Incremental AVCDL Adoption

Revision

Version 5
9/1/23 1:14 PM

Author

Charles Wilson

Abstract

This document describes an incremental approached to AVCDL adoption.

Audience

The audience of this document are the cybersecurity development lifecycle practice leads who will be guiding AVCDL adoption within their organization.

Note: This document presumes that the reader is already familiar with the AVCDL primary and secondary documents. As such no AVCDL document references will be provided as that would make this document unnecessarily long.

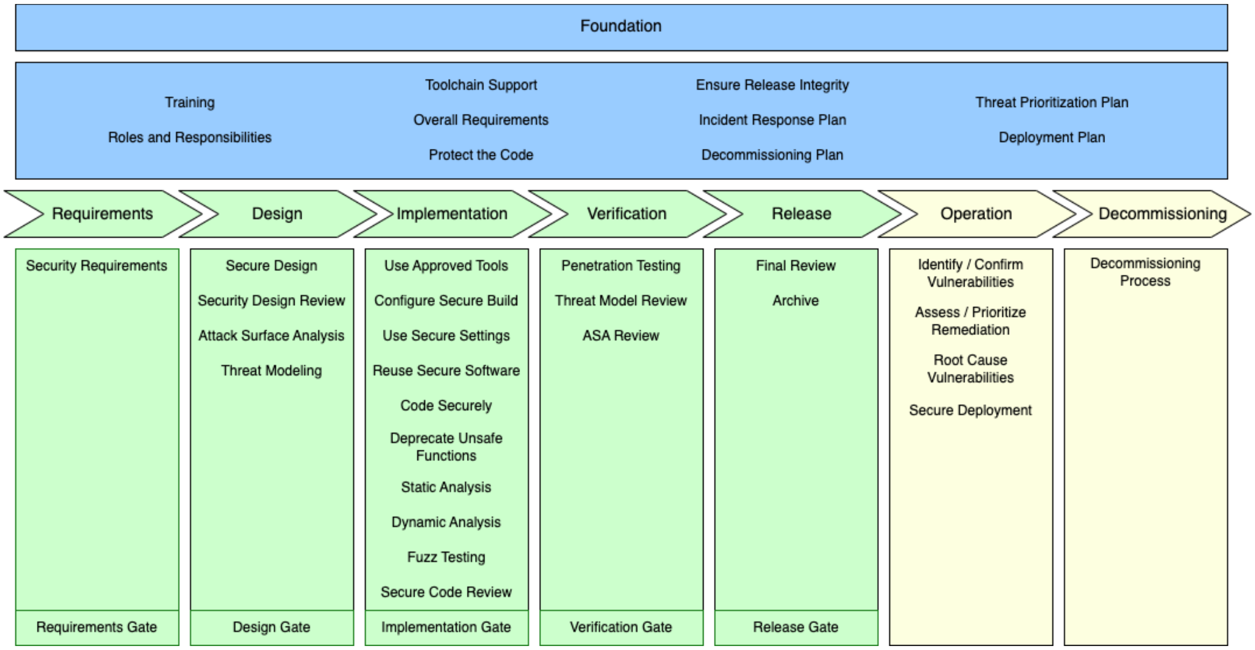
Note: This document is not subject to certification body review.

License

Overview

The AVCDL [1] is a comprehensive cybersecurity development lifecycle. Its scope presents a challenge to wholesale adoption. This document presents an incremental approach to facilitate adoption.

The following shows the AVCDL framework.



The framework can be broadly divided into three areas: foundational (blue), developmental (green), and operational (yellow).

We will treat these as separate tracks for the purposes of implementation within this document.

Adoption Stages

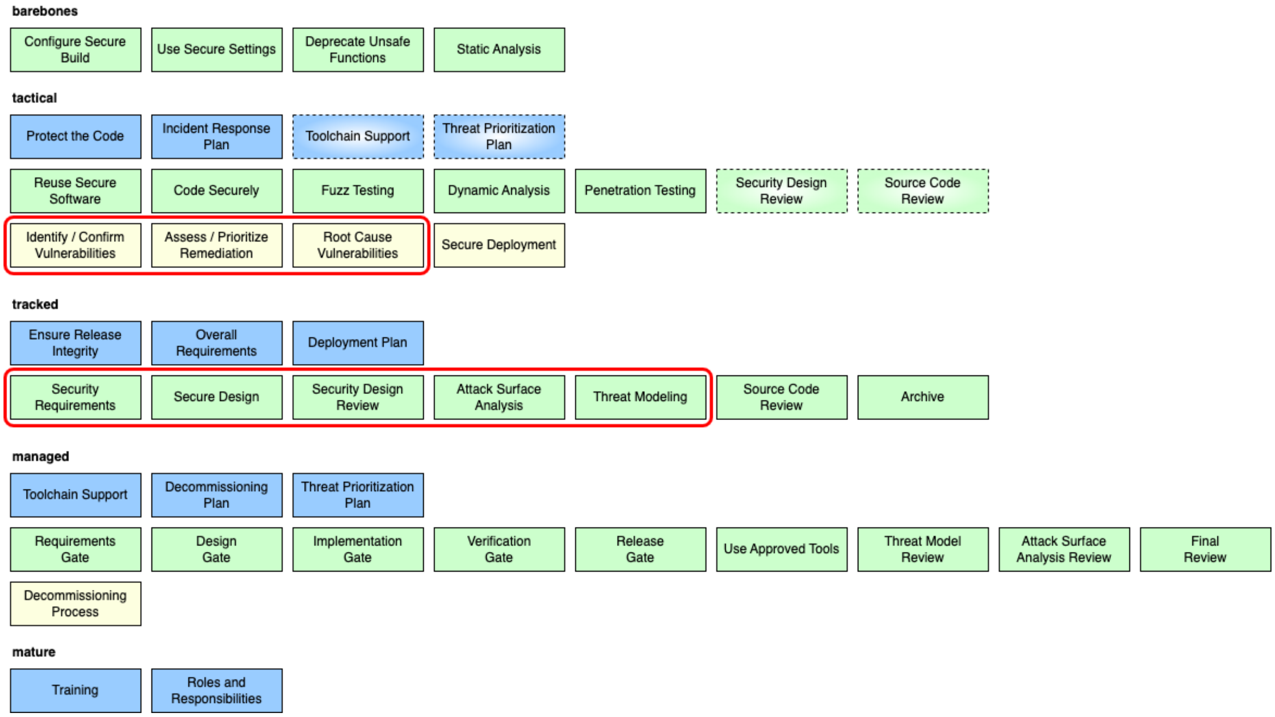
Five stages of adoption will be considered. These are:

- Barebones
- Tactical
- Tracked
- Managed
- Mature

Note: Activities within a stage presume the adoption of activities in the preceding stages.

Stages Visualized

The following shows an overview of the phased adoption.



barebones

Configure Secure Build | Use Secure Settings | Deprecate Unsafe Functions | Static Analysis

tactical

Protect the Code | Incident Response Plan | Toolchain Support | Threat Prioritization Plan

Reuse Secure Software | Code Securely | Fuzz Testing | Dynamic Analysis | Penetration Testing | Security Design Review | Source Code Review

Identify / Confirm Vulnerabilities | Assess / Prioritize Remediation | Root Cause Vulnerabilities | Secure Deployment

tracked

Ensure Release Integrity | Overall Requirements | Deployment Plan

Security Requirements | Secure Design | Security Design Review | Attack Surface Analysis | Threat Modeling | Source Code Review | Archive

managed

Toolchain Support | Decommissioning Plan | Threat Prioritization Plan

Requirements Gate | Design Gate | Implementation Gate | Verification Gate | Release Gate | Use Approved Tools | Threat Model Review | Attack Surface Analysis Review | Final Review

Decommissioning Process

mature

Training | Roles and Responsibilities

The various activities (phase requirements) have been split out of the framework diagram and reassembled in their various tracks and assigned to one of the stages.

Note: Items in dashed lines represent activities given a preliminary implementation in the stage in which they appear. These will then be refined and fully implemented in a later stage.

Note: Items enclosed in red represent activities directly supporting safety-related activities.

Adoption by Stage

The five stages are provided as a general mapping of complexity. The relationship of the various activities to the stages is one of complexity and organizational impact. The further along in the stages your organization progresses, the greater the interplay and interdependence there will be between various groups within the organization.

It is far easier to implement the earlier stages and make adjustment for your organization's tooling, and then undertake the later stages, than to attempt to implement the later stages and backfill the earlier.

The stages will now be addressed in order of ascending organizational complexity.

Note: Organizations may implement activities at any time. It is unlikely that later stage activities will be successfully implemented until all those from previous stages have been implemented.

Barebones

The barebones stage represents a level of cybersecurity support requiring the least from the development teams. These activities can be undertaken by cybersecurity SMEs in conjunction with devops. These represent the lowest hanging fruit. All are developmental in nature.

Foundational

none

Developmental

- Configure Secure Build
- Use Secure Settings
- Deprecate Unsafe Functions
- Static Analysis

Operational

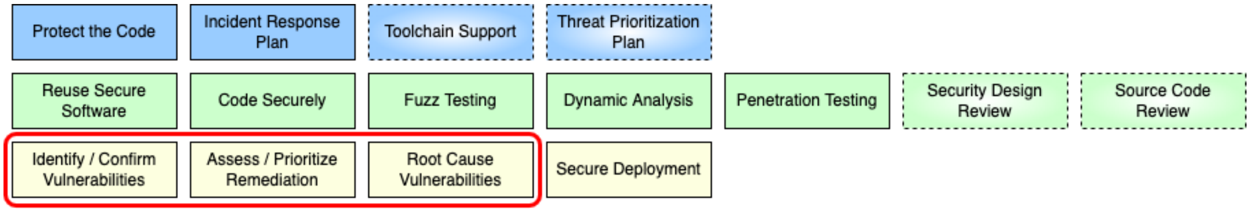
none

Tactical

The tactical stage represents a level of cybersecurity support focused on the secure and correct implementation of the system. All three areas of the AVCDL lifecycle are addressed. There is a much greater interaction with the development, devops, and operations teams.

There are several activities in this stage which are preliminary (dashed outlines). The intent is that these activities do not need to be implemented as formally as the others. Their inclusion is due to the support they provide to the other activities in this stage.

This stage also introduces activities which directly support safety activities (surrounding red outline).



Foundational

- Protect the Code
- Incident Response Plan
- Toolchain Support (preliminary)
- Threat Prioritization Plan (preliminary)

Developmental

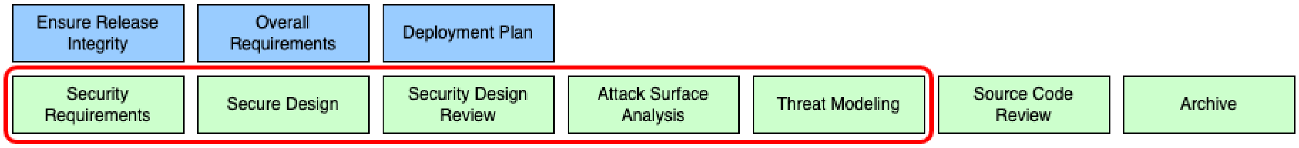
- Reuse Secure Software
- Code Securely
- Fuzz Testing
- Dynamic Analysis
- Penetration Testing
- Secure Design Review (preliminary)
- Source Code Review (preliminary)

Operational

- Identify / Confirm Vulnerabilities (safety relevant)
- Assess / Prioritize Remediation (safety relevant)
- Root Cause Vulnerabilities (safety relevant)
- Secure Deployment

Tracked

The tracked stage represents a level of cybersecurity support focused on the secure design of the system. In this stage, the activities of the requirements and design phase of the AVCDL are addressed. This requires far more coordination with systems engineering and development teams early in the creation of the system.



Foundational

- Ensure Release Integrity
- Overall Requirements
- Deployment Plan

Developmental

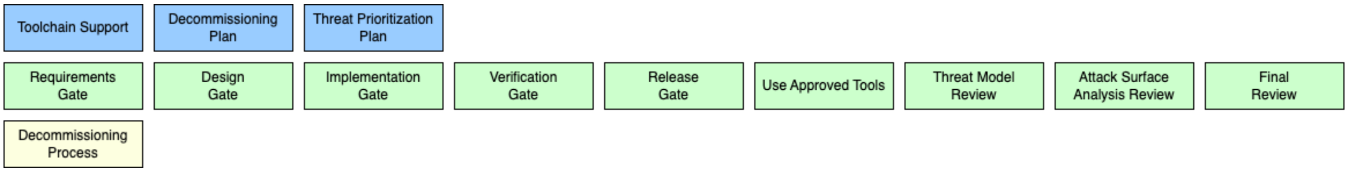
- Security Requirements (safety relevant)
- Secure Design (safety relevant)
- Security Design Review (safety relevant)
- Attack Surface Analysis (safety relevant)
- Threat Modeling (safety relevant)
- Source Code Review
- Archive

Operational

none

Managed

The managed stage represents a level of cybersecurity support focused on the management of the end-to-end lifecycle of the system. In this stage, the interaction between cybersecurity and project management is emphasized.



Foundational

- Toolchain Support
- Decommissioning Plan
- Threat Prioritization Plan

Developmental

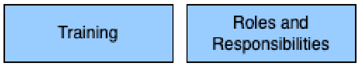
- Requirements Gate
- Design Gate
- Implementation Gate
- Verification Gate
- Release Gate
- Use Approved Tools
- Threat Modeling Review
- Attack Surface Analysis Review
- Final Review

Operational

- Decommissioning Process

Mature

The mature stage represents a level of cybersecurity support focused on the long-term support of the system. In this stage, attention is given to the training and ownership activities.



Training

Roles and Responsibilities

Foundational

- Training
- Roles and Responsibilities

Developmental

none

Operational

none

Relationship to Supply Chain Activities

As with any complex system, the supply chain must be given consideration. There are three cybersecurity related supplier activities used in conjunction with the AVCDL.

- Autonomous Vehicle Cybersecurity Manufacturer Disclosure Statement (AVCMDS)
- Supplier Self-reported Maturity Assessment (CMM)
- Cybersecurity Interface Agreement (CIA)

Since it is unlikely that any two organizations are at the same level of maturity with respect to their cybersecurity practices, undertaking these three activities is critical to the success of the project, regardless of the relative maturity of the two organizations. By undertaking these activities, alignment of cybersecurity activities and identification of gaps can be achieved.

References

1. **Autonomous Vehicle Cybersecurity Development Lifecycle** (AVCDL primary document)