Assignment 3:
Common Control Identifier (CCI) Mapping for AeroTech X9

March 28, 2025

URGENT TASK: Supply Chain Compromise Response

AeroTech Industries has received notification of a suspected supply chain attack affecting a common Free Open Source Software (FOSS) JSON processing library (JSONparser 3.2.1) widely used in many software systems. This library may be present in the AeroTech X9 software stack or in components provided by sub-tier suppliers. As the cybersecurity team, you must immediately develop a response plan to:

1. Determine if your AeroTech X9 system is compromised
2. Develop a plan to identify compromised components
3. Develop a plan to determine if our suppliers software libraries are compromised. Two of our software suppliers will not provide details of their software library and claim it is Proprietery Information. We only have the binary. One supplier is claiming their software is Commercial-Of-The-Shelf (COTS) and they are not contractually obligated to provide the support for this task. We only have the binary. Three other suppliers will assist with scanning thei codebase but need a detailed process on what tools are required, steps they need to take, and description of what they will provide to us.
4. Establish processes to prevent similar compromises in the future including continuous monitoring.

Include this task response as a separate section in your deliverables. This will be weighted as 25% of your assignment grade.

Objective

Building on your attack tree analysis and security control selection from Assignment 3, this assignment requires you to map your selected controls to the appropriate Common Control Identifiers (CCIs) from NIST Special Publication 800-53 Revision 5. This mapping process will prepare you for developing a comprehensive System Security Plan (SSP) in Assignment 5.

Background

Your previous threat modeling, attack tree analysis, and security control selection have identified critical vulnerabilities and appropriate mitigations. Now, you must map these security controls to standardized Common Control Identifiers to ensure compliance with defense security requirements and facilitate the transition to a full System Security Plan.

Instructions

1. Supply Chain Compromise Response

- **Incident Response Plan**:
  - Create a comprehensive inventory of all instances where the JSONparser 3.2.1 library may be used in the AeroTech X9 system
  - Document a methodology to trace potentially compromised components through your supply chain
  - Establish criteria for determining whether a component is compromised
  - Design containment, eradication, and recovery procedures
- **Future Prevention Strategy**:
  - Design a continuous monitoring system for software dependencies
  - Create security requirements for suppliers that address software supply chain risks
  - Establish a verification and validation process for third-party components
  - Develop a Software Bill of Materials (SBOM) maintenance process that specifically addresses:
    - C and C++ dependencies
    - Python packages
    - Java libraries and frameworks
    - Ada components
  - Describe the incorporation of your SBOM and supply chain attack monitoring into the CI/CD development pipeline we use at Aerotech.
  - If there are no commercial tools to generate an SBOM for a given language provide a plan for determining the dependencies the supplier developed and delivered binary files and also for cases where we are delivered source code.
  - Integrate supply chain security controls with your existing security framework
  - Document any continuous monitoring processes and handling of Vulnerability Exploitability eXchange (VEX) files.

2. Review of Security Controls

- Briefly summarize the security controls you selected in Assignment 2
- Group related controls by control families as defined in NIST SP 800-53 Rev. 5
- Identify any gaps in control coverage based on this grouping

You may have already done this in assignment 2.

3. Common Control Identifier (CCI) Research

- Research and understand the CCI structure and its relationship to NIST SP 800-53 controls
- Identify the CCI List version you will be using (reference the current DoD CCI List)
- Understand how CCIs provide a more granular breakdown of security control requirements

4. CCI Mapping

For each security control you previously selected:

- Identify and list all corresponding Common Control Identifiers (CCIs)
- Document the CCI ID, title, and definition
- Determine the relevance of each CCI to your specific AeroTech X9 implementation.
- Determine if a given CCI is applicable. If not, document the rationale in your Security Control Tracability Matrix from Assignment 2.

5. CCI Implementation Specifications

For each identified CCI:

- Add to your SCTM :
  - Responsible orgnizations for implementation, e.g. Software Engineering, Systems Engineering, Supply Chain Management, etc.
  - Verification methods to ensure proper implementation
- Specify whether implementation is:
  - System-specific (implemented within the X9 system)
  - Common (inherited from a broader organization, e.g. Aerotech background checks employees or implements password rotation)
  - Hybrid (combination of system-specific and common)

Deliverables

1. **Supply Chain Compromise Response Plan** (5-10 pages)
   - Incident response procedures to identify compromised components
   - Software Bill of Materials (SBOM) development strategy for C, C++, Python, Java, and Ada codebases
   - Sub-tier supplier assessment methodology
   - Remediation steps for affected components
   - Future prevention strategy including:
     - Secure software development practices
     - Continuous monitoring of dependencies
     - Supplier security requirements
     - Verification and validation processes
2. **Control-to-CCI Mapping Matrix** (Updated security control traceability matrix from Assignment 2)
   - Expand your existing security control traceability matrix to include:
     - CCI identifiers mapped to each control
     - CCI definitions and relevance to AeroTech X9
     - Implementation responsibility (system-specific, common, hybrid)
     - CCI priority level (High, Medium, Low)
3. **CCI Implementation Plan** (As many pages as required.)
   - Detailed specifications for implementing each CCI
   - Technical configurations and procedural requirements
   - Dependencies between CCIs
   - Implementation timeline and milestones
4. **CCI Assessment Guide** (As many pages as required.)
   - Assessment procedures for each CCI
   - Compliance criteria and evaluation methods
   - Test cases and verification activities
   - Documentation requirements for proving compliance

Evaluation Criteria

- **Supply Chain Response**:
  - Comprehensive approach to identifying compromised components
  - Practical and implementable remediation strategies
  - Robust future prevention measures with specific processes
  - Integration with existing security controls and frameworks
- **Completeness**: Thorough mapping of all selected security controls to relevant CCIs
- **Accuracy**: Correct interpretation and application of CCIs to the AeroTech X9 system
- **Specificity**: Detailed implementation specifications tailored to the AeroTech X9 architecture
- **Practicality**: Realistic assessment procedures that could be implemented by security assessors
- **Integration**: Clear connections between CCIs and the eventual System Security Plan structure

Resources

- NIST Special Publication 800-53 Revision 5:
  `https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final`
- DoD Cloud Computing Security Requirements Guide (SRG)
- Common Control Identifiers (CCI) List:
  `https://public.cyber.mil/stigs/cci/`
- NIST Cybersecurity Framework
- Risk Management Framework (RMF) documentation
- NIST SP 800-161 Rev. 1: Supply Chain Risk Management Practices for Federal Information Systems
- CISA Secure Software Development Framework (SSDF)
- Executive Order 14028: Improving the Nation's Cybersecurity (Section 4 on enhancing software supply chain security)
- NTIA Software Bill of Materials (SBOM) guidance
- Previous AeroTech X9 documentation, attack tree analysis, and security control selection

Submission Guidelines

- All documents should be professionally formatted with proper citations
- Include a cover page with your team name, assignment title, and submission date
- Submit all deliverables as a single zip file named "TeamName_Assignment4.zip"
- Due date: [Insert appropriate date, typically 2-3 weeks after assignment distribution]

This assignment will directly feed into your final System Security Plan development in Assignment 5, so ensure your CCI mapping is thorough and well-documented.