**Основной набор объектов:**  
  
Основная логика работы формата OVAL включает в себя следующие ключевые компоненты:

1. Definitions: описывают конкретные уязвимости, настройки или аспекты безопасности системы, которые подлежат проверке.
2. Metadata: предоставляют дополнительную информацию о каждом определении, такую как описание, ссылки на источники и другие сведения.
3. Criteria: определяют логические условия, которые используются для определения того, удовлетворяет ли система Definitions.
4. Tests: определяют, какие конкретные аспекты системы следует проверить и как их проверять.

В общем, логика работы OVAL заключается в том, чтобы определить, какие аспекты системы следует проверить, как их проверять и как интерпретировать результаты. Это позволяет автоматизировать процесс проверки систем на наличие уязвимостей и несоответствий конфигурации.

**Критерии:**

При просмотре кажется, что все критерии имеют свою роль, особенно если учесть, что они проверяют разные аспекты системы (версии ОС, версии Ruby и т. д.). Однако есть несколько моментов, которые можно было бы исключить:

1. Первый подкритерий (Red Hat Enterprise Linux must be installed) может показаться избыточным, так как дальнейшие проверки уже предполагают, что система базируется на Red Hat.
2. Так же, дублирование некоторых проверок, например, проверка на то, что компонент подписан ключом "Red Hat redhatrelease2". Если этот ключ является стандартом для всех компонентов, возможно, его стоит проверить один раз, а не для каждого компонента отдельно.

**Краткое описание:**

Формат OVAL содержит множество деталей, которые могут быть избыточными для некоторых пользователей. Для упрощения формата, можно рассмотреть следующие шаги:

1. Объединение Информации: вместо разделения информации на разные блоки (как <description>, <advisory>, <metadata>), можно объединить всю ключевую информацию в одном блоке.
2. Упрощение Критериев: вместо сложной структуры критериев с множественными операторами, можно использовать более простую структуру, где каждый критерий представлен в виде списка условий.
3. Сокращение Избыточных Данных: некоторые данные, такие как rights, severity или детали о cve, могут быть представлены в сокращенном виде или исключены, если они не являются критически важными.

Пример:  
  
definitions>

<definition>

<info>

<description>The cloud-init packages provide a set of init scripts for cloud instances. Cloud instances need special scripts to run during initialization to retrieve and install SSH keys, and to let the user run various scripts.

Users of cloud-init are advised to upgrade to these updated packages.</description>

<links>

<cve href="https://access.redhat.com/security/cve/CVE-2019-0816" cvss3="5.4/CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N"/>

<bugzilla href="https://bugzilla.redhat.com/1680165"/>

</links>

</info>

<affected\_products>

<product>cpe:/a:redhat:enterprise\_linux:8</product>

<product>cpe:/a:redhat:enterprise\_linux:8::appstream</product>

<product>cpe:/a:redhat:enterprise\_linux:8::crb</product>

<product>cpe:/a:redhat:enterprise\_linux:8::highavailability</product>

<product>cpe:/a:redhat:enterprise\_linux:8::nfv</product>

<product>cpe:/a:redhat:enterprise\_linux:8::realtime</product>

<product>cpe:/a:redhat:enterprise\_linux:8::resilientstorage</product>

<product>cpe:/a:redhat:enterprise\_linux:8::sap</product>

<product>cpe:/a:redhat:enterprise\_linux:8::sap\_hana</product>

<product>cpe:/a:redhat:enterprise\_linux:8::supplementary</product>

<product>cpe:/o:redhat:enterprise\_linux:8</product>

<product>cpe:/o:redhat:enterprise\_linux:8::baseos</product>

</affected\_products>

<criteria\_list>

<criteria>(cloud-init is earlier than 0:18.5-1.el8.4 (Test ID: oval:com.redhat.rhba:tst:20191992001) AND cloud-init is signed with Red Hat redhatrelease2 key (Test ID: oval:com.redhat.rhba:tst:20191992002) AND (Red Hat Enterprise Linux 8 is installed (Test ID: oval:com.redhat.rhba:tst:20191992003) OR Red Hat CoreOS 4 is installed (Test ID: oval:com.redhat.rhba:tst:20191992004)))</criteria>

</criteria\_list>

</definition>

Такой формат сосредотачивает внимание на самой важной информации, исключая избыточные детали.