural Gas
• Trusted Geolocation in the Cloud (NISTIR 7904)

⭐ Applicable to financial sector
Ways to Collaborate

Harry Perper, Chief Engineer
NCCoE

harry.perper@nist.gov
301-975-0367
Twitter: @hperper
financial_nccoe@nist.gov
Questions?
Data Integrity (ransomware recovery)
Data Integrity

Recovering from ransomware and other destructive events

Overview

• Businesses face a near-constant threat of destructive malware, ransomware, and malicious insider activities that can alter or destroy critical data and cripple operations.

• Organizations need to be able to recover quickly from a ransomware attack and trust the accuracy and precision of the recovered data.

• This project will explore methods to effectively recover operating systems, databases, user files, applications, and software/system configurations after a successful malware attack.

Project Status

PG published, ready to demo in our lab at the NCCoE.

Collaborate with Us

• Read Data Integrity Project Description.
• Email di-nccoe@nist.gov to join the Community of Interest for this project.
DATA INTEGRITY (RANSOMWARE RECOVERY)

Legend:
- Security Monitoring Data Flow
- User Data Flow

System Admin

Security Analyst

Legend:
- Security Monitoring Data Flow
- User Data Flow
Data Integrity: Potential Outcomes

Adopting all or part of the example implementation can:

• Detect backup data-tampering
• Reduce the impact of a data-corruption event
• Reduce downtime caused by data-corruption
• Improve trustworthiness of backup data
• Reduce the negative impact to the reputation of an organization due to data-corruption events
• Provide management with improved continuity of operations
Privileged Account Management
Privileged Account Management

Securing privileged access for the financial services sector

Challenges

- System administrators in the financial sector often share passwords, and directly access the systems they administer.

- Organizations need the ability to manage and monitor the access administrators have to data and systems.

Diagram:

- Administrators and other "privileged" users
  - Applications
  - Infrastructure
  - (X)aaS

Security Monitoring

Multi-factor Authentication ???
High-Level Architecture

- Access management
- Multi-factor authentication
- User isolation
- User monitoring
- System password obfuscation
- User action controls (command limiting)

This project demonstrates ways to manage administrator access to data and systems
Access Rights Management
Access Rights Management

Securing access for the financial services sector

Challenges

• Identity and access systems in the financial sector are often disjointed, complex to operate, and vulnerable to attackers or insider threats

• Organizations need the ability to easily issue, validate, and modify access rights from a central location

Project Status

PG published, ready to demo in our lab at the NCCoE

Collaborate with Us

• Read Access Rights Management Project Description
• Email financial_nccoe@nist.gov to join the Community of Interest for this project
Currently many organizations rely on manual processes to provision user access changes.
This project demonstrates ways to link existing and separate systems into a comprehensive solution.
Access Rights Management: Potential Outcomes

Adopting all or part of the example implementation can:

• Reduce damage caused by a successful insider threat attack by limiting the amount of data that any one person has access to

• Limit opportunity for a successful attack by reducing the available attack surface

• Increase the probability that investigations of attacks or anomalous system behavior will reach successful conclusions

• Reduce complexity, which leads to: faster and more accurate access policy modifications and fewer policy violations due to access inconsistencies

• Simplify compliance by producing automated reports and documentation