SIEMENS
Ingenuity for life

Version 1.0
January 2020

Usecases for making XCCDF extensible wrt. “Applicability”

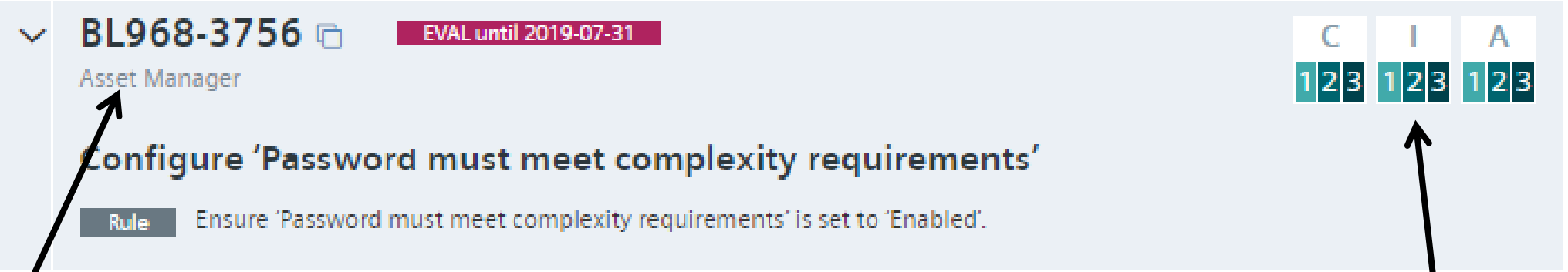
Dr. Bernd Grobauer, Siemens CT RDA CST

Need for Extensibility wrt. Applicability

SIEMENS
Ingenuity for life

- Baselines may have to be geared towards a certain constituency, e.g., personnel within a company (as is the case for Siemens), contractors (as is the case for DISA), etc.
- Processes and thus the required meta-data per rule necessarily vary from organization to organization

➔ **format needs extension points regarding applicability metadata**



Target audience / responsible person

```
applicability:
  (...)
  - system: com.siemens.cert.target_audience
    roles:
      - asset_manager
```

Applicability of rule with respect to Siemens-specific asset-classification

```
applicability:
  - system: com.siemens.cert.acp
    c: '123'
    i: '123'
    a: '123'
```

Siemens is not the only one ... witness the DISA STIGs

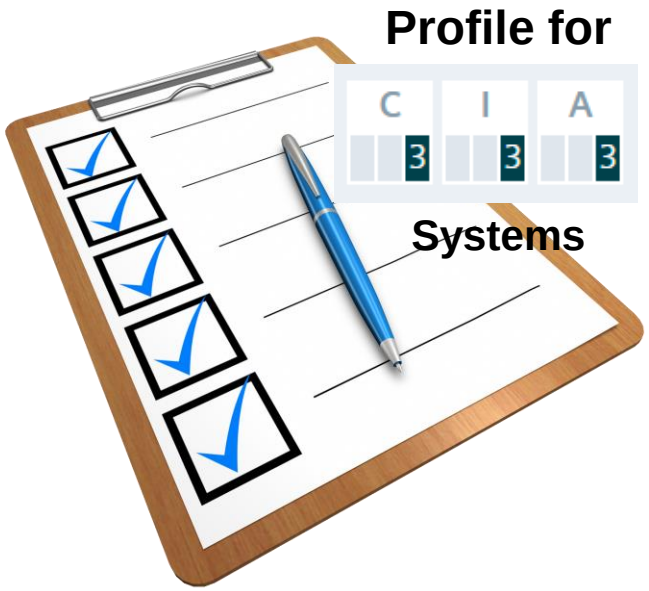
SIEMENS
Ingenuity for life

```
<description>
blah blah blah

&lt;/VulnDiscussion&gt;&lt;/VulnDiscussion&gt;
&lt;FalsePositives&gt;&lt;/FalsePositives&gt;
&lt;FalseNegatives&gt;&lt;/FalseNegatives&gt;
&lt;Documentable&gt;false&lt;/Documentable&gt;
&lt;Mitigations&gt;&lt;/Mitigations&gt;
&lt;SeverityOverrideGuidance&gt;
&lt;/SeverityOverrideGuidance&gt;
&lt;PotentialImpacts&gt;&lt;/PotentialImpacts&gt;
&lt;ThirdPartyTools&gt;&lt;/ThirdPartyTools&gt;
&lt;MitigationControl&gt;&lt;/MitigationControl&gt;
&lt;Responsibility&gt;&lt;/Responsibility&gt;
&lt;IAControls&gt;&lt;/IAControls&gt;

</description>
```

Profiles vs. Applicability: can't we just use profiles?

SIEMENS
Ingenuity for life

Indeed, one person's applicability metadata (per rule) is another person's profile.



Profile for Systems

C	I	A
3	3	3

From certain metadata on applicability, we can generate profiles and vice versa.

Rule 042

C	I	A
3	3	3

Rule *056*

C	I	A
2 3		

Rule *213*

C	I	A
1 2 3		

Rule *089*

C	I	A
3		

Rule *107*

C	I	A
2 3	2 3	2 3

Rule *023*

C	I	A
1 2 3	1 2 3	1 2 3

. . .

Still organizations may want to maintain such information within custom applicability structures and then automatically generate profiles in order to leverage standard SCAP mechanisms...

and not all applicability information is necessarily profile related.

Other uses for an applicability extension point

SIEMENS
Ingenuity for life

- Allows us to add data used during authoring and review directly into the rule, keeping everything in one place
  - Custom export generates, e.g., XLSX spread sheet with authoring/review information which may be removed/pruned once the baseline has been completed
  - New demand for additional meta information can be met very fast
    - tooling which does not require the new meta data just ignores it

- Combination of machine-readable meta-data about possible problems associated with implementation of a rule with human-readable information informing about the likely problem
  - used by tooling for generating artefacts for automated implementation
  - used by generation of human-readable export about “dangerous” rules

Pro‘s and cons of making XCCDF extensible for applicability structures

SIEMENS
Ingenuity for life

- **Pros**:
  - XCCDF would start to live up to its name (currently, it must be seen as „SXCCDF“ („somewhat extensible ...“)
  - We can move away from situations where organizations need to shoehorn information into XCCDF using rather creative techniques.
  - XCCDF can be used „as intended“ for checklists tailored for certain constituencies
  - Allowing a mechanism to extend XCCDF in a defined rather than round-about way may lead to more exchange/reuse (even standardization) of useful meta information
- **Cons**:
  - Not every tool will understand every extension ... but that has not kept us from allowing extensions for fixes and checks.


```
<description>
blah blah blah

&lt;/VulnDiscussion&gt;&lt;/VulnDiscussion&gt;
&lt;FalsePositives&gt;&lt;/FalsePositives&gt;
&lt;FalseNegatives&gt;&lt;/FalseNegatives&gt;
&lt;Documentable&gt;false&lt;/Documentable&gt;
&lt;Mitigations&gt;&lt;/Mitigations&gt;
&lt;SeverityOverrideGuidance&gt;
&lt;/SeverityOverrideGuidance&gt;
&lt;PotentialImpacts&gt;&lt;/PotentialImpacts&gt;
&lt;ThirdPartyTools&gt;&lt;/ThirdPartyTools&gt;
&lt;MitigationControl&gt;&lt;/MitigationControl&gt;
&lt;Responsibility&gt;&lt;/Responsibility&gt;
&lt;IAControls&gt;&lt;/IAControls&gt;

</description>
```

My strongest argument that XCCDF needs more extensibility...

Users will always have requirements for data not forseen in the XCCDF spec and WILL add the data in some way.
The only choice we have is whether we create a standardized mechanism for this or not (and accept this in consequence)