Secure Settings Document

# Revision

Version 3

11/15/21 10:50 AM

# SME

Garth Scheidemantel

# Abstract

This document describes the process to identify, select and apply security settings to tools used to build the product software.

# Group / Owner

Security / Security Architect

# Motivation

This document is motivated by the need to ensure that the software is built with tools whose security settings are based on security best practices. This is necessary given the nature of safety-critical, cyber-physical systems, subject to certifications such as **ISO 21434** and **ISO 26262**.

# License

This work was created by **Motional** and is licensed under the **Creative Commons Attribution-Share Alike (CC4-SA)** License.

[**https://creativecommons.org/licenses/by/4.0/legalcode**](https://creativecommons.org/licenses/by/4.0/legalcode)

# Overview

The most secure application can be compromised because of poorly chosen tool settings. Such configuration errors may be in access control, database management, cryptographic material handling, or communication tools. Security settings must be chosen to ensure the appropriate level of security for the intended task.

The following diagram illustrates the process to be used:

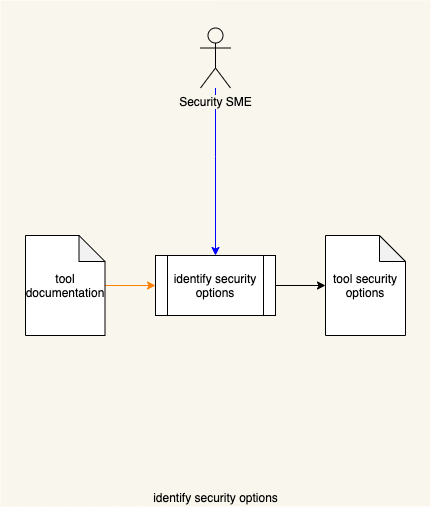
Diagram

Description automatically generated

# Process

## Identify Security Options

|  |  |
| --- | --- |
| **Inputs** | Tool documentation |
| **Outputs** | Tool security options |
| **Participants** | Security SME |



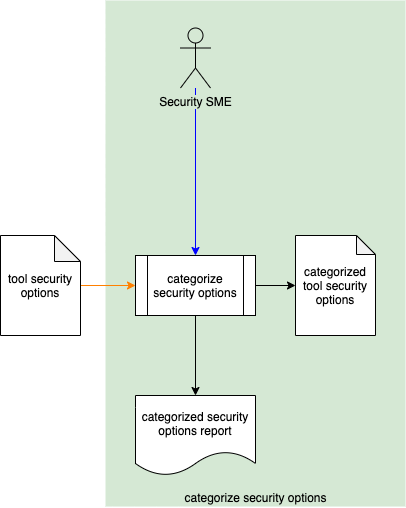
The Security SME reviews the **Tool Documentation** and identifies the security options. A **Tool Security Options** list is generated.

The **Tool Security Options** is a list of 3-tuples. The values of the tuples are as following:

* Option
* Description of the option
* Security relevance

## Categorize Security Options

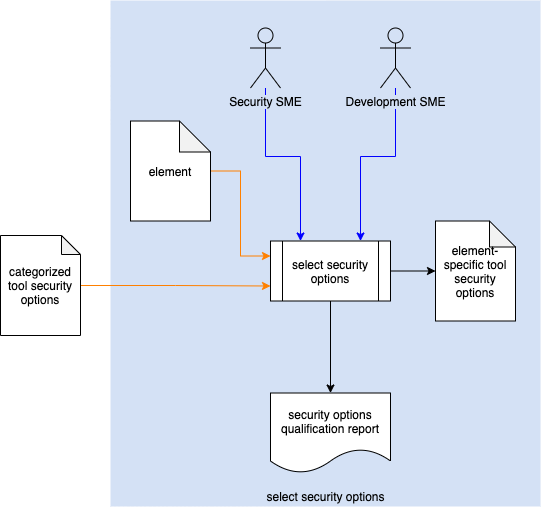
|  |  |
| --- | --- |
| **Inputs** | Tool security options |
| **Outputs** | Categorized tool security options |
| **Participants** | Security SME |



Using the **Tool Security Options**, the Security SME assigns each option a security priority category. A **Categorized Tool Security Options** list (organized by category) is generated. A **Categorized Security Options Report** is generated.

## Select Security Options

|  |  |
| --- | --- |
| **Inputs** | Element  Categorized tool security options |
| **Outputs** | Element-specific tool security options |
| **Participants** | Development SME  Security SME |

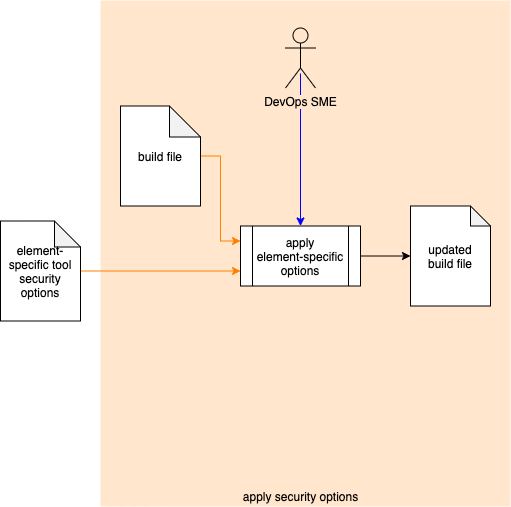


Using the **Categorized Tool Security Options** and **Element** under consideration, the Security SME and Development SME select applicable security options to be applied to the **Element**. An **Element-specific Tool Security Options** list is generated. A **Security Options Qualification Report** is generated.

**Note:** If a security option is not used, the justification for not selecting it must be documented.

## Apply Security Options

|  |  |
| --- | --- |
| **Inputs** | Element-specific tool security options  Build file |
| **Outputs** | Updated build file |
| **Participants** | DevOps SME |



Using the **Element-specific Tool Security Options** and **Build File**, the Dev Ops SME applies the selected settings to the appropriate section of the **Build File**. An **Updated Build File** is generated.

# References

1. **NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems**  
   <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf>
2. **Categorized Security Options Report** (AVCDL tertiary document)
3. **Security Options Qualification Report** (AVCDL tertiary document)