Tools & Techniques.

CCN presentation based on the T&T paper presented in the 8th ICCC, heavily influenced by comments received from GE BSI and NL NCSA n Led by UK and Spain

n Original aim - to define tools that will support all of the working methods described in the other work areas.

n Redirected to define workflows (allowing development of tools) AND

n To encourage use of tools by vendors.

Problem:

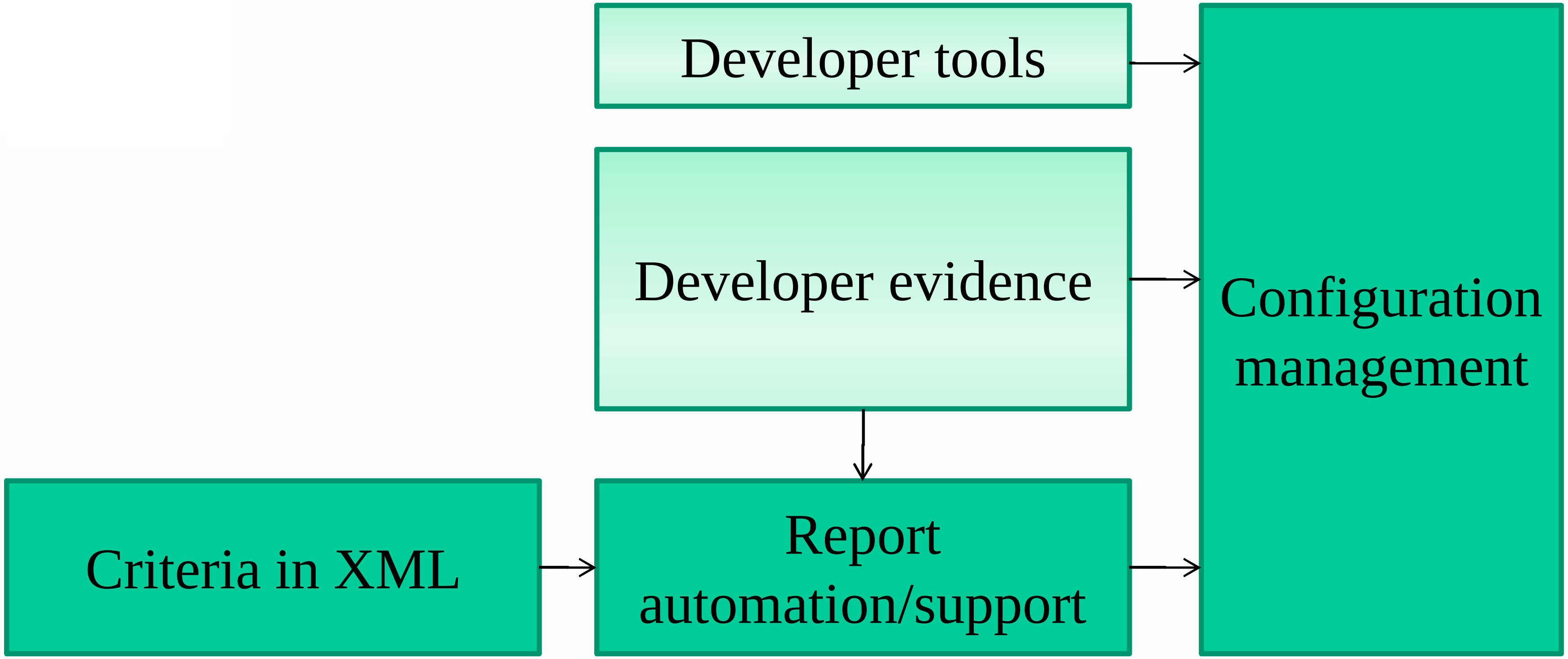
Vendors are using tools and techniques (mostly coding in an initial stage) to improve products and reduce vulnerabilities in the field.

Vendors usually do not need to apply such T&T to pass a CC evaluation.

Aim:

The CC certification, as a minimum, must mean that the product has been developed using state of the art secure development tools and techniques.

Evaluator Tools



Developer tools

Developer evidence

Criteria in XML

Report automation/support

Configuration management

The threat analysis and risk mitigation should drive the tools and techniques used in development.

Rather than being a nice surprise, not applying the state of the art in secure development should raise the need for justification in an evaluation.

The tools and techniques to be discussed here should not only focus on avoidance and/or detection of vulnerabilities in software, but also on mitigation of (exploitable) vulnerabilities.

Ignoring the early stages of the life cycle (design, requirement analysis, risk analysis, reviews, amongst others) is in general not a good idea.

Attack patterns should be used to characterize the required T&T;

1.are similar to “code smells” but then related to exploitable vulnerabilities,

2.consistent to the intended use of the TOE as formulated in (the assumptions in) the PP/ST,

3.consistent with the attack potential of an attacker,

4.and collected from sources such as industry best practices and/or developer threat analysis.

Developers are using tools to analyze and to verify properties and behavior .

Analysis:

1. static analysis
2. dynamic analysis
3. combined analysis.

Verification:

1.Mathematical reasoning
2.Formal methods
3.Model checking
4.Simulation
5.(Visual) Inspection/review
6.Testing
7.Design verification
8.Requirement traceability
9.Risk analysis(Environment:)
11. …

The evaluation is to gain from the use of the same developer tools.

From a number of required techniques

How do you handle this attack path?
How do you verify this countermeasure?

The evaluation will seek the tool support and will draw upon that.

Techniques and processes first,
Tool support second.

Questions welcomed.

Centro Criptológico Nacional.
www.oc.ccn.cni.es
organismo.certificacion@cni.es