# SFR Database Proof-of-Concept Orientation Document

**This document provides a text and visual overview of the basic features of the Security Functional Requirements Database (SFRDB) Proof-of-Concept. The format of this document provides Comments explaining screenshots of the SFRDB, which are meant to aid the user in operating the tool. Limitations, considerations, and some statistics are covered in the README.md file located here: sfr-catalog/README.md at main · commoncriteria/sfr-catalog (github.com)**

**<u>Feature Outline and Guide</u>**:

- **General Search Notes:** (Read this first!)

  o You may search for any combination of Threat, Objective, or SFR. However, the search results are based on which Threats, Objectives, and SFRs have been related to each other in a document.

  o The PP filter card will not appear until a selection of either Threat, Objective, or SFR has been made.

  o Threats and Assumptions are in the same filter card, and so are Objectives and Environmental Objectives. These are not related to any SFRs.

  o Multiple PPs can be selected by ctrl-clicking items in the dropdown.

  o The CC Part 2 [2022] SFR information is only available in text format, and appears as an option when selecting an SFR family that appears in the CC Part 2 [2022].

- **Threat/Objective Search**
- **SFR Search**
- **Filter Numbers**
- **View TDs**
- **Copy to Clipboard**
- **Switch between Text and XML**

**Considerations:** (As of Jan 2024)

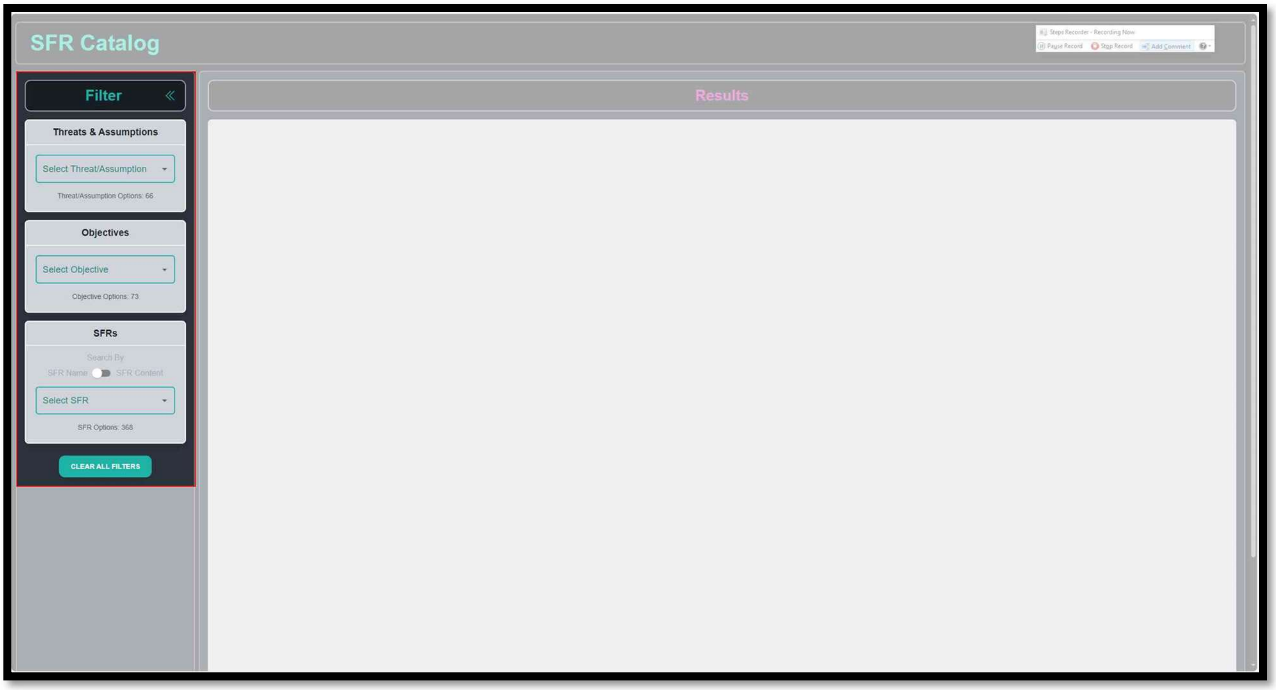
• This tool is a proof-of-concept, and there are currently no plans to develop it further:

• This tool currently refers to a JSON document that has ingested the following documents:

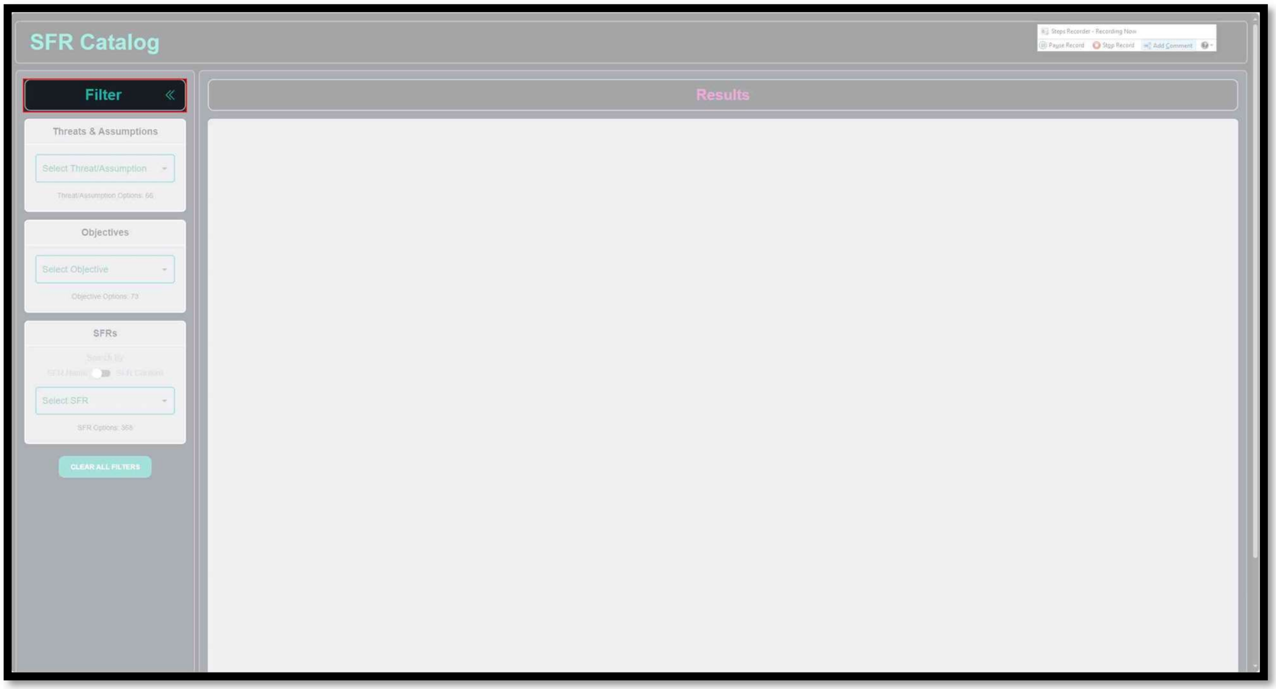
- PPs:
    - Application 1.4
    - MDF 3.3
    - GPCP 1.0
    - GPOS 4.3
    - Virtualization 1.1
- Mods:
    - Bluetooth 1.0
    - MACSEC 1.0
    - SBC 1.0
    - Virtualization (Client) 2.4
    - Virtualization (Server 1.1
    - VPN Client 2.4
    - VPN Gateway 1.3
    - WIDS 1.0
    - WLAN Access 1.0
    - WLAN Client 1.0
- FPs:
    - SSH 1.0
    - TLS 1.0

**Please provide any feedback you have to the issues board associated with this repo. Your feedback will help this tool or any that comes after it and is greatly appreciated!**

**Comment: "This is the 'Filter Panel' that contains 'Filter Cards' that allow a user to select a Threat, Assumption, Objective, Environmental Objective, SFR, or PP (once other selections have been made)."**



## Comment: "The Filter Panel toggles between open and closed with a click of the arrow shown here."

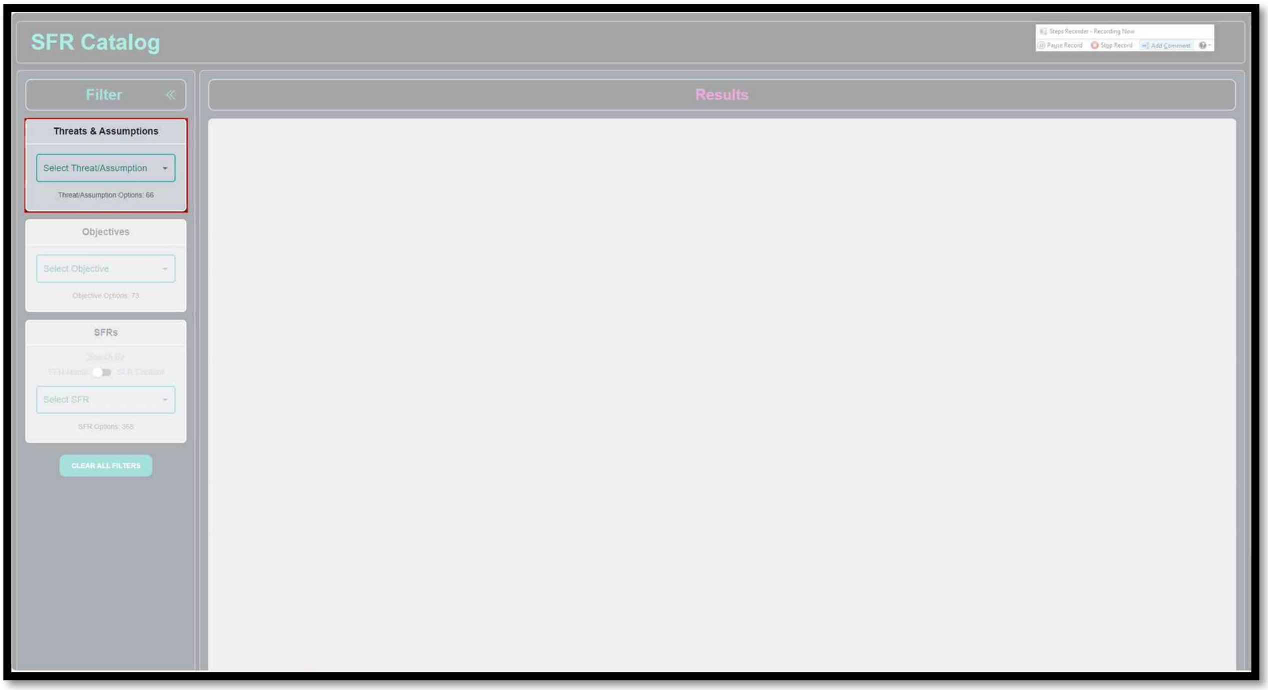


Threat/Assumption Options: 66

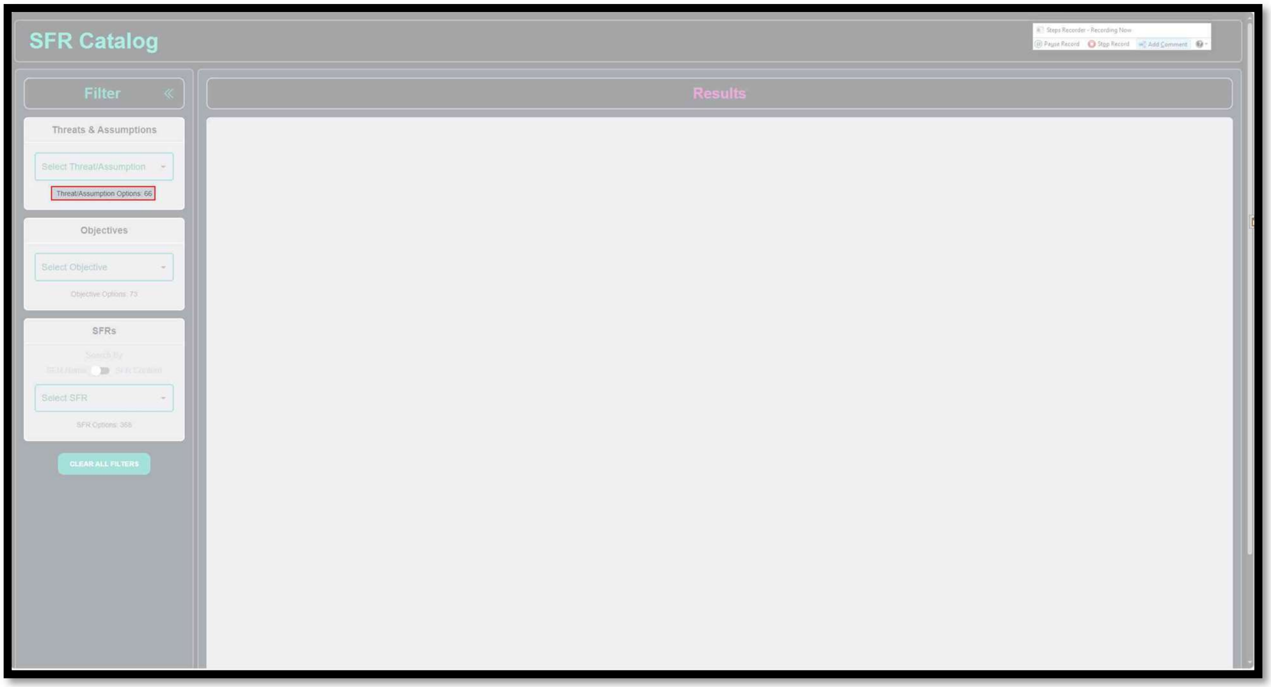
Objective Options: 73

SFR Options: 368

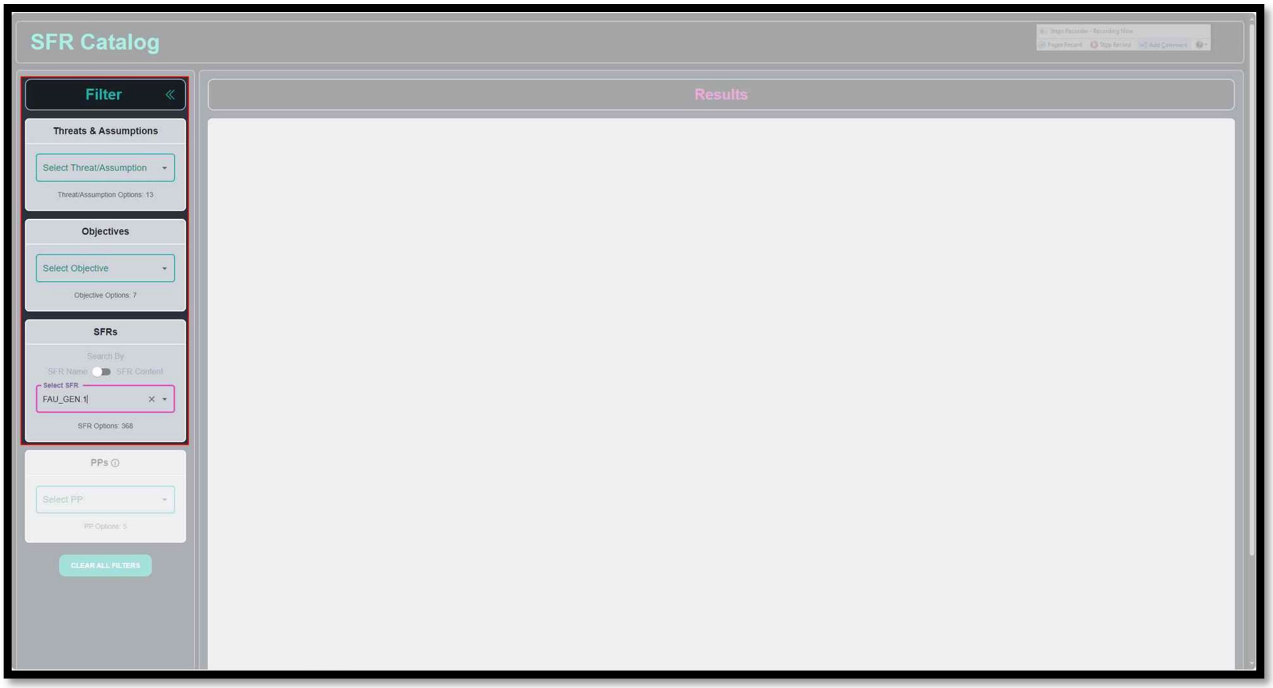
**Comment: "This is a 'Filter Card' That allows a user to select from a Threat, Assumption, Objective, Environmental Objective, SFR, or PP (after any other selection has been made). Threats, Assumptions, Security Objectives, and SFRs come from 17 released PPs and the CC 2022 Part 2. Only those PPs that have had an XML release are represented."**



**Comment: "These are the 'Filter Numbers,' and they change as selections are made to show a user how many items are related to a particular selection or set of selections. For example, no selections have been made, so the Filter Number shows all available Threats and Assumptions, of which there are 66. As will be shown in the following steps, making selections will filter this list and the number shown will decrease."**



**Comment: "As shown, a selection has been made in the 'SFRs' Filter Card, and then Filter Numbers for both the Threats & Assumptions and Objectives Filter Cards have decreased. The numbers shown for the Threats & Assumptions and Objectives Filter Numbers represent the filtered list of items that are related to the SFR selection."**



SFR Catalog

Filter

Results

Threats & Assumptions

Select Threat/Assumption

Threat/Assumption Options: 13

Objectives

Select Objective

Objective Options: 7

SFRs

Search By

SFR Name / SFR Content

Select SFR: FAU_GEN.1

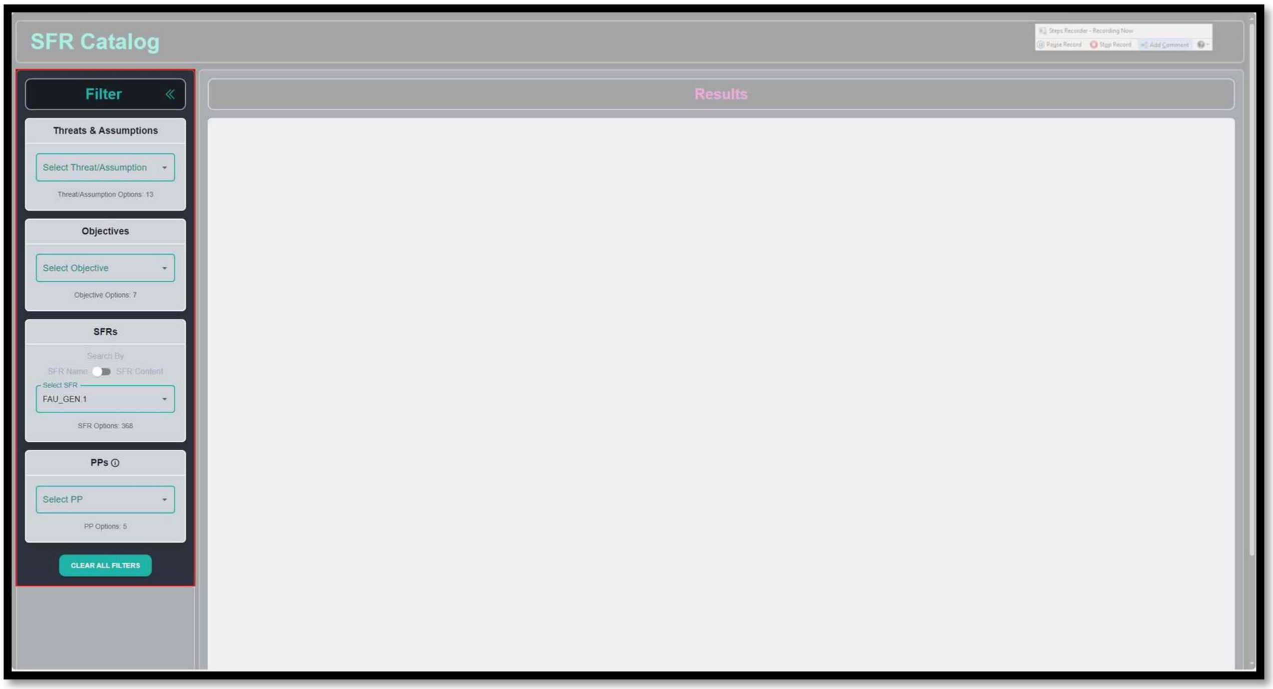
SFR Options: 368

PPs

Select PP

PP Options: 5

## Comment: "Also, now that a selection has been made, the PP Filter Card is available. The PP Filter Card also has Filter Numbers which show how many PPs contain the Threats, Assumptions, Objectives, or SFRs selected."



Threat/Assumption Options: 13

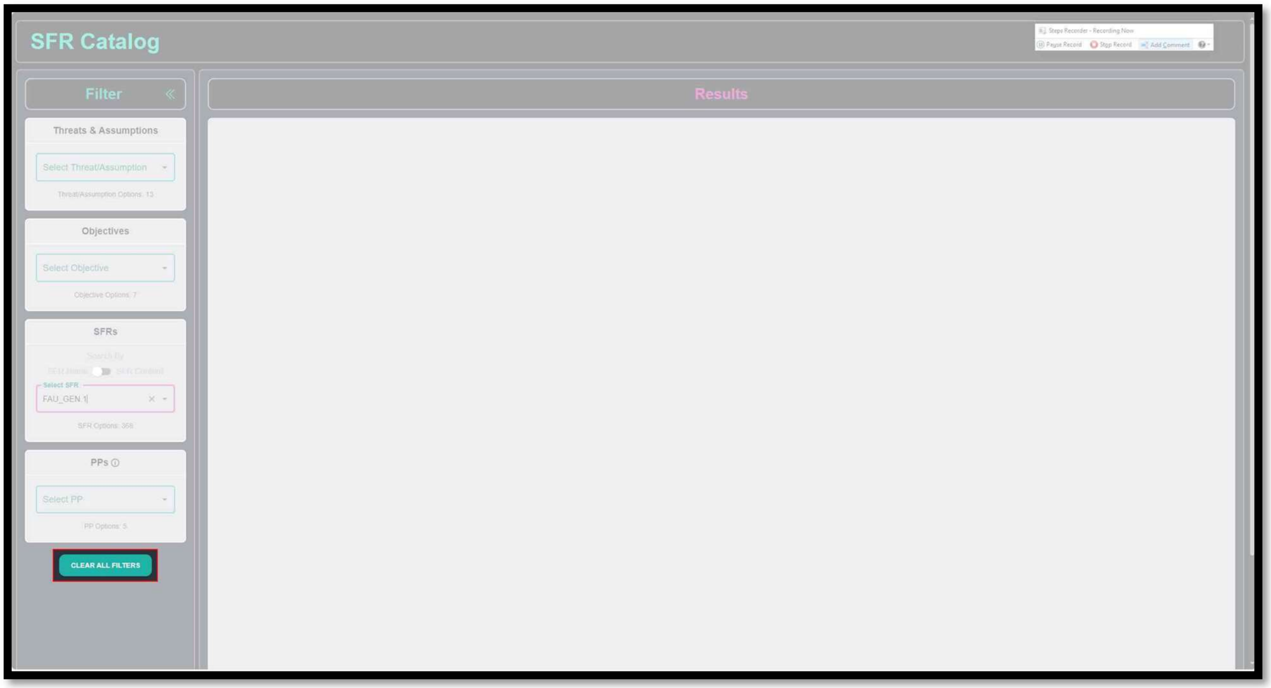
Objective Options: 7

Select SFR: FAU_GEN.1

SFR Options: 368

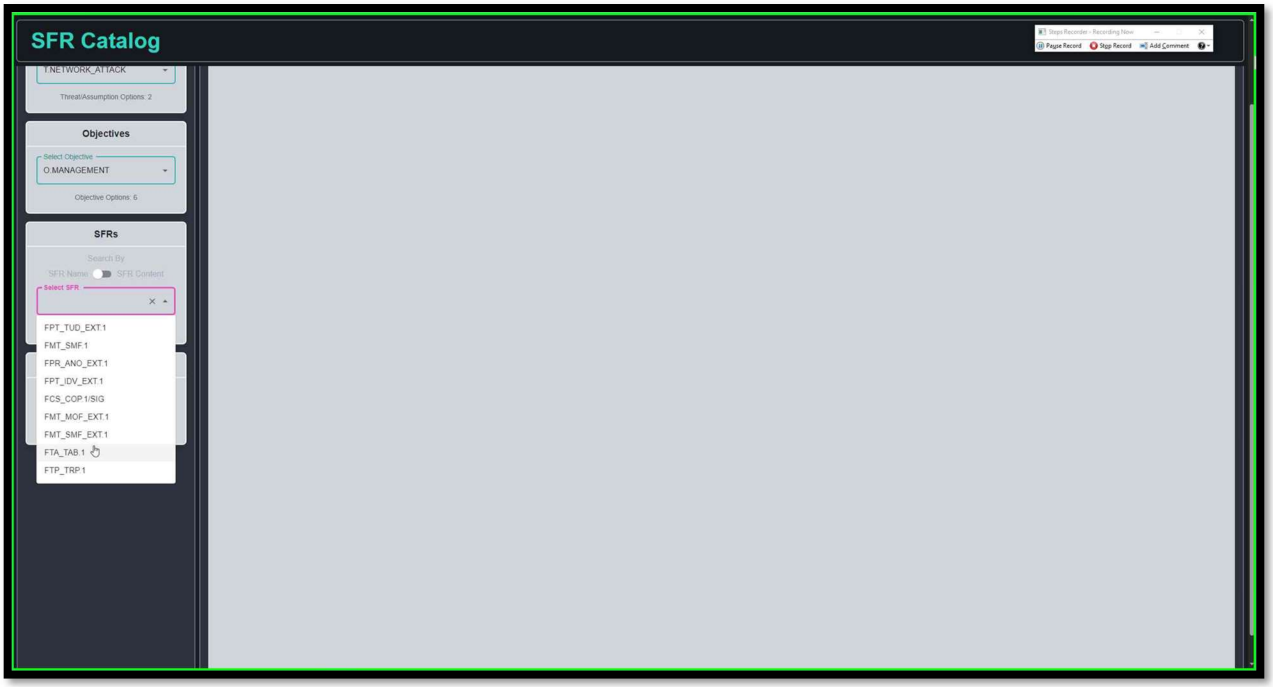
PP Options: 5

## Comment: "This button allows a user to clear all filters and reset the application to unfiltered lists."



Select SFR: FAU_GEN.1

**Comment: “In the following six screenshots, the user will select an SFR, then select two PPs in which to compare the implementation of the chosen SFR. Note, the Content Pane will display on the implementation of the chosen SFR from the selected PPs. Different Threats, Objectives, or SFRs cannot be compared against one another, only the implementations of a single Threat, Objective, or SFR between PPs may be compared.”**

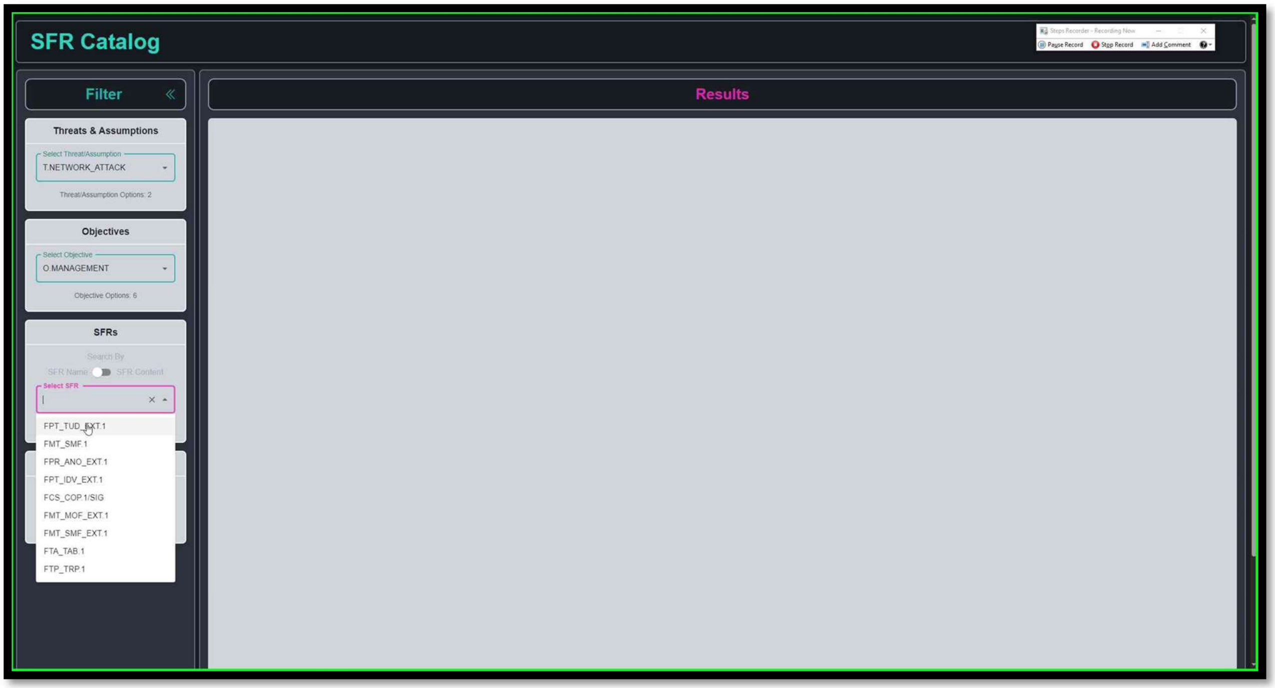


T.NETWORK_ATTACK

Threat/Assumption Options: 2

Select Objective: O.MANAGEMENT

Objective Options: 6



SFR Catalog

Filter

Results

Threats & Assumptions

Select Threat/Assumption: T.NETWORK_ATTACK

Threat/Assumption Options: 2

Objectives

Select Objective: O.MANAGEMENT

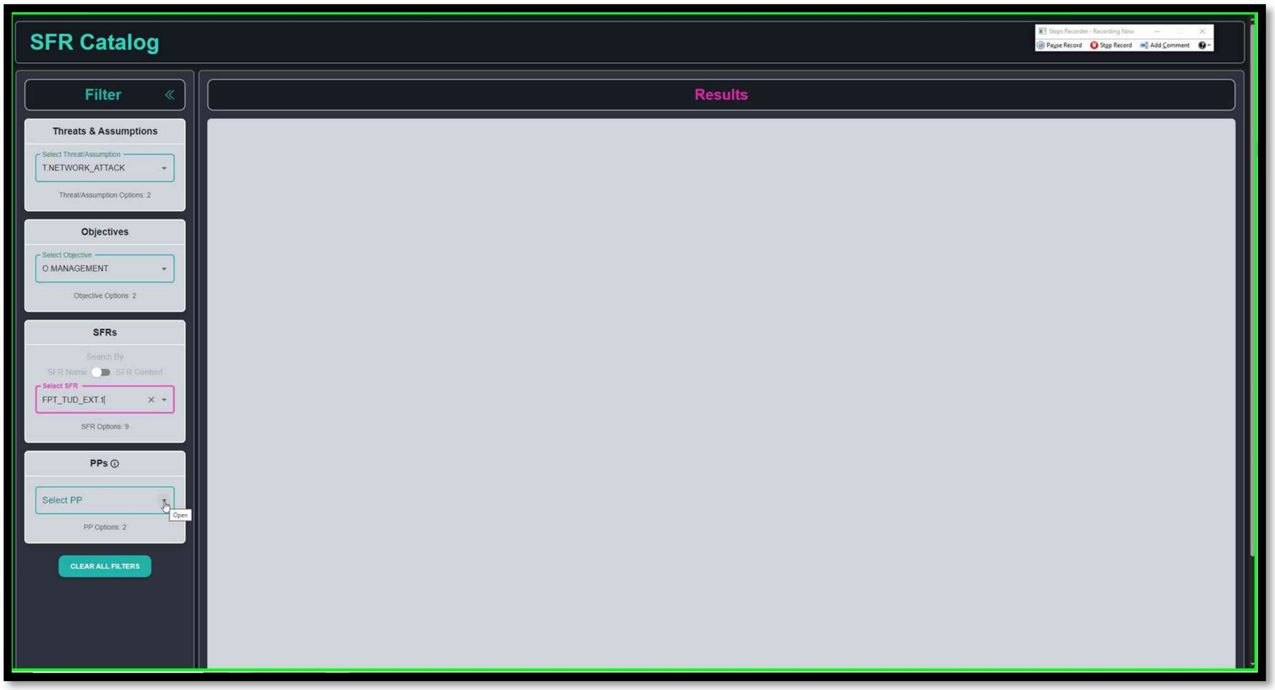
Objective Options: 6

SFRs

Search By

SFR Name / SFR Content

Select SFR



SFR Catalog

Filter

Results

Threats & Assumptions

Select Threat/Assumption: T.NETWORK_ATTACK

Threat/Assumption Options: 2

Objectives

Select Objective: O.MANAGEMENT

Objective Options: 2

SFRs

Search By

SFR Name / SFR Content

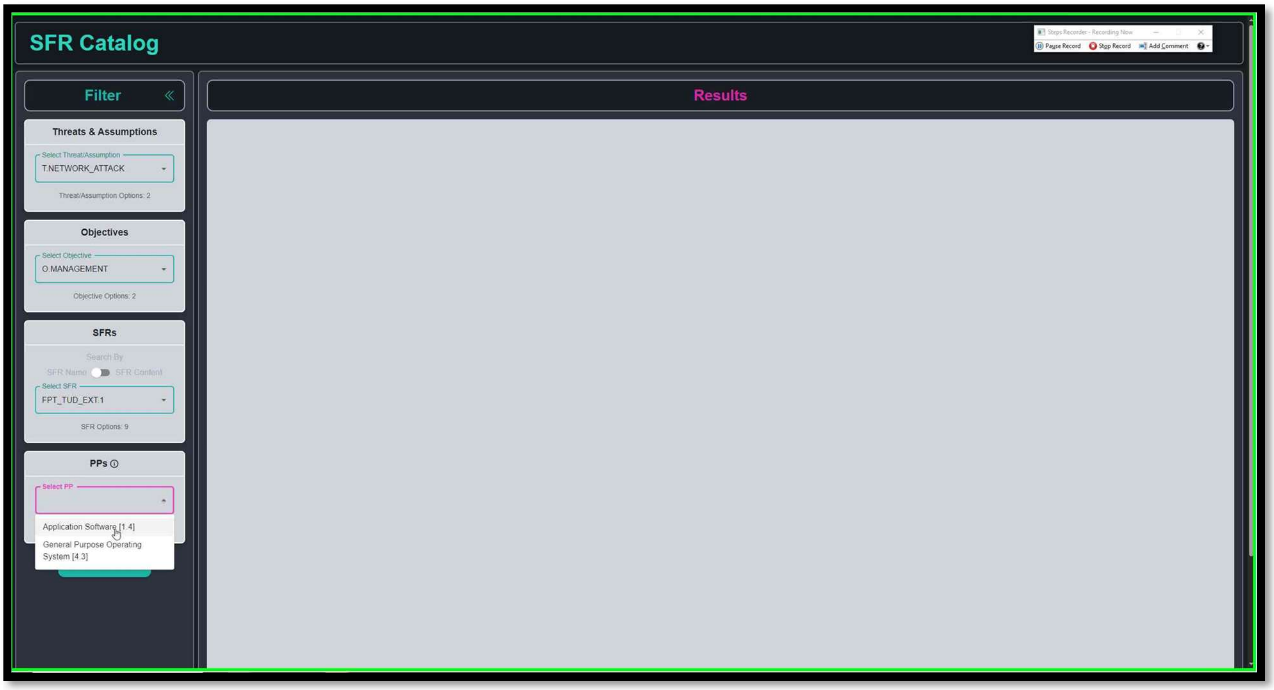
Select SFR: FPT_TUD_EXT.1

SFR Options: 9

PPs

Select PP

PP Options: 2



Select Threat/Assumption: T.NETWORK_ATTACK

Threat/Assumption Options: 2

Select Objective: O.MANAGEMENT

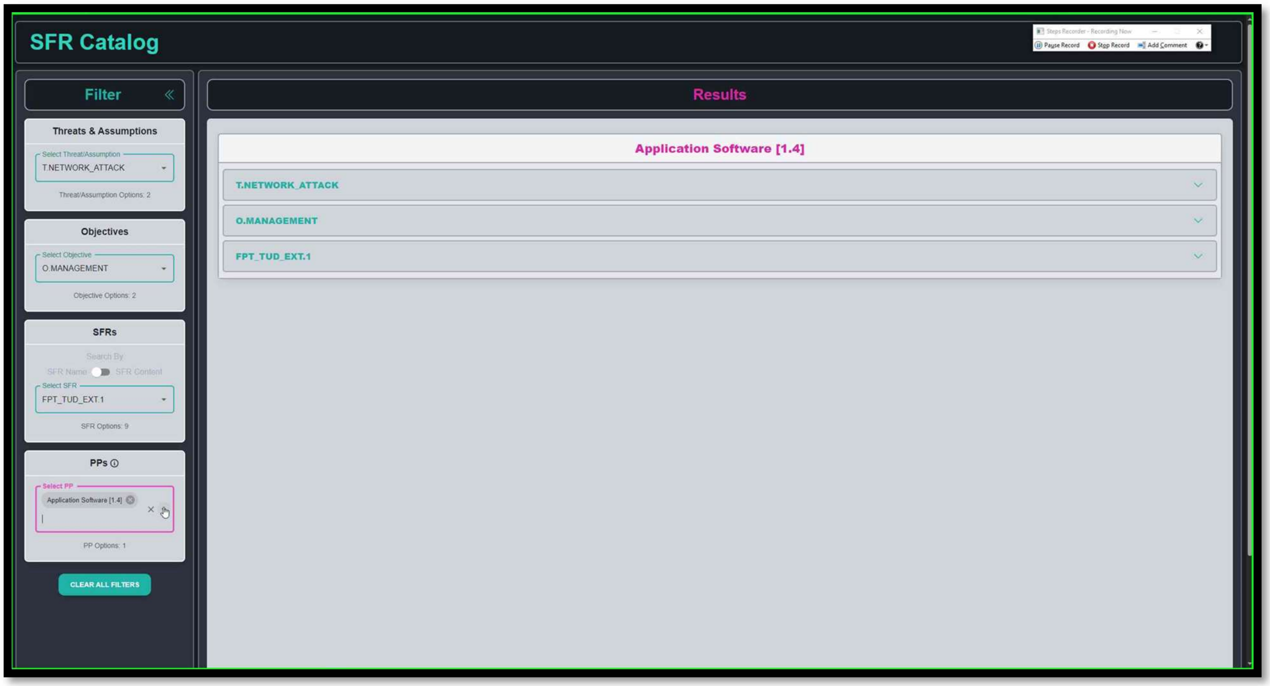
Objective Options: 2

Select SFR: FPT_TUD_EXT.1

SFR Options: 9

Select PP

- Application Software [1.4]
- General Purpose Operating System [4.3]



Select Threat/Assumption: T.NETWORK_ATTACK

Threat/Assumption Options: 2

Select Objective: O.MANAGEMENT

Objective Options: 2

Select SFR: FPT_TUD_EXT.1

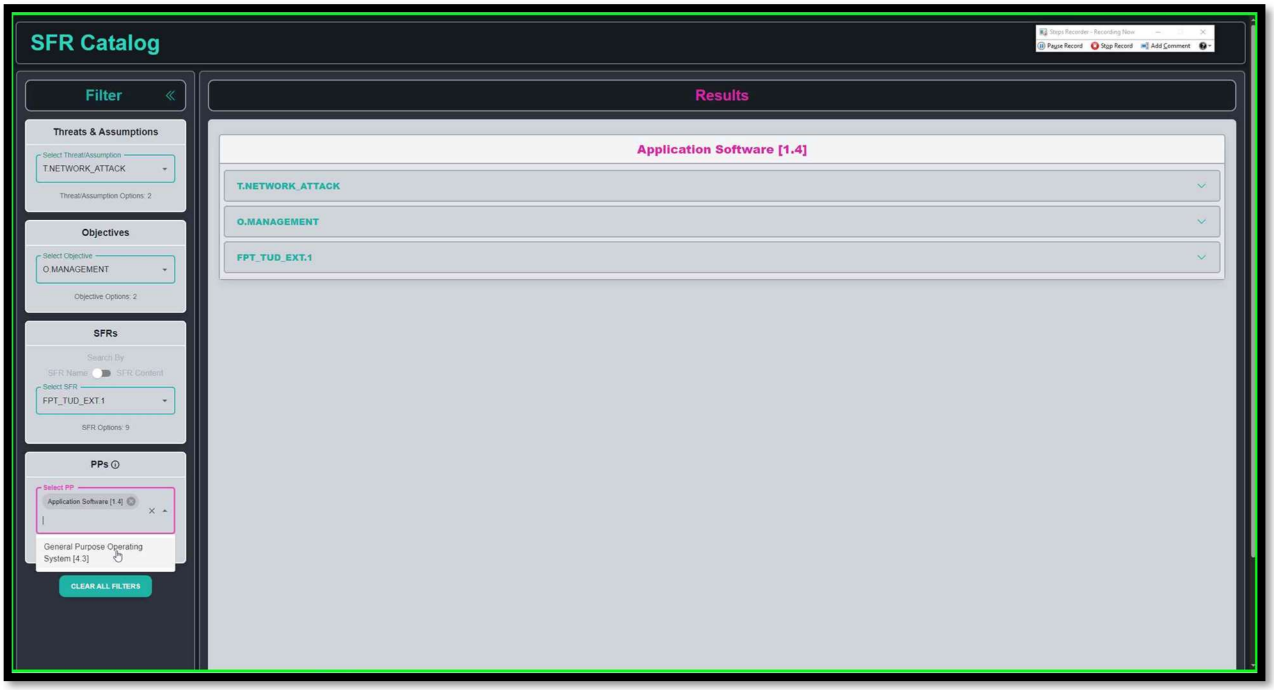
SFR Options: 9

Select PP: Application Software [1.4]

PP Options: 1

Application Software [1.4]

- T.NETWORK_ATTACK
- O.MANAGEMENT
- FPT_TUD_EXT.1



SFR Catalog

Filter

Threats & Assumptions

Select Threat/Assumption: T.NETWORK_ATTACK

Threat/Assumption Options: 2

Objectives

Select Objective: O.MANAGEMENT

Objective Options: 2

SFRs

Search By

SFR Name / SFR Content

Select SFR: FPT_TUD_EXT.1

SFR Options: 9

PPs

Select PP: Application Software [1.4]

General Purpose Operating System [4.3]

Results

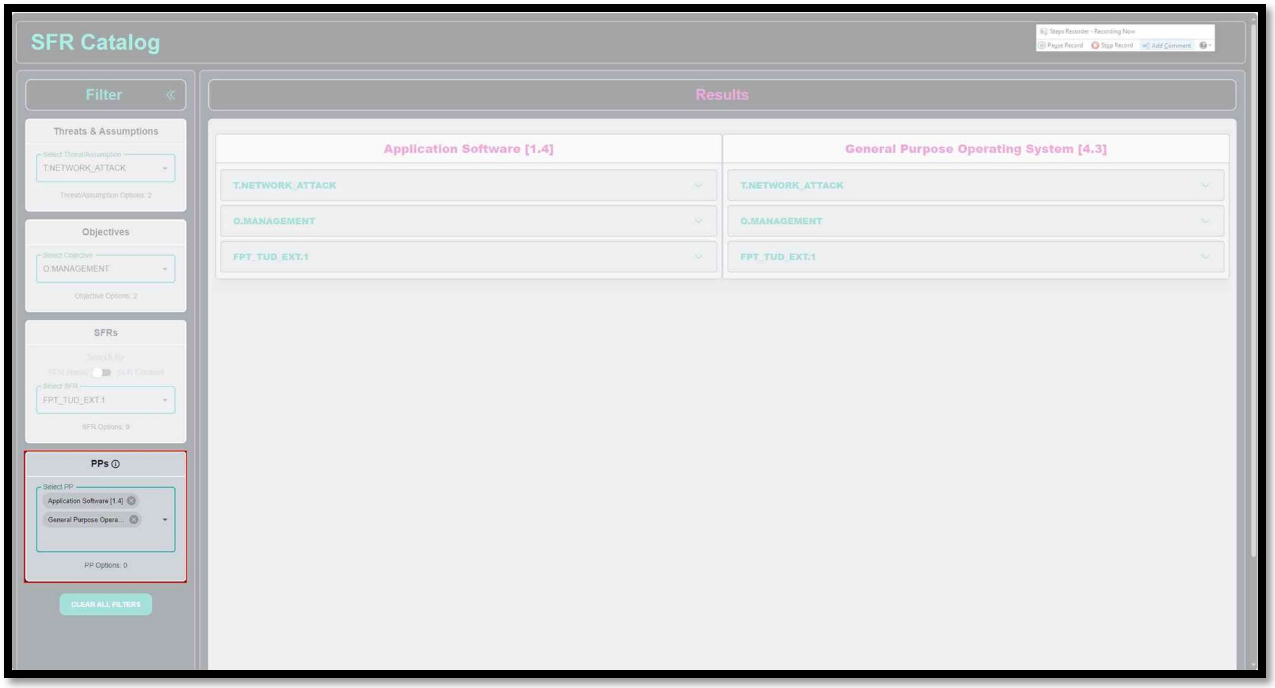
Application Software [1.4]

T.NETWORK_ATTACK

O.MANAGEMENT

FPT_TUD_EXT.1

## Comment: "Here, two PPs have been selected for comparison."



Threats & Assumptions

Select Threat/Assumption: T.NETWORK_ATTACK

Threat/Assumption Options: 2

Objectives

Select Objective: O.MANAGEMENT

Objective Options: 2

SFRs

Search by

SFR Name / SFR Content

Select SFR: FPT_TUD_EXT.1

SFR Options: 9

PPs

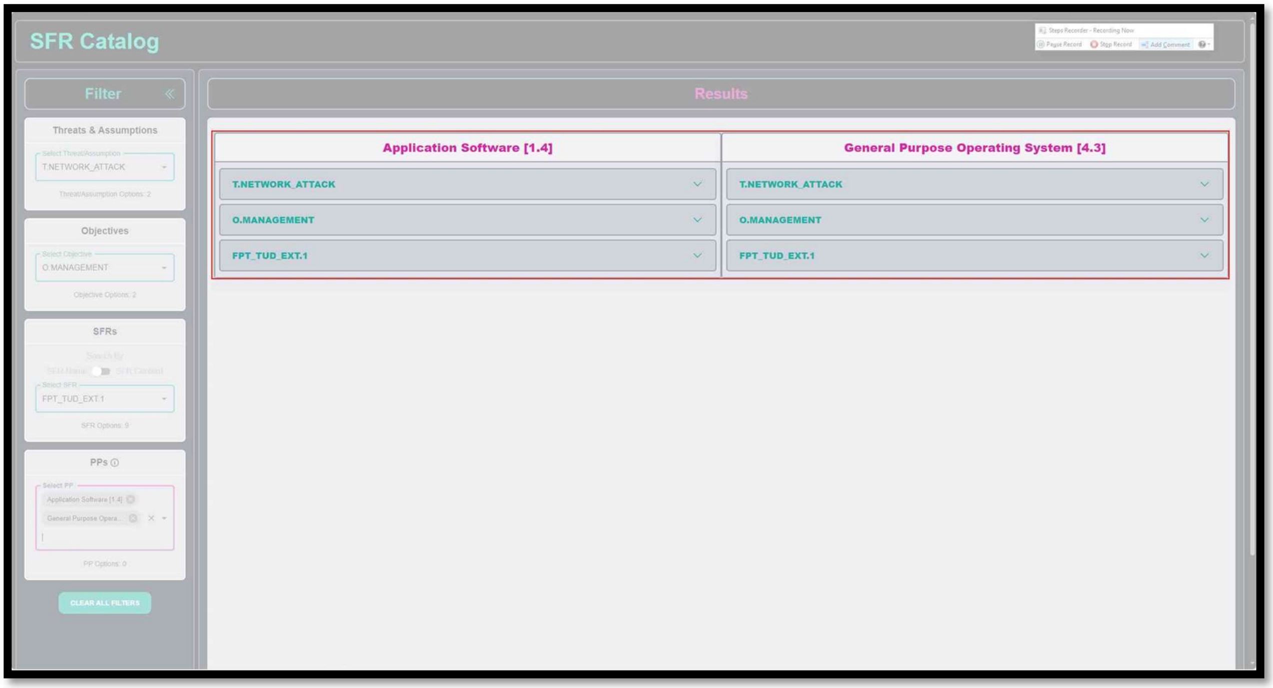
Select PP: Application Software [1.4], General Purpose Opera...

PP Options: 0

CLEAR ALL FILTERS

| Application Software [1.4] | General Purpose Operating System [4.3] |
|---|---|
| T.NETWORK_ATTACK | T.NETWORK_ATTACK |
| O.MANAGEMENT | O.MANAGEMENT |
| FPT_TUD_EXT.1 | FPT_TUD_EXT.1 |

## Comment: "Both PPs can be seen here in the 'Content Pane.'"



Select Threat/Assumption: T.NETWORK_ATTACK

Threat/Assumption Options: 2

Select Objective: O.MANAGEMENT

Objective Options: 2

Select SFR: FPT_TUD_EXT.1

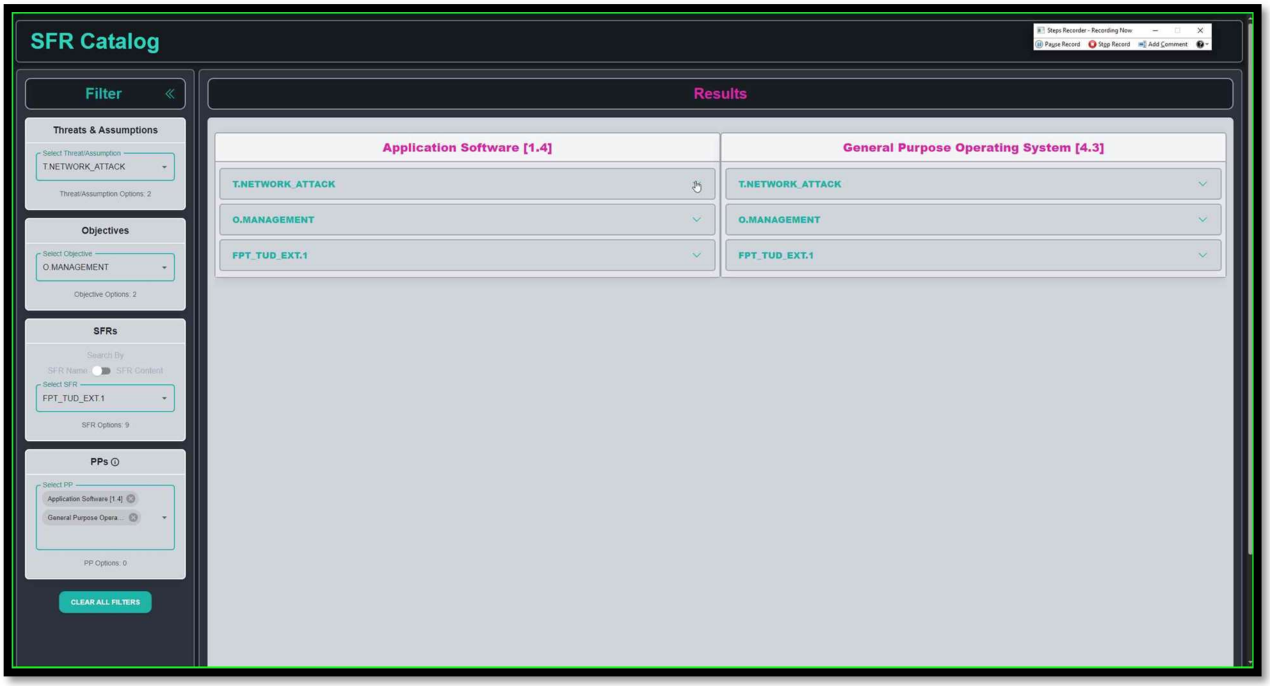
SFR Options: 9

Select PP: Application Software [1.4], General Purpose Opera...

PP Options: 0

| Application Software [1.4] | General Purpose Operating System [4.3] |
|---|---|
| T.NETWORK_ATTACK | T.NETWORK_ATTACK |
| O.MANAGEMENT | O.MANAGEMENT |
| FPT_TUD_EXT.1 | FPT_TUD_EXT.1 |

## Comment: "Click the arrow to open each of the content accordions."



SFR Catalog

Filter

Threats & Assumptions

Select Threat/Assumption: T.NETWORK_ATTACK

Threat/Assumption Options: 2

Objectives

Select Objective: O.MANAGEMENT

Objective Options: 2

SFRs

Search By: SFR Name / SFR Content

Select SFR: FPT_TUD_EXT.1

SFR Options: 9

PPs

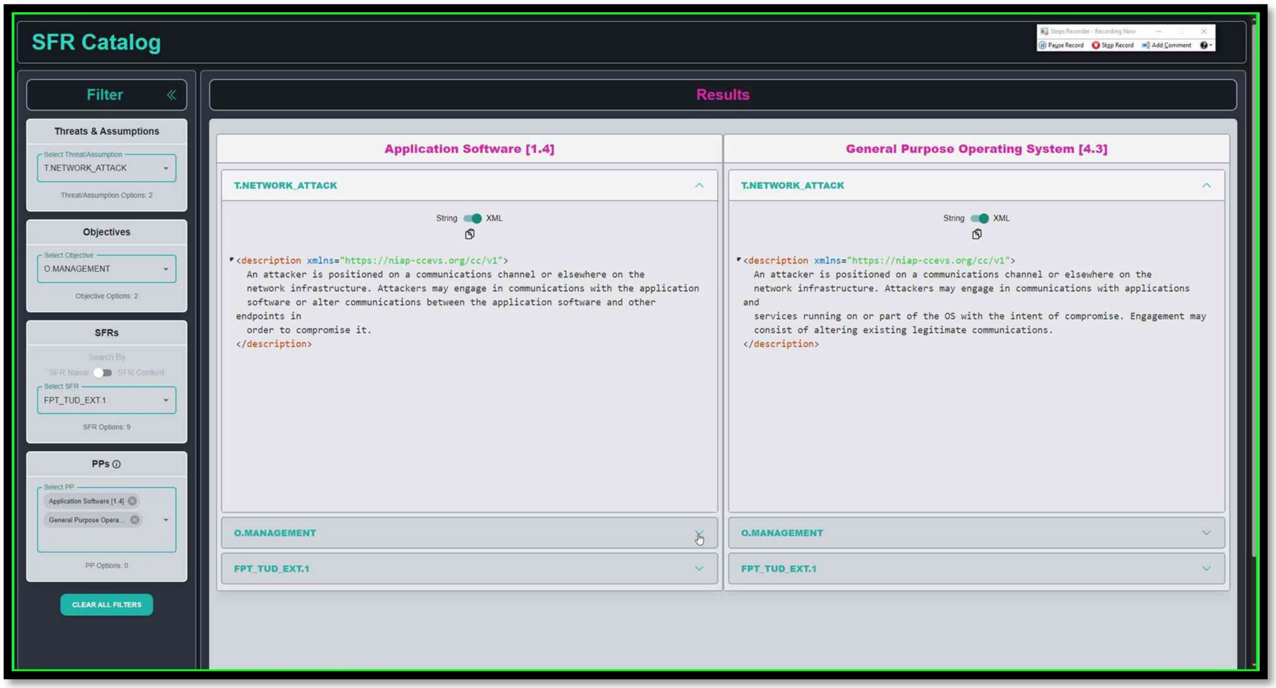
Select PP: Application Software [1.4], General Purpose Opera...

PP Options: 0

Results

| Application Software [1.4] | General Purpose Operating System [4.3] |
|---|---|
| T.NETWORK_ATTACK | T.NETWORK_ATTACK |
| O.MANAGEMENT | O.MANAGEMENT |
| FPT_TUD_EXT.1 | FPT_TUD_EXT.1 |

## Comment: "Continue to click each arrow to open all accordions at once.'"



Threats & Assumptions

Select Threat/Assumption: T.NETWORK_ATTACK

Threat/Assumption Options: 2

Objectives

Select Objective: O.MANAGEMENT

Objective Options: 2

SFRs

Select SFR: FPT_TUD_EXT.1

SFR Options: 9

PPs

Select PP: Application Software [1.4], General Purpose Opera...

PP Options: 0

**Application Software [1.4]**

T.NETWORK_ATTACK

```
<description xmlns="https://niap-ccevs.org/cc/v1">
  An attacker is positioned on a communications channel or elsewhere on the
  network infrastructure. Attackers may engage in communications with the application
  software or alter communications between the application software and other
endpoints in
  order to compromise it.
</description>
```

O.MANAGEMENT

FPT_TUD_EXT.1

**General Purpose Operating System [4.3]**

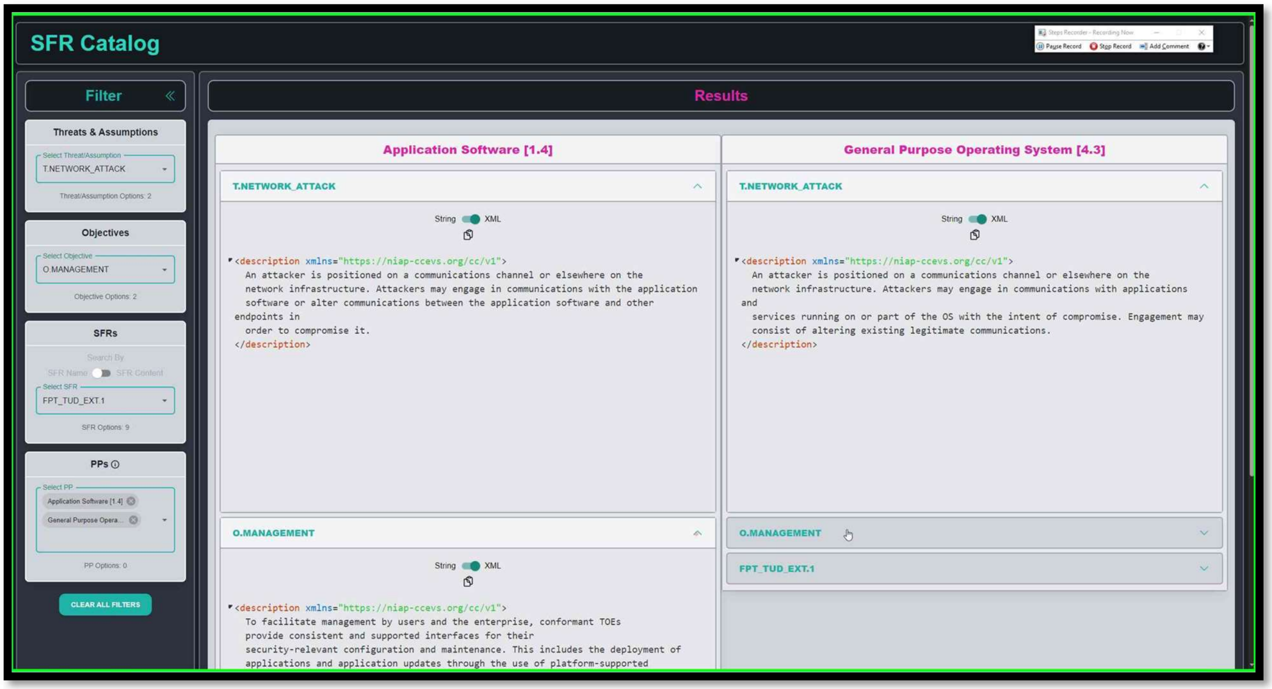
T.NETWORK_ATTACK

```
<description xmlns="https://niap-ccevs.org/cc/v1">
  An attacker is positioned on a communications channel or elsewhere on the
  network infrastructure. Attackers may engage in communications with applications
and
  services running on or part of the OS with the intent of compromise. Engagement may
  consist of altering existing legitimate communications.
</description>
```

O.MANAGEMENT

FPT_TUD_EXT.1

## Comment: "Continue to click each arrow to open all accordions at once."



Threats & Assumptions
Select Threat/Assumption: T.NETWORK_ATTACK
Threat/Assumption Options: 2

Objectives
Select Objective: O.MANAGEMENT
Objective Options: 2

SFRs
Search By: SFR Name / SFR Content
Select SFR: FPT_TUD_EXT.1
SFR Options: 9

PPs
Select PP: Application Software [1.4], General Purpose Opera...
PP Options: 0

**Application Software [1.4]**

T.NETWORK_ATTACK

```
<description xmlns="https://niap-ccevs.org/cc/v1">
  An attacker is positioned on a communications channel or elsewhere on the
  network infrastructure. Attackers may engage in communications with the application
  software or alter communications between the application software and other
endpoints in
  order to compromise it.
</description>
```

O.MANAGEMENT

```
<description xmlns="https://niap-ccevs.org/cc/v1">
  To facilitate management by users and the enterprise, conformant TOEs
  provide consistent and supported interfaces for their
  security-relevant configuration and maintenance. This includes the deployment of
  applications and application updates through the use of platform-supported
```

**General Purpose Operating System [4.3]**

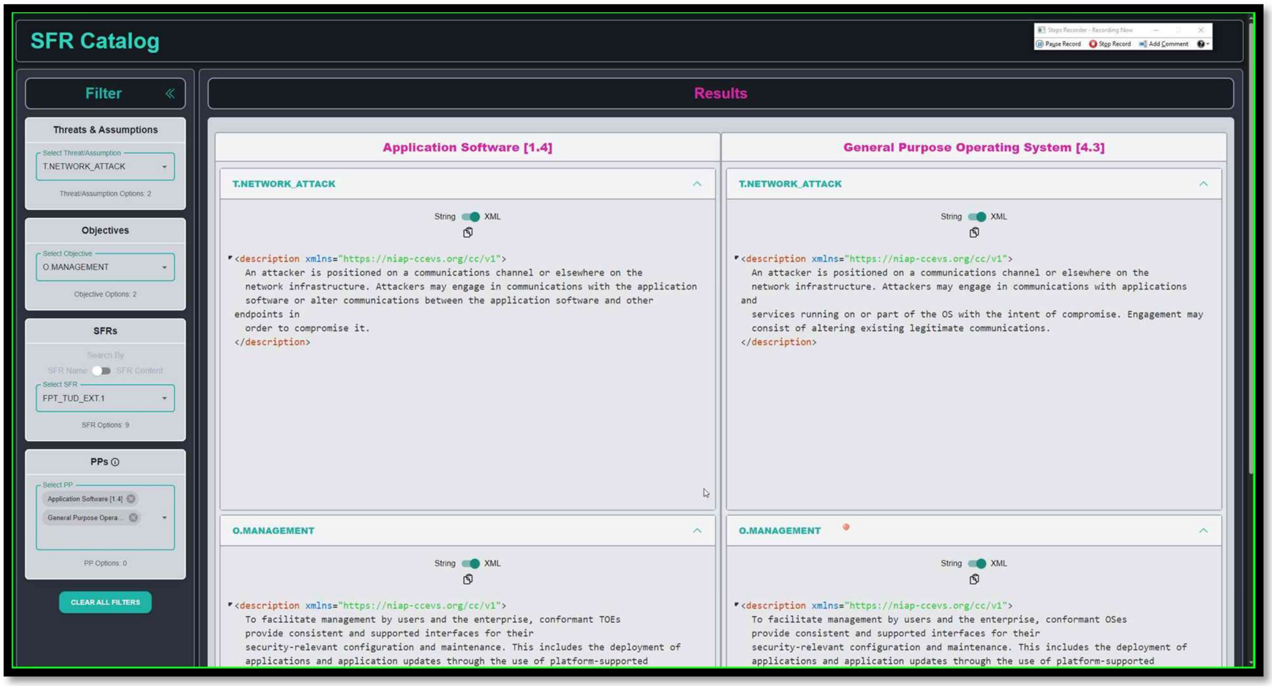
T.NETWORK_ATTACK

```
<description xmlns="https://niap-ccevs.org/cc/v1">
  An attacker is positioned on a communications channel or elsewhere on the
  network infrastructure. Attackers may engage in communications with applications
and
  services running on or part of the OS with the intent of compromise. Engagement may
  consist of altering existing legitimate communications.
</description>
```

O.MANAGEMENT

FPT_TUD_EXT.1

## Comment: "A user may scroll down to view all Threats, Objectives, or SFRs."



Threats & Assumptions

Select Threat/Assumption: T.NETWORK_ATTACK

Threat/Assumption Options: 2

Objectives

Select Objective: O.MANAGEMENT

Objective Options: 2

SFRs

Select SFR: FPT_TUD_EXT.1

SFR Options: 9

PPs

Select PP: Application Software [1.4], General Purpose Opera...

PP Options: 0

Application Software [1.4]

T.NETWORK_ATTACK

```
<description xmlns="https://niap-ccevs.org/cc/v1">
  An attacker is positioned on a communications channel or elsewhere on the
  network infrastructure. Attackers may engage in communications with the application
  software or alter communications between the application software and other
endpoints in
  order to compromise it.
</description>
```

O.MANAGEMENT

```
<description xmlns="https://niap-ccevs.org/cc/v1">
  To facilitate management by users and the enterprise, conformant TOEs
  provide consistent and supported interfaces for their
  security-relevant configuration and maintenance. This includes the deployment of
  applications and application updates through the use of platform-supported
```

General Purpose Operating System [4.3]

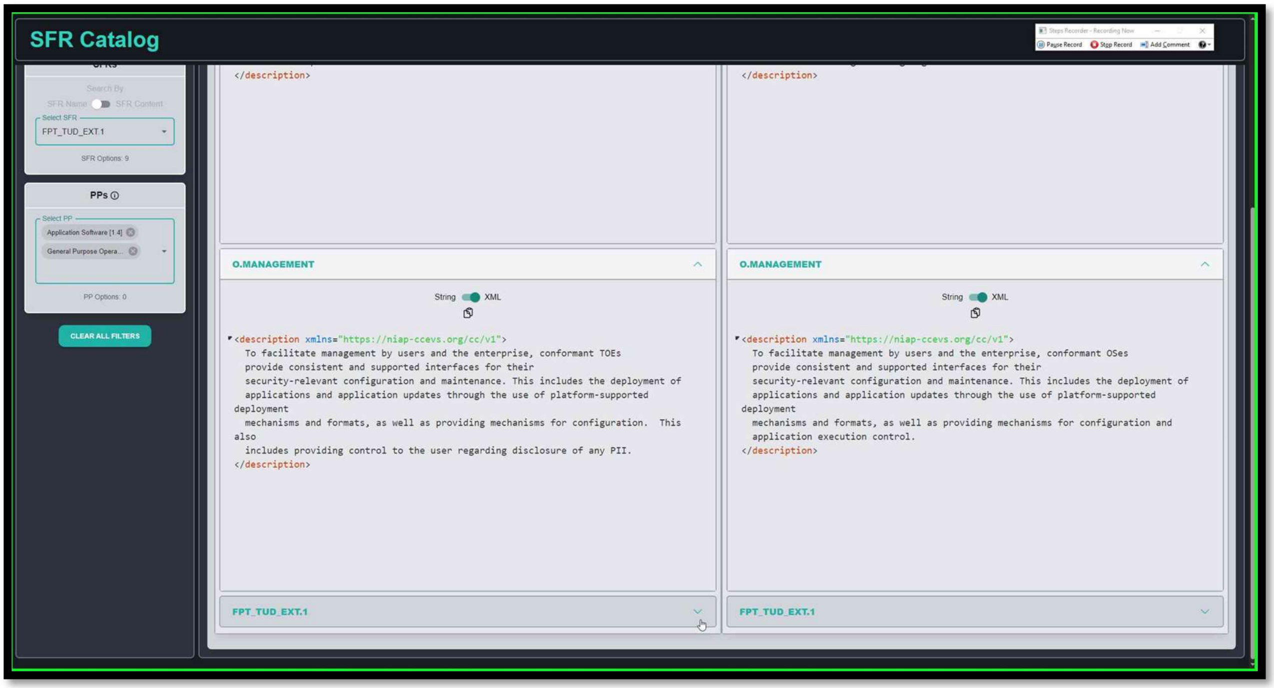
T.NETWORK_ATTACK

```
<description xmlns="https://niap-ccevs.org/cc/v1">
  An attacker is positioned on a communications channel or elsewhere on the
  network infrastructure. Attackers may engage in communications with applications
and
  services running on or part of the OS with the intent of compromise. Engagement may
  consist of altering existing legitimate communications.
</description>
```

O.MANAGEMENT

```
<description xmlns="https://niap-ccevs.org/cc/v1">
  To facilitate management by users and the enterprise, conformant OSes
  provide consistent and supported interfaces for their
  security-relevant configuration and maintenance. This includes the deployment of
  applications and application updates through the use of platform-supported
```

## Comment: "Continue to click each arrow to open all accordions at once."



Select SFR: FPT_TUD_EXT.1

SFR Options: 9

Select PP: Application Software [1.4], General Purpose Opera...

PP Options: 0

```
</description>
```

```
</description>
```

O.MANAGEMENT

```
<description xmlns="https://niap-ccevs.org/cc/v1">
  To facilitate management by users and the enterprise, conformant TOEs
  provide consistent and supported interfaces for their
  security-relevant configuration and maintenance. This includes the deployment of
  applications and application updates through the use of platform-supported
deployment
  mechanisms and formats, as well as providing mechanisms for configuration.  This
also
  includes providing control to the user regarding disclosure of any PII.
</description>
```

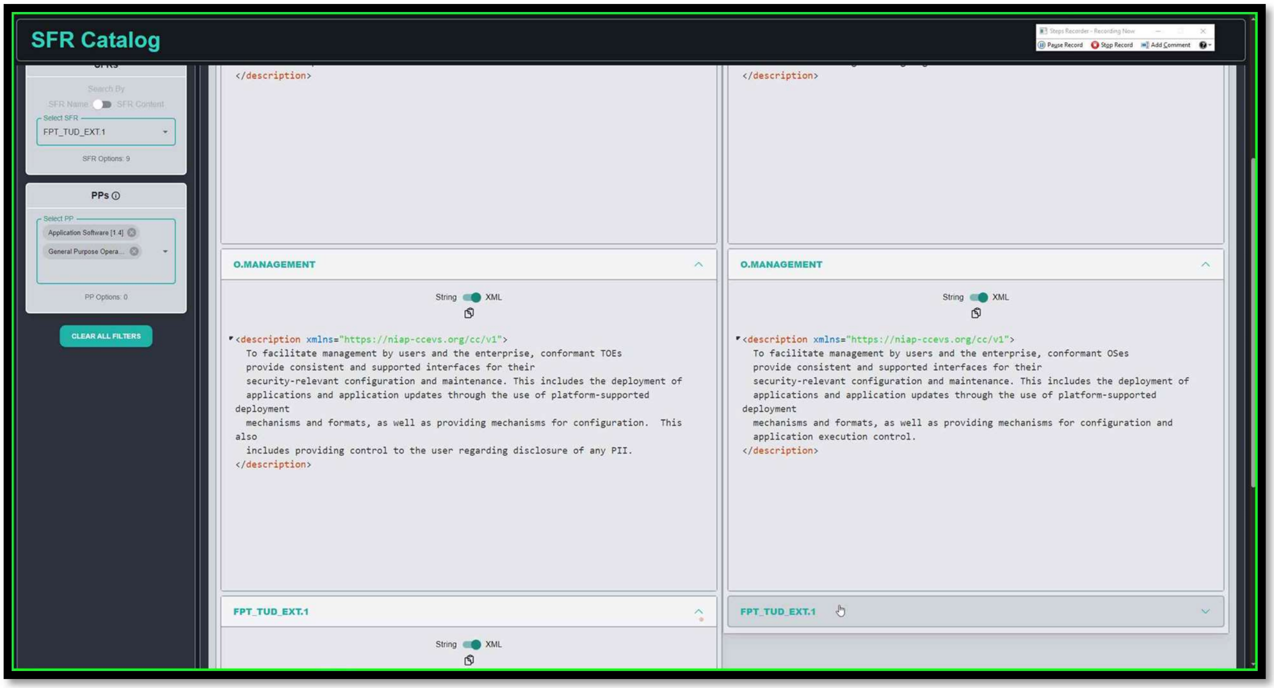
O.MANAGEMENT

```
<description xmlns="https://niap-ccevs.org/cc/v1">
  To facilitate management by users and the enterprise, conformant OSes
  provide consistent and supported interfaces for their
  security-relevant configuration and maintenance. This includes the deployment of
  applications and application updates through the use of platform-supported
deployment
  mechanisms and formats, as well as providing mechanisms for configuration and
  application execution control.
</description>
```

FPT_TUD_EXT.1

FPT_TUD_EXT.1

## Comment: "Continue to click each arrow to open all accordions at once."



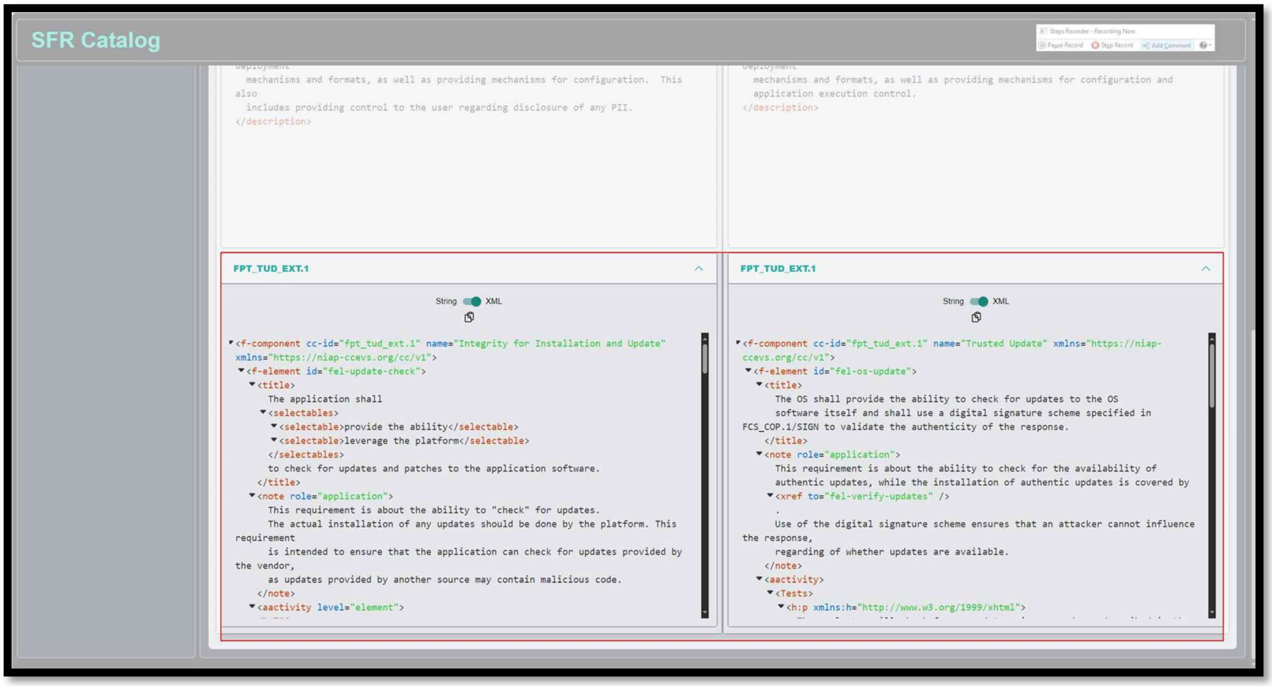
```
</description>
```

```
<description xmlns="https://niap-ccevs.org/cc/v1">
  To facilitate management by users and the enterprise, conformant TOEs
  provide consistent and supported interfaces for their
  security-relevant configuration and maintenance. This includes the deployment of
  applications and application updates through the use of platform-supported
deployment
  mechanisms and formats, as well as providing mechanisms for configuration.  This
also
  includes providing control to the user regarding disclosure of any PII.
</description>
```

```
</description>
```

```
<description xmlns="https://niap-ccevs.org/cc/v1">
  To facilitate management by users and the enterprise, conformant OSes
  provide consistent and supported interfaces for their
  security-relevant configuration and maintenance. This includes the deployment of
  applications and application updates through the use of platform-supported
deployment
  mechanisms and formats, as well as providing mechanisms for configuration and
  application execution control.
</description>
```

## Comment: "Here, a user can visually compare any of the selections with one another."



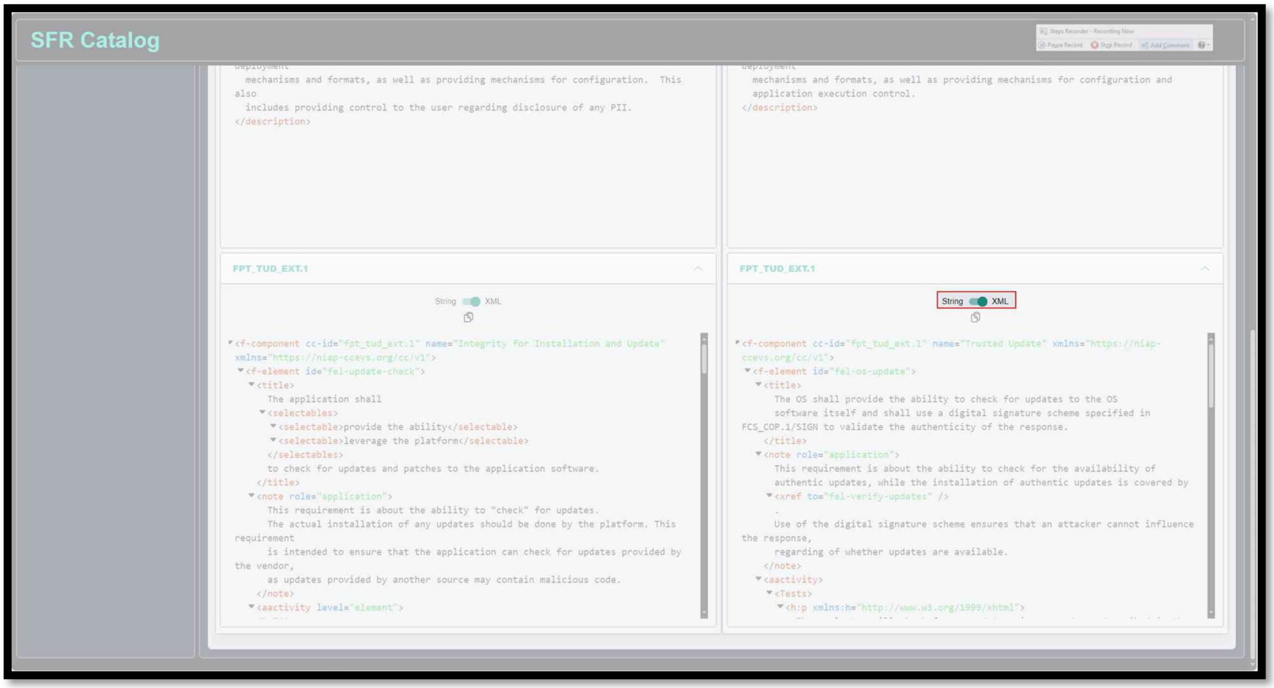
```
  mechanisms and formats, as well as providing mechanisms for configuration.  This
also
  includes providing control to the user regarding disclosure of any PII.
</description>
```

```
▾<f-component cc-id="fpt_tud_ext.1" name="Integrity for Installation and Update"
xmlns="https://niap-ccevs.org/cc/v1">
 ▾<f-element id="fel-update-check">
  ▾<title>
     The application shall
   ▾<selectables>
    ▾<selectable>provide the ability</selectable>
    ▾<selectable>leverage the platform</selectable>
     </selectables>
     to check for updates and patches to the application software.
   </title>
  ▾<note role="application">
     This requirement is about the ability to "check" for updates.
     The actual installation of any updates should be done by the platform. This
requirement
     is intended to ensure that the application can check for updates provided by
the vendor,
     as updates provided by another source may contain malicious code.
   </note>
  ▾<aactivity level="element">
```

```
  mechanisms and formats, as well as providing mechanisms for configuration and
  application execution control.
</description>
```

```
▾<f-component cc-id="fpt_tud_ext.1" name="Trusted Update" xmlns="https://niap-
ccevs.org/cc/v1">
 ▾<f-element id="fel-os-update">
  ▾<title>
     The OS shall provide the ability to check for updates to the OS
     software itself and shall use a digital signature scheme specified in
FCS_COP.1/SIGN to validate the authenticity of the response.
   </title>
  ▾<note role="application">
     This requirement is about the ability to check for the availability of
     authentic updates, while the installation of authentic updates is covered by
   ▾<xref to="fel-verify-updates" />
     .
     Use of the digital signature scheme ensures that an attacker cannot influence
the response,
     regarding of whether updates are available.
   </note>
  ▾<aactivity>
   ▾<Tests>
    ▾<h:p xmlns:h="http://www.w3.org/1999/xhtml">
```

## Comment: "This toggle will allow a user to switch between XML and text view."



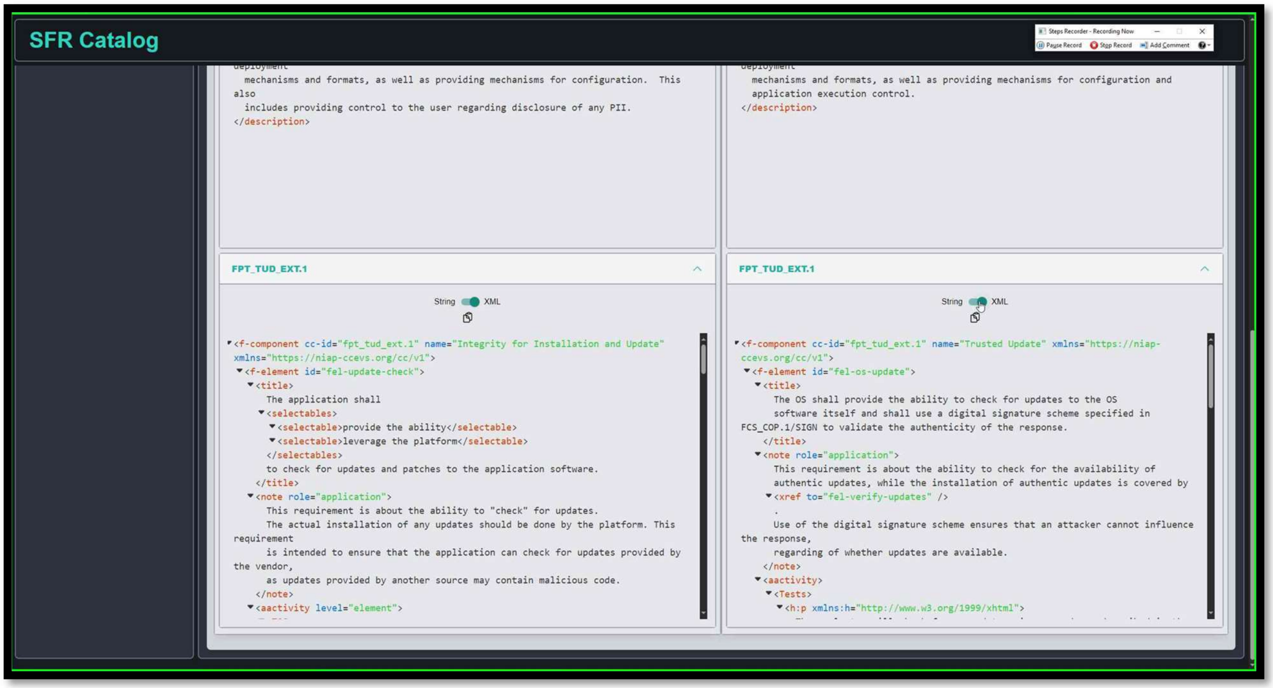
```
deployment
  mechanisms and formats, as well as providing mechanisms for configuration.  This
also
  includes providing control to the user regarding disclosure of any PII.
</description>
```

```
<f-component cc-id="fpt_tud_ext.1" name="Integrity for Installation and Update"
xmlns="https://niap-ccevs.org/cc/v1">
  <f-element id="fel-update-check">
    <title>
      The application shall
      <selectables>
        <selectable>provide the ability</selectable>
        <selectable>leverage the platform</selectable>
      </selectables>
      to check for updates and patches to the application software.
    </title>
    <note role="application">
      This requirement is about the ability to "check" for updates.
      The actual installation of any updates should be done by the platform. This
requirement
      is intended to ensure that the application can check for updates provided by
the vendor,
      as updates provided by another source may contain malicious code.
    </note>
    <aactivity level="element">
```

```
deployment
  mechanisms and formats, as well as providing mechanisms for configuration and
  application execution control.
</description>
```

```
<f-component cc-id="fpt_tud_ext.1" name="Trusted Update" xmlns="https://niap-
ccevs.org/cc/v1">
  <f-element id="fel-os-update">
    <title>
      The OS shall provide the ability to check for updates to the OS
      software itself and shall use a digital signature scheme specified in
FCS_COP.1/SIGN to validate the authenticity of the response.
    </title>
    <note role="application">
      This requirement is about the ability to check for the availability of
      authentic updates, while the installation of authentic updates is covered by
      <xref to="fel-verify-updates" />
      .
      Use of the digital signature scheme ensures that an attacker cannot influence
the response,
      regarding of whether updates are available.
    </note>
    <aactivity>
      <Tests>
        <h:p xmlns:h="http://www.w3.org/1999/xhtml">
```

## Comment: "The next two screenshots will demonstrate the toggle procedure."



```
deployment
  mechanisms and formats, as well as providing mechanisms for configuration.  This
also
  includes providing control to the user regarding disclosure of any PII.
</description>
```

FPT_TUD_EXT.1

String XML

```
<f-component cc-id="fpt_tud_ext.1" name="Integrity for Installation and Update"
xmlns="https://niap-ccevs.org/cc/v1">
 <f-element id="fel-update-check">
  <title>
     The application shall
    <selectables>
     <selectable>provide the ability</selectable>
     <selectable>leverage the platform</selectable>
    </selectables>
     to check for updates and patches to the application software.
  </title>
  <note role="application">
     This requirement is about the ability to "check" for updates.
     The actual installation of any updates should be done by the platform. This
requirement
     is intended to ensure that the application can check for updates provided by
the vendor,
     as updates provided by another source may contain malicious code.
  </note>
  <aactivity level="element">
```

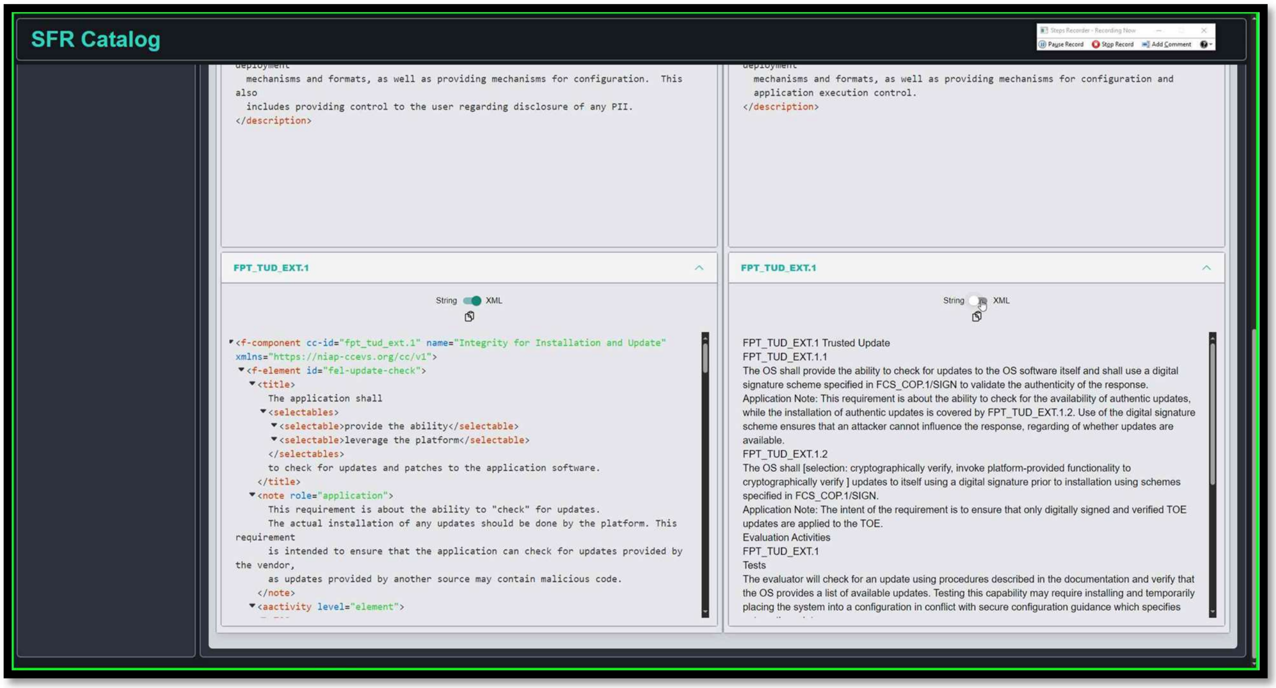
```
deployment
  mechanisms and formats, as well as providing mechanisms for configuration and
  application execution control.
</description>
```

FPT_TUD_EXT.1

String XML

```
<f-component cc-id="fpt_tud_ext.1" name="Trusted Update" xmlns="https://niap-
ccevs.org/cc/v1">
 <f-element id="fel-os-update">
  <title>
     The OS shall provide the ability to check for updates to the OS
     software itself and shall use a digital signature scheme specified in
FCS_COP.1/SIGN to validate the authenticity of the response.
  </title>
  <note role="application">
     This requirement is about the ability to check for the availability of
     authentic updates, while the installation of authentic updates is covered by
   <xref to="fel-verify-updates" />
     .
     Use of the digital signature scheme ensures that an attacker cannot influence
the response,
     regarding of whether updates are available.
  </note>
  <aactivity>
   <Tests>
    <h:p xmlns:h="http://www.w3.org/1999/xhtml">
```

## Comment: "This is the toggled text on the right."



```
  mechanisms and formats, as well as providing mechanisms for configuration.  This
also
  includes providing control to the user regarding disclosure of any PII.
</description>
```

FPT_TUD_EXT.1

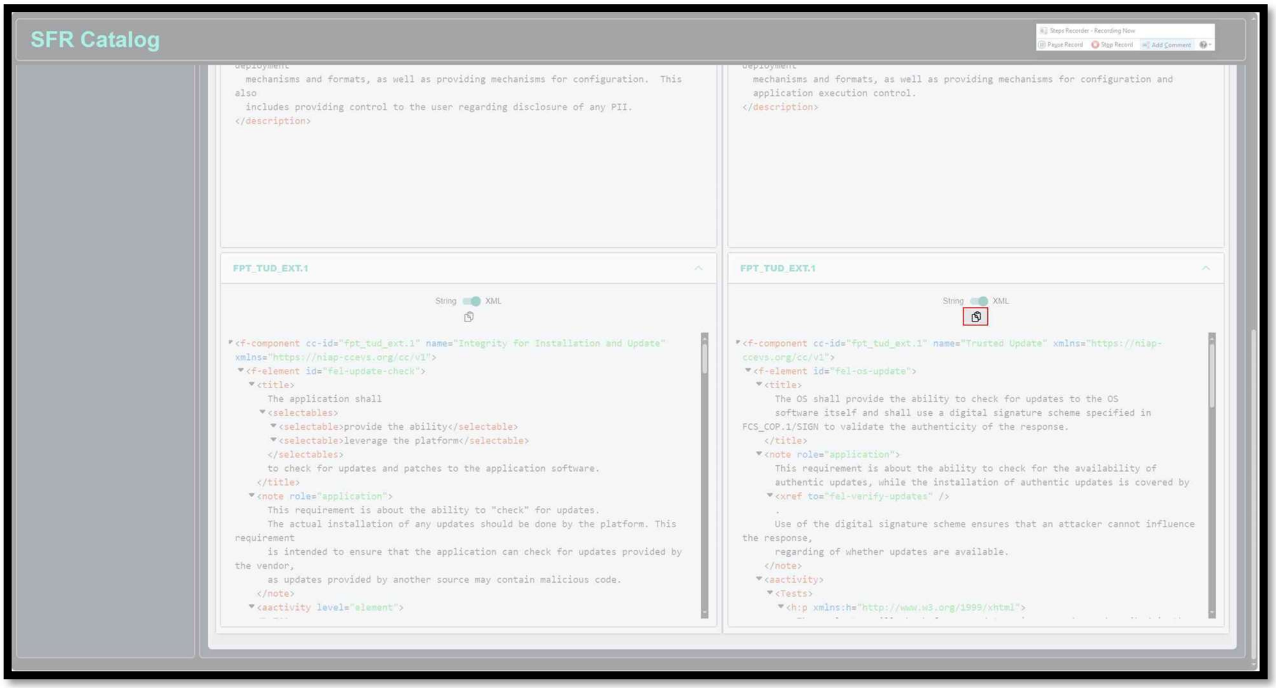
```
<f-component cc-id="fpt_tud_ext.1" name="Integrity for Installation and Update"
xmlns="https://niap-ccevs.org/cc/v1">
 <f-element id="fel-update-check">
  <title>
    The application shall
   <selectables>
    <selectable>provide the ability</selectable>
    <selectable>leverage the platform</selectable>
    </selectables>
    to check for updates and patches to the application software.
  </title>
  <note role="application">
    This requirement is about the ability to "check" for updates.
    The actual installation of any updates should be done by the platform. This
requirement
    is intended to ensure that the application can check for updates provided by
the vendor,
    as updates provided by another source may contain malicious code.
  </note>
  <aactivity level="element">
```

```
  mechanisms and formats, as well as providing mechanisms for configuration and
  application execution control.
</description>
```

FPT_TUD_EXT.1

FPT_TUD_EXT.1 Trusted Update
FPT_TUD_EXT.1.1
The OS shall provide the ability to check for updates to the OS software itself and shall use a digital signature scheme specified in FCS_COP.1/SIGN to validate the authenticity of the response.
Application Note: This requirement is about the ability to check for the availability of authentic updates, while the installation of authentic updates is covered by FPT_TUD_EXT.1.2. Use of the digital signature scheme ensures that an attacker cannot influence the response, regarding of whether updates are available.
FPT_TUD_EXT.1.2
The OS shall [selection: cryptographically verify, invoke platform-provided functionality to cryptographically verify ] updates to itself using a digital signature prior to installation using schemes specified in FCS_COP.1/SIGN.
Application Note: The intent of the requirement is to ensure that only digitally signed and verified TOE updates are applied to the TOE.
Evaluation Activities
FPT_TUD_EXT.1
Tests
The evaluator will check for an update using procedures described in the documentation and verify that the OS provides a list of available updates. Testing this capability may require installing and temporarily placing the system into a configuration in conflict with secure configuration guidance which specifies

## Comment: "This button will allow a user to copy the selected XML to their clipboard for pasting elsewhere."



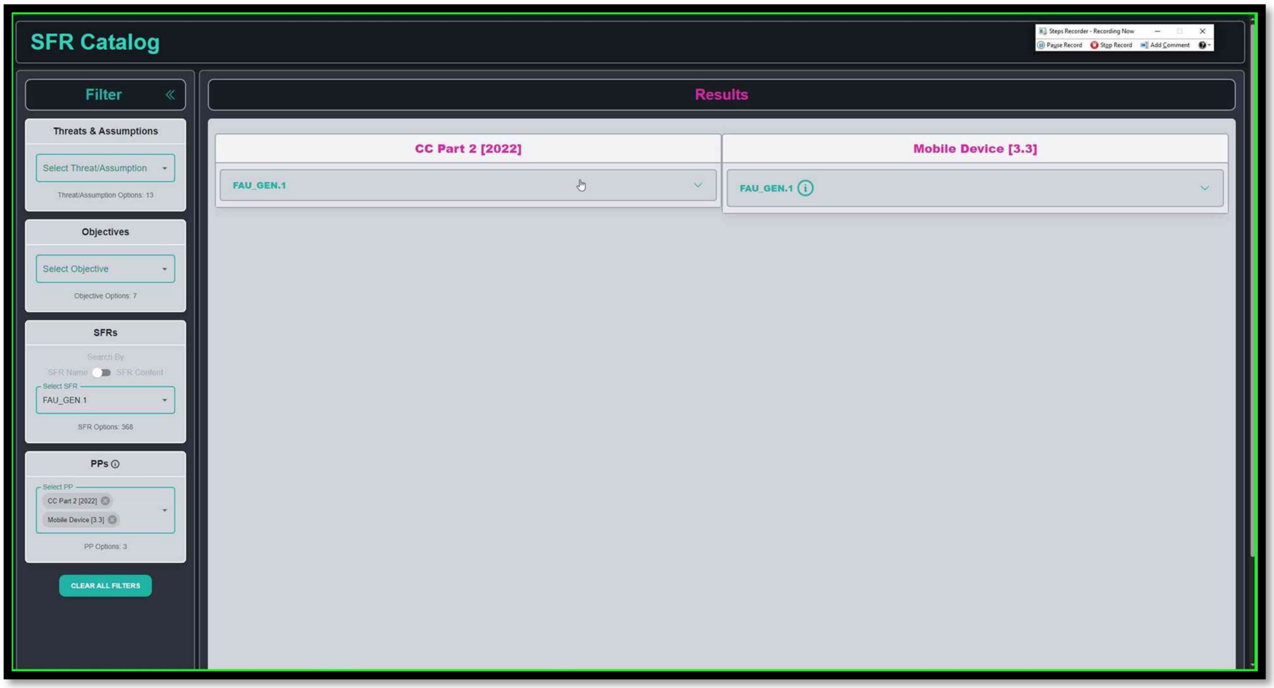
```
deployment
  mechanisms and formats, as well as providing mechanisms for configuration.  This
also
  includes providing control to the user regarding disclosure of any PII.
</description>
```

```
<f-component cc-id="fpt_tud_ext.1" name="Integrity for Installation and Update"
xmlns="https://niap-ccevs.org/cc/v1">
 <f-element id="fel-update-check">
  <title>
    The application shall
   <selectables>
    <selectable>provide the ability</selectable>
    <selectable>leverage the platform</selectable>
   </selectables>
    to check for updates and patches to the application software.
  </title>
  <note role="application">
    This requirement is about the ability to "check" for updates.
    The actual installation of any updates should be done by the platform. This
requirement
    is intended to ensure that the application can check for updates provided by
the vendor,
    as updates provided by another source may contain malicious code.
  </note>
  <aactivity level="element">
```

```
deployment
  mechanisms and formats, as well as providing mechanisms for configuration and
  application execution control.
</description>
```

```
<f-component cc-id="fpt_tud_ext.1" name="Trusted Update" xmlns="https://niap-
ccevs.org/cc/v1">
 <f-element id="fel-os-update">
  <title>
    The OS shall provide the ability to check for updates to the OS
    software itself and shall use a digital signature scheme specified in
FCS_COP.1/SIGN to validate the authenticity of the response.
  </title>
  <note role="application">
    This requirement is about the ability to check for the availability of
    authentic updates, while the installation of authentic updates is covered by
   <xref to="fel-verify-updates" />
    .
    Use of the digital signature scheme ensures that an attacker cannot influence
the response,
    regarding of whether updates are available.
  </note>
  <aactivity>
   <Tests>
    <h:p xmlns:h="http://www.w3.org/1999/xhtml">
```

## Comment: "Below is an example of the CC 2022 Part 2 displayed next to another PP for comparison. The next screenshot will show their contents compared."



SFR Catalog

Filter

Threats & Assumptions

Select Threat/Assumption

Threat/Assumption Options: 13

Objectives

Select Objective

Objective Options: 7

SFRs

Search By

SFR Name SFR Content

Select SFR: FAU_GEN.1

SFR Options: 368

PPs

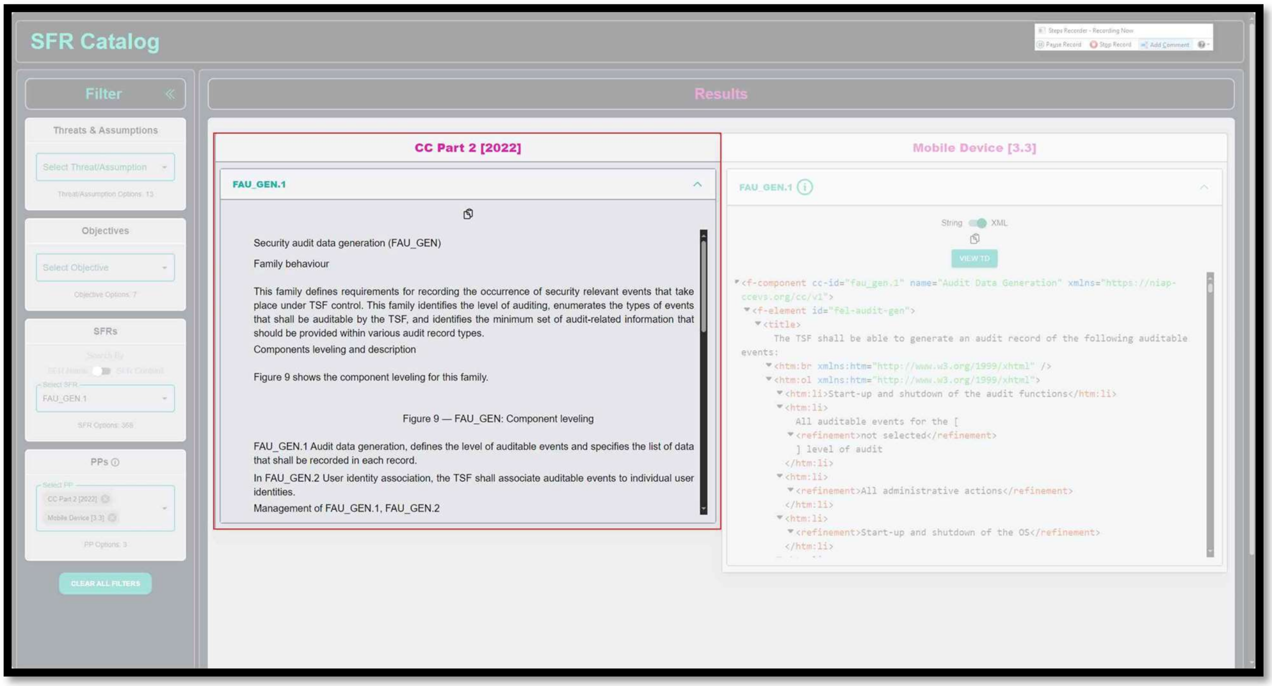
Select PP: CC Part 2 [2022], Mobile Device [3.3]

PP Options: 3

Results

| CC Part 2 [2022] | Mobile Device [3.3] |
|---|---|
| FAU_GEN.1 | FAU_GEN.1 |

## Comment: "Here the CC 2022 Part 2 is displayed. This is an option for any SFR whose family is represented in the CC 2022 Part 2."



Security audit data generation (FAU_GEN)

Family behaviour

This family defines requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types.

Components leveling and description

Figure 9 shows the component leveling for this family.

Figure 9 — FAU_GEN: Component leveling

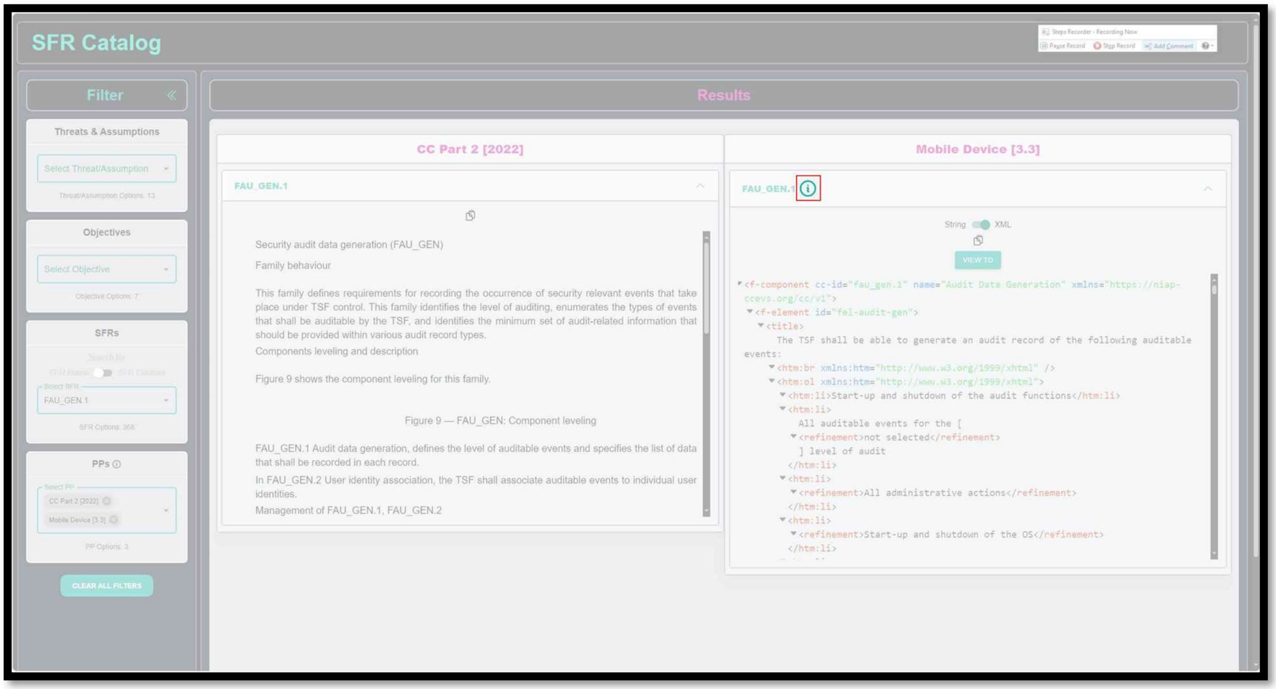
FAU_GEN.1 Audit data generation, defines the level of auditable events and specifies the list of data that shall be recorded in each record.

In FAU_GEN.2 User identity association, the TSF shall associate auditable events to individual user identities.

Management of FAU_GEN.1, FAU_GEN.2

```
<f-component cc-id="fau_gen.1" name="Audit Data Generation" xmlns="https://niap-ccevs.org/cc/v1">
  <f-element id="fel-audit-gen">
    <title>
      The TSF shall be able to generate an audit record of the following auditable events:
        <htm:br xmlns:htm="http://www.w3.org/1999/xhtml" />
        <htm:ol xmlns:htm="http://www.w3.org/1999/xhtml">
          <htm:li>Start-up and shutdown of the audit functions</htm:li>
          <htm:li>
            All auditable events for the [
            <refinement>not selected</refinement>
            ] level of audit
          </htm:li>
          <htm:li>
            <refinement>All administrative actions</refinement>
          </htm:li>
          <htm:li>
            <refinement>Start-up and shutdown of the OS</refinement>
          </htm:li>
```

## Comment: "This icon indicates that a TD is recorded for this SFR within this PP. Hover over the icon to see what TD number is applied."



Security audit data generation (FAU_GEN)

Family behaviour

This family defines requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types.

Components leveling and description

Figure 9 shows the component leveling for this family.

Figure 9 — FAU_GEN: Component leveling

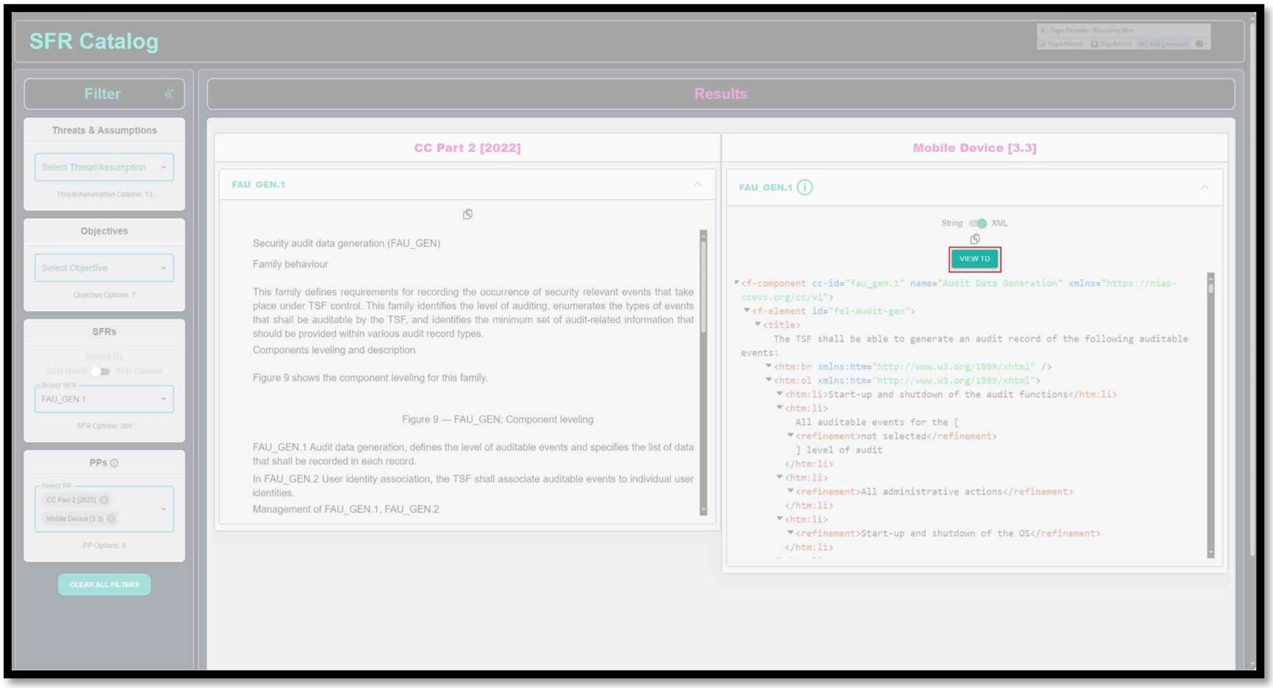
FAU_GEN.1 Audit data generation, defines the level of auditable events and specifies the list of data that shall be recorded in each record.

In FAU_GEN.2 User identity association, the TSF shall associate auditable events to individual user identities.

Management of FAU_GEN.1, FAU_GEN.2

```
<f-component cc-id="fau_gen.1" name="Audit Data Generation" xmlns="https://niap-ccevs.org/cc/v1">
 <f-element id="fel-audit-gen">
  <title>
    The TSF shall be able to generate an audit record of the following auditable events:
    <htm:br xmlns:htm="http://www.w3.org/1999/xhtml" />
    <htm:ol xmlns:htm="http://www.w3.org/1999/xhtml">
     <htm:li>Start-up and shutdown of the audit functions</htm:li>
     <htm:li>
       All auditable events for the [
      <refinement>not selected</refinement>
       ] level of audit
     </htm:li>
     <htm:li>
      <refinement>All administrative actions</refinement>
     </htm:li>
     <htm:li>
      <refinement>Start-up and shutdown of the OS</refinement>
     </htm:li>
```

## Comment: "This button will allow a user to view the HTML of the TD."



Security audit data generation (FAU_GEN)

Family behaviour

This family defines requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types.

Components leveling and description

Figure 9 shows the component leveling for this family.

Figure 9 — FAU_GEN: Component leveling

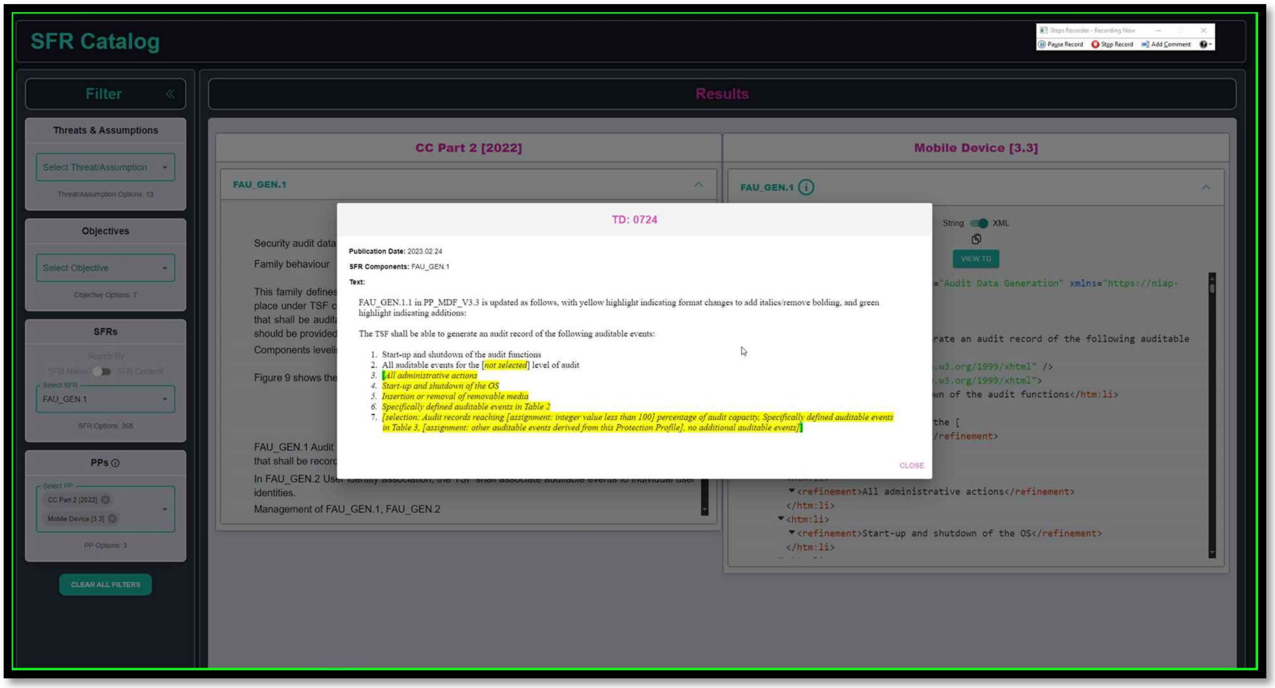
FAU_GEN.1 Audit data generation, defines the level of auditable events and specifies the list of data that shall be recorded in each record.

In FAU_GEN.2 User identity association, the TSF shall associate auditable events to individual user identities.

Management of FAU_GEN.1, FAU_GEN.2

```
<f-component cc-id="fau_gen.1" name="Audit Data Generation" xmlns="https://niap-ccevs.org/cc/v1">
 <f-element id="fel-audit-gen">
  <title>
     The TSF shall be able to generate an audit record of the following auditable events:
    <htm:br xmlns:htm="http://www.w3.org/1999/xhtml" />
    <htm:ol xmlns:htm="http://www.w3.org/1999/xhtml">
     <htm:li>Start-up and shutdown of the audit functions</htm:li>
     <htm:li>
       All auditable events for the [
      <refinement>not selected</refinement>
       ] level of audit
     </htm:li>
     <htm:li>
      <refinement>All administrative actions</refinement>
     </htm:li>
     <htm:li>
      <refinement>Start-up and shutdown of the OS</refinement>
     </htm:li>
```

## User mouse wheel down in "Catalog - Work - Microsoft Edge"



Security audit data

Family behaviour

This family defines place under TSF c that shall be audit should be provided

Components leveli

Figure 9 shows the

FAU_GEN.1 Audit that shall be record

In FAU_GEN.2 Use identities.

Management of FAU_GEN.1, FAU_GEN.2

```
="Audit Data Generation" xmlns="https://niap-
rate an audit record of the following auditable
.w3.org/1999/xhtml" />
.w3.org/1999/xhtml">
wn of the audit functions</htm:li>
the [
/refinement>
  <refinement>All administrative actions</refinement>
</htm:li>
<htm:li>
  <refinement>Start-up and shutdown of the OS</refinement>
</htm:li>
```

**TD: 0724**

**Publication Date:** 2023.02.24

**SFR Components:** FAU_GEN.1

**Text:**

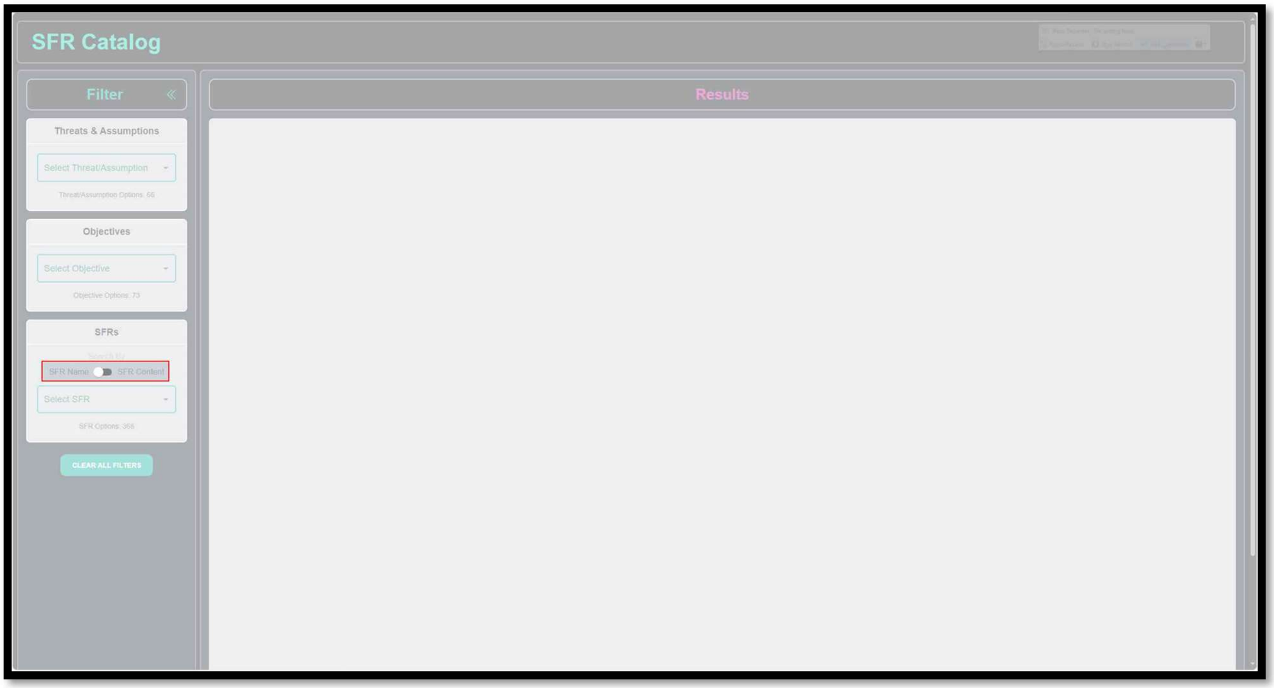
FAU_GEN.1.1 in PP_MDF_V3.3 is updated as follows, with yellow highlight indicating format changes to add italics/remove bolding, and green highlight indicating additions:

The TSF shall be able to generate an audit record of the following auditable events:

1. Start-up and shutdown of the audit functions
2. All auditable events for the [*not selected*] level of audit
3. *[All administrative actions*
4. *Start-up and shutdown of the OS*
5. *Insertion or removal of removable media*
6. *Specifically defined auditable events in Table 2*
7. *[selection: Audit records reaching [assignment: integer value less than 100] percentage of audit capacity, Specifically defined auditable events in Table 3, [assignment: other auditable events derived from this Protection Profile], no additional auditable events]*]

CLOSE

## Comment: "This toggle allows a user to switch between searching for the name (or identifier) of an SFR and searching for content within an SFR."


SFR Catalog
Filter «
Results
Threats & Assumptions
Select Threat/Assumption
Threat/Assumption Options: 66
Objectives
Select Objective
Objective Options: 73
SFRs
Search By
SFR Name
SFR Content
Select SFR
SFR Options: 366
CLEAR ALL FILTERS