R155 Informed Authoring of Cybersecurity Test Plans

Call for Feedback Regarding the OpenXSAM Clause 9 Module

Clause 9 of the ISO/SAE 21434 regulation requires that OEMS, tier 1 and 2 manufacturers, and security analysts provide high-quality documentation during the concept phase of a products lifecycle. It is vital that the documentation includes which mitigation from UNECE R155 was selected, as it is necessary for validation and verification testing. Deliverables created during this period include item definitions, cybersecurity goals, and cybersecurity concepts. To produce an agreed upon machine readable standard format; itemis, Block Harbor Cybersecurity, and Keysight came together to create a draft designed for security consultants to test the cybersecurity of projects at the conceptual level. The following structure is the outcome of this collaboration, and we encourage community members to provide us feedback on this draft at secure-xsam@itemis.com.

Example

```
<openXSAM>
<ItemDefinition>
   <VerificationStatus>passed</VerificationStatus>
   <ValidationStatus>passed</ValidationStatus>
   <Functions>…</Functions>
 <Components>…</Components>
 <Data>…</Data>
   <Channels>…</Channels>
</ItemDefinition>
<CSConcept>
   <Risks>
      <Risk name="Confidentiality of the Update that comes over UDS" treatment="REDUCE">
           <CSGoal verificationStatus="passed" validationStatus="passed">
              <CSRequirement verificationStatus="passed" validationStatus="passed">
                   ...ReqIF content...
              </CSRequirement>
           </CSGoal>
      </Risk>
   </Risks>
</CSConcept>
</openXSAM>
```

Use Case

Security testers want to validate if the controls are working as intended. To accomplish this, they need to formulate a suitable test plan. This process is comprised of three steps: import, author, and reporting results.

Import

The item definition and cybersecurity concepts must be imported into the test plan authoring tool. The structure modeled above is designed to focus on machine readability, and further additions can be made to achieve that goal. Focusing on importability also increases the ease of collaboration on projects.

Author

With all the necessary information present within the test plan authoring tool; a security tester can now interact with the data to determine what types of tests to run. They can also modify the information in the test plan authoring tool of their choice. This allows a security tester to continue to modify and iterate on the cybersecurity test suite of the product.

Reporting Test Results

After the tests have been completed, the security tester can use the testing tool to report the test results to a security database of their choice. This step results in demonstrating the concerned and actual risks to the stakeholders; and the results can be used to inform changes within a product's cybersecurity feature set.

Structure

The structure is designed in a way to be self-explanatory and easy to implement, while retaining a high level of machine readability. This draft utilizes two parent elements to contain all the required information of clause 9. These two elements are the ItemDefinition and CSConcept.

ItemDefinition

The Item Definition element holds the security related architecture of the analyzed system (Clause 9.3), which is a precondition for performing the TARA (Clause 15). The item consists of functions, components, stored data, and channels. Additionally, the verification and validation status can be viewed as a property of the item definition element.

CSConcept

The CSConcept element contains the information regarding risks, their categorical name, the description of the attack, and validation/verification status of goals. It contains cybersecurity requirements, which can be formulated based on the Requirements Interchange Format (ReqIF) standard. A CSRequirement could also reference UNECE R155 mitigations that were designed to be covered.

Call for Suggestions

The structure detailed in this paper is currently being drafted. Community feedback will be taken into consideration and implemented in future iterations; and that process will continue until a final format is decided upon via community consensus.

You can provide your feedback at secure-xsam@itemis.com.