

# 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 \(github.com\)](https://github.com/commoncriteria/sfr-catalog/blob/main/README.md)

## Feature Outline and Guide:

- **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."**



**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."**

The screenshot displays the 'SFR Catalog' application interface. On the left is a 'Filter' sidebar, and on the right is a 'Results' area. The sidebar contains three filter cards: 'Threats & Assumptions', 'Objectives', and 'SFRs'. The 'Threats & Assumptions' card is highlighted with a red border and contains a dropdown menu labeled 'Select Threat/Assumption' with 'Threat/Assumption Options: 66' below it. The 'Objectives' card contains a dropdown menu labeled 'Select Objective' with 'Objective Options: 73' below it. The 'SFRs' card contains a dropdown menu labeled 'Select SFR' with 'SFR Options: 988' below it. At the bottom of the sidebar is a 'CLEAR ALL FILTERS' button. The 'Results' area is currently empty. In the top right corner of the application, there is a navigation bar with links for 'Steps Recorder - Recording Now', 'Page Record', 'Stop Record', and 'Add Comment'.

**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."**

The screenshot displays the 'SFR Catalog' application interface. The top header bar is dark gray with the title 'SFR Catalog' in teal on the left and a navigation menu on the right containing 'Step Recorder - Recording New', 'Page Record', 'Step Record', and 'Add Comment'. Below the header, the interface is split into two main sections: 'Filter' on the left and 'Results' on the right. The 'Filter' section contains three filterable categories: 'Threats & Assumptions' with a dropdown menu showing 'ThreatAssumption Options: 66' (highlighted with a red box), 'Objectives' with a dropdown menu showing 'Objective Options: 73', and 'SFRs' with a dropdown menu showing 'SFR Options: 368'. A 'CLEAR ALL FILTERS' button is located at the bottom of the filter section. The 'Results' section is currently empty, showing a large gray area.

**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."**



**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."**

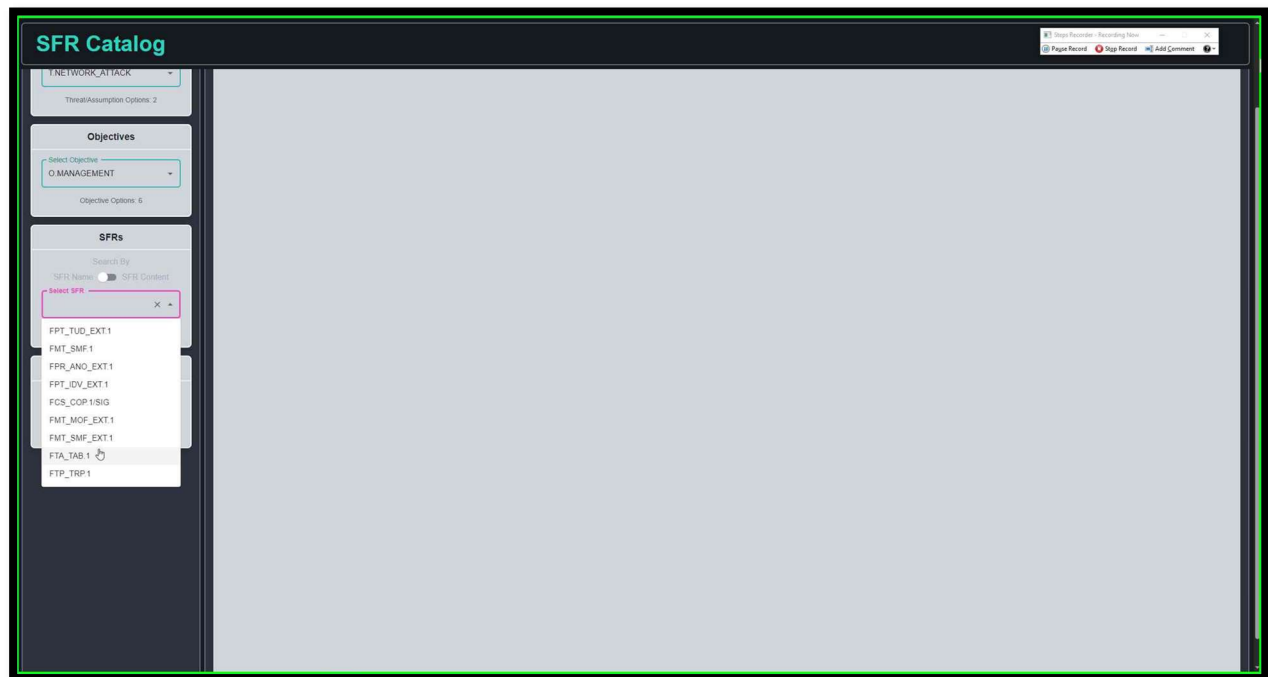
The screenshot displays the 'SFR Catalog' application interface. On the left, a 'Filter' sidebar contains four filterable categories: 'Threats & Assumptions' (13 options), 'Objectives' (7 options), 'SFRs' (368 options, with a toggle for 'SFR ID: Name' and 'SFR ID: Content'), and 'PPs' (5 options). A 'CLEAR ALL FILTERS' button is located at the bottom of the sidebar. The main area on the right is labeled 'Results' and is currently empty. The top right corner of the interface includes a 'Steps Recorder - Recording Now' notification and links for 'Page Record', 'Page Record', and 'Add Comment'.

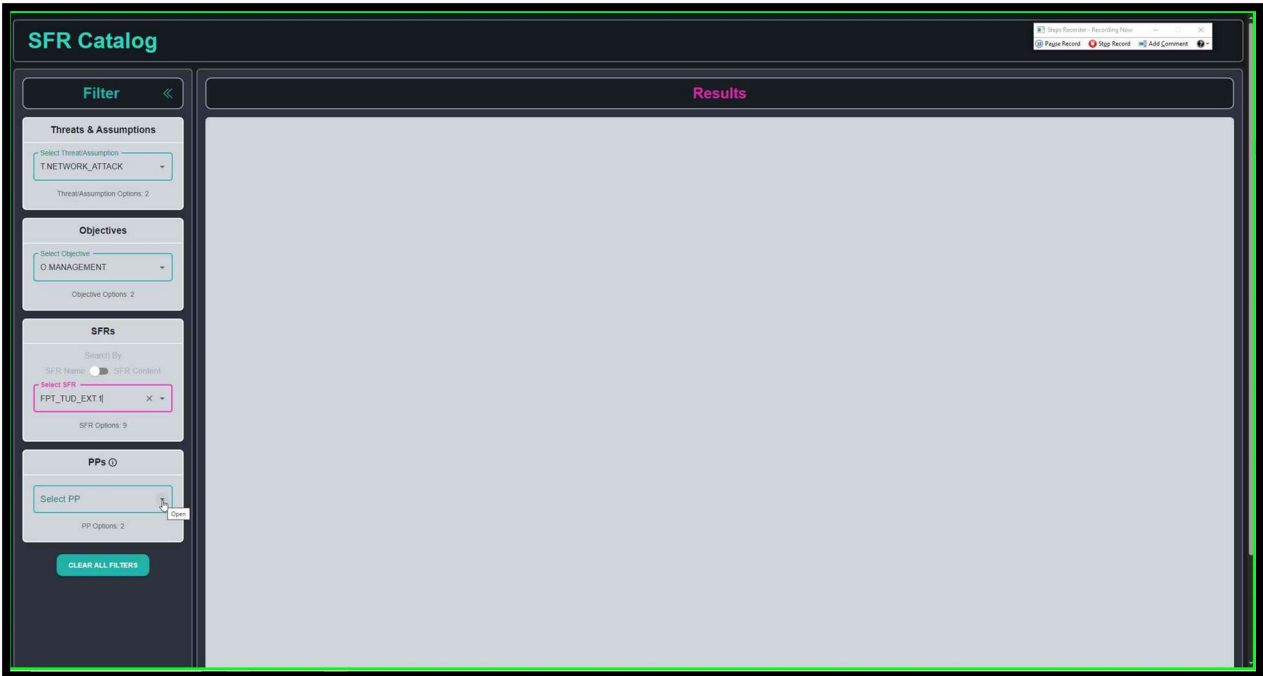
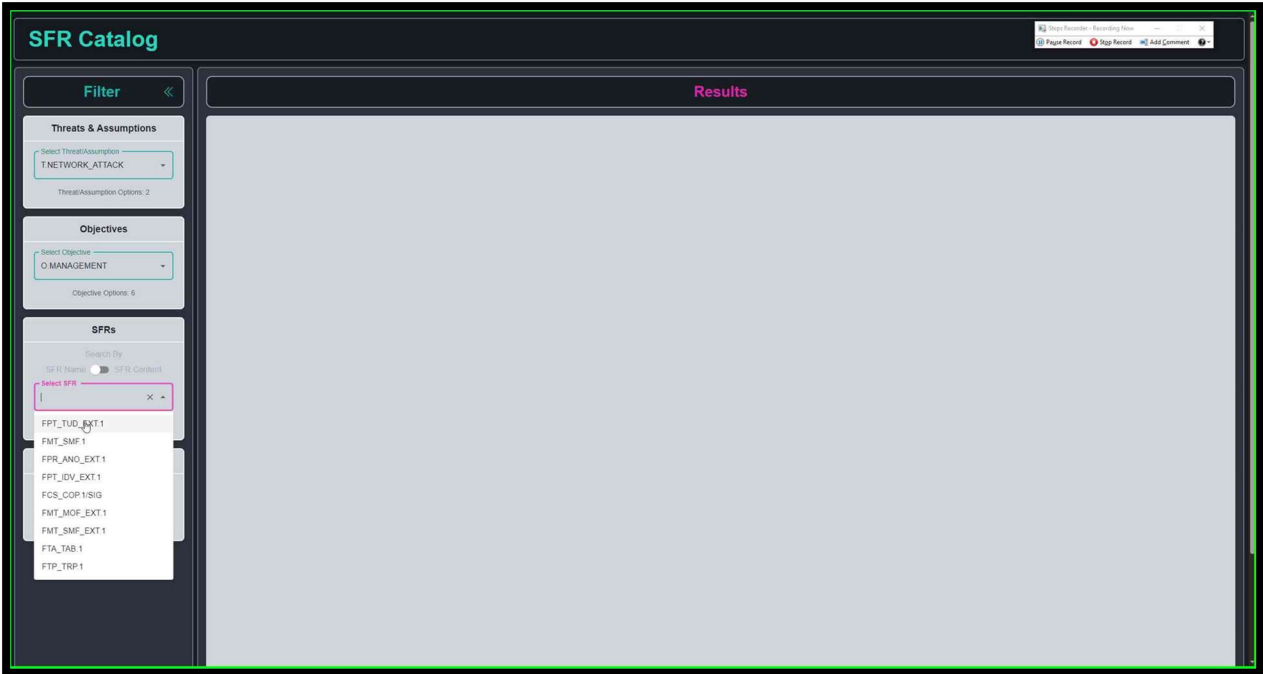


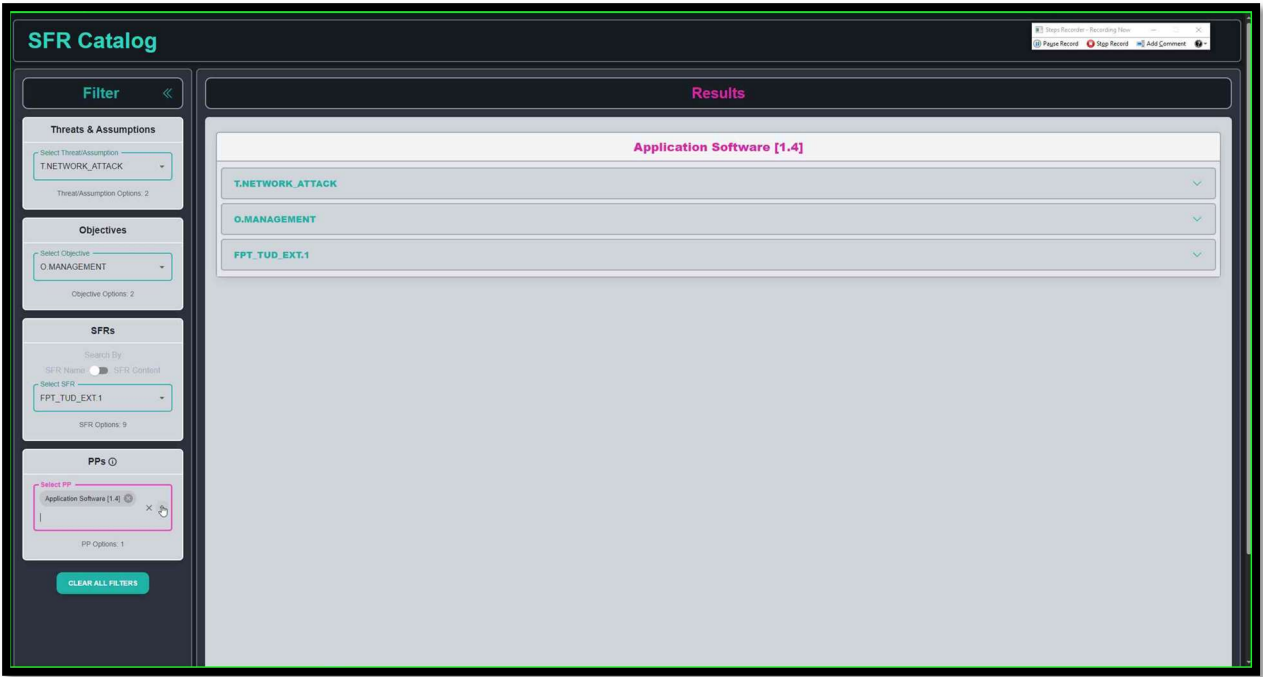
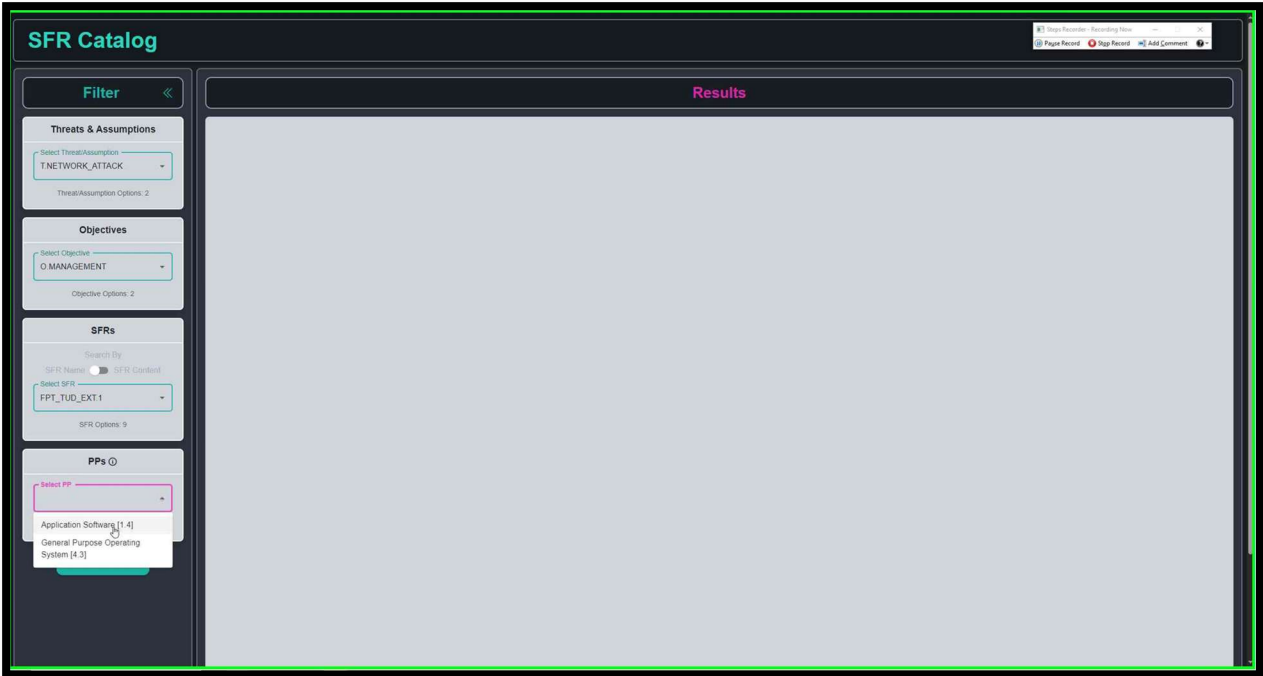
**Comment: "This button allows a user to clear all filters and reset the application to unfiltered lists."**



**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.”**







SFR Catalog

Steps Recorder - Recording Step

Page RecordPage RecordAdd Comment

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 NameSFR Comment

Select SFR

FPT\_TUD\_EXT.1

SFR Options: 9

PPs

Select PP

Application Software [1.4]

General Purpose Operating System [4.3]

CLEAR ALL FILTERS

Results

Application Software [1.4]

T.NETWORK\_ATTACK

O.MANAGEMENT

FPT\_TUD\_EXT.1

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

SFR Catalog

Steps Recorder - Recording View
Page Record
Stop Record
Add Comment

Filter

Threats & Assumptions

Select ThreatAssumption
T.NETWORK\_ATTACK
ThreatAssumption Options: 2

Objectives

Select Objective
O.MANAGEMENT
Objective Options: 3

SFRs

Select SFR
SFR ID: FPT\_TUD\_EXT.1
SFR Options: 3

PPs

Select PP
Application Software [1.4]
General Purpose Operating System [4.3]
PP Options: 0

CLEAR ALL FILTERS

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

SFR Catalog

Filter

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: 9

CLEAR ALL FILTERS

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

SFR Catalog

Steps Recorder - Recording Now  
Page Record Stop Record Add Comment

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 Control:  
Select SFR  
FPT\_TUD\_EXT.1  
SFR Options: 9

PPs

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

CLEAR ALL FILTERS

Results

Application Software [1.4]

T.NETWORK\_ATTACK  
O.MANAGEMENT  
FPT\_TUD\_EXT.1

General Purpose Operating System [4.3]

T.NETWORK\_ATTACK  
O.MANAGEMENT  
FPT\_TUD\_EXT.1



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

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 ID Name SFR Condition

Select SFR

FPT.TUD\_EXT.1

SFR Options: 9

PPs

Select PPT

Application Software [1.4]

General Purpose Opera...

PP Options: 0

CLEAR ALL FILTERS

Results

Application Software [1.4]

T.NETWORK\_ATTACK

String XML

<description xmlns="https://nmap-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

String XML

<description xmlns="https://nmap-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."

SFR Catalog

Stop Recorder · Recording Mode · Page Record · Stop Record · Add Comment

Filter

Threats & Assumptions

Select ThreatAssumption  
T.NETWORK\_ATTACK

ThreatAssumption Options: 2

Objectives

Select Objective  
O.MANAGEMENT

Objective Options: 2

SFRs

Search By  
SFR ID Name · SFR Condition

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

Results

Application Software [1.4]

T.NETWORK\_ATTACK

String XML

<description xmlns="https://nlap-ccavs.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

String XML

<description xmlns="https://nlap-ccavs.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

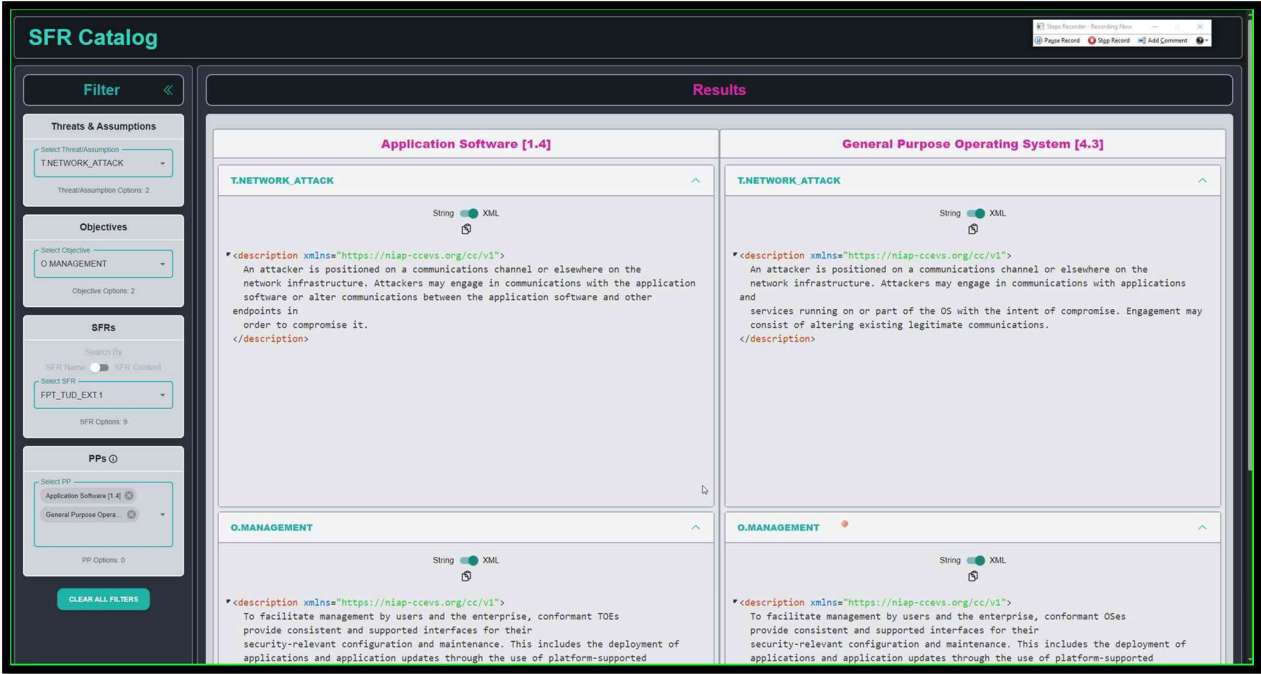
String XML

<description xmlns="https://nlap-ccavs.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."



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

The screenshot displays the 'SFR Catalog' application interface. On the left is a sidebar with search and filter options. The main area consists of two side-by-side panels, each showing a list of items with expandable sections.

**Sidebar:**

- Search By:** SFRs, Items, SFRs, Content
- Select SFR:** FPT\_TUD\_EXT.1
- SFR Options:** 9
- PPs:** 0
- Select PP:** Application Software (1 of 1), General Purpose Opera...
- PP Options:** 0
- CLEAR ALL FILTERS**

**Main Panels:**

Each panel displays a list of items. The first item in each list is expanded, showing a section titled 'O.MANAGEMENT'. The content of this section is as follows:

String ☒ XML

**O.MANAGEMENT**

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.

**Footer:**

FPT\_TUD\_EXT.1

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

The screenshot displays the 'SFR Catalog' application interface, which is divided into a left sidebar and a main content area. The sidebar contains search filters for SFRs and PPs, with a 'CLEAR ALL FILTERS' button at the bottom. The main content area is split into two identical panels, each showing a list of SFRs. The first SFR, 'FPT\_TUD\_EXT.1', is expanded, revealing its description and XML content. The description text is: '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.' The XML content is: '<description xmlns="https://niap-cc-evs.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>'. The interface includes a top navigation bar with a 'Steps Recorder' button and a bottom status bar with 'Page Record', 'Page Review', and 'Add Comment' buttons.

**SFR Catalog**

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**

**</description>**

**O.MANAGEMENT**

String XML

**<description xmlns="https://niap-cc-evs.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>**

**FPT\_TUD\_EXT.1**

String XML

**</description>**

**O.MANAGEMENT**

String XML

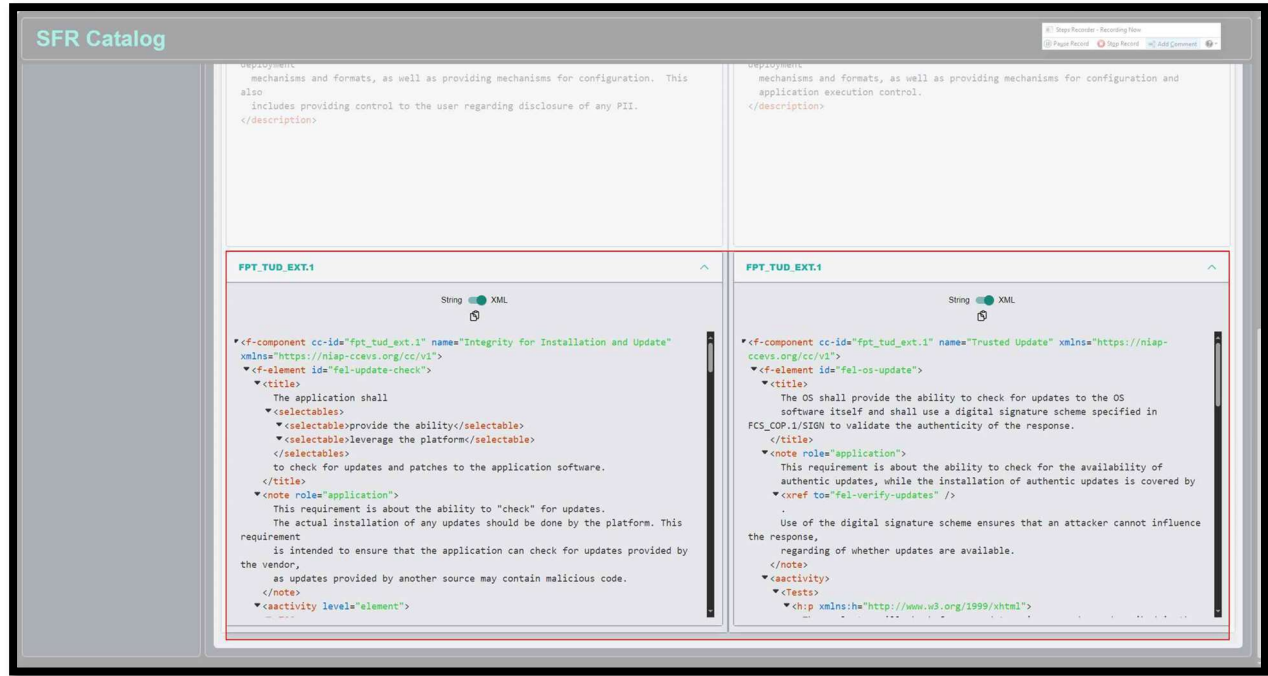
**<description xmlns="https://niap-cc-evs.org/cc/v1">**  
To facilitate management by users and the enterprise, conformant OSes provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through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

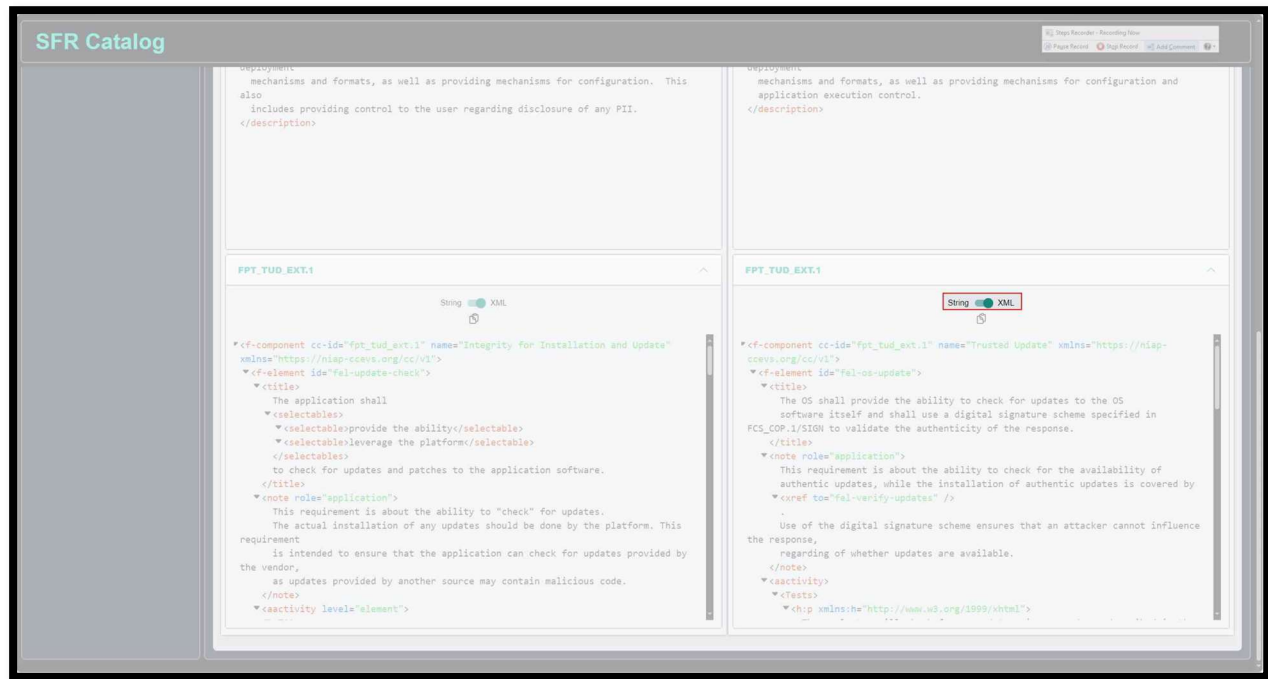
String XML

Steps Recorder - Recording Now  
Page Record Page Review Add Comment

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



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



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

**SFR Catalog**

Deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII.

**FPT\_TUD\_EXT.1**

String XML

**Integrity for Installation and Update**

The application shall

- provide the ability to
- Leverage the platform to

to check for updates and patches to the application software.

**Trusted Update**

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.

This requirement is about the ability to check for the availability of authentic updates, while the installation of authentic updates is covered by

Use of the digital signature scheme ensures that an attacker cannot influence the response, regarding of whether updates are available.



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

SFR Catalog

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://nisp-cc-evs.org/cc/v1"><f-element id="fel-update-check"><title>The application shall</title><selectables><selectable>provide the ability</selectable><selectable>leverage the platform</selectable></selectables></f-element><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><activity level="element">

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

FPT\_TUD\_EXT.1

String XML

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 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."**

The screenshot displays the SFR Catalog application interface. At the top, a header bar contains the title "SFR Catalog" on the left and a navigation menu on the right with options: "Steps Recorder", "Recording View", "Page Record", "Step Record", "Add Comment", and a user profile icon. The main content area is divided into two vertical panels, each showing a different XML document titled "FPT\_TUD\_EXT.1".

The left panel displays the XML content for "FPT\_TUD\_EXT.1" with a "String" and "XML" icon. The XML content includes a description and a component definition for "Integrity For Installation and Update".

The right panel displays the XML content for "FPT\_TUD\_EXT.1" with a "String" and "XML" icon. The XML content includes a description and a component definition for "Trusted Update". A red box highlights a "Copy" icon (a document with a plus sign) located above the XML content in the right panel.

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

Select SFR

FAU\_GEN.1

SFR Options: 368

PPs

Select PP

CC Part 2 [2022]

Mobile Device [3.3]

PP Options: 3

CLEAR ALL FILTERS

Results

CC Part 2 [2022]

FAU\_GEN.1

Mobile Device [3.3]

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."**

**SFR Catalog**

**Filter**

Threats & Assumptions  
Select Threat/Assumption  
Threat/Assumption Options: 13

Objectives  
Select Objective  
Objective Options: 7

SFRs  
Search By  
TSF ID:  TSF ID:   
Select SFR  
FAU\_GEN.1  
SFR Options: 302

PPs  
Select PPs  
CC Part 2 [2022]  
Mobile Device [3.3]  
PP Options: 9  
**CLEAR ALL FILTERS**

**Results**

**CC Part 2 [2022]**

**FAU\_GEN.1**

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

**Mobile Device [3.3]**

**FAU\_GEN.1**

String XML

VSX/10

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

**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."**

The screenshot displays the 'SFR Catalog' application interface. On the left is a 'Filter' sidebar with sections for 'Threats & Assumptions', 'Objectives', 'SFRs', and 'PPs'. The 'SFRs' section shows 'FAU\_GEN.1' selected. The 'PPs' section shows 'CC Part 2 [2022]' and 'Mobile Device [3.3]' selected. The main 'Results' area is split into two panels. The left panel, titled 'CC Part 2 [2022]', shows the 'FAU\_GEN.1' SFR details, including its description and a reference to 'Figure 9'. The right panel, titled 'Mobile Device [3.3]', shows the same 'FAU\_GEN.1' SFR details but with an XML snippet. A red box highlights a circular icon with a '1' inside, located next to the 'FAU\_GEN.1' header in the right panel. This icon indicates that a TD is recorded for this SFR within the selected PP.

**SFR Catalog**

Filter

Threats & Assumptions

Select Threat/Assumption

Threat/Assumption Options: 12

Objectives

Select Objective

Objective Options: 7

SFRs

Search SFR

100% Visible 100% Visible

Select SFR

FAU\_GEN.1

SFR Options: 368

PPs

Select PP

CC Part 2 [2022]

Mobile Device [3.3]

PP Options: 3

CLEAR ALL FILTERS

**Results**

**CC Part 2 [2022]**

**FAU\_GEN.1**

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

**Mobile Device [3.3]**

**FAU\_GEN.1**

String XML

VIEW TO

```
<cf-component cc-id="fau_gen.1" name="Audit Data Generation" xmlns="https://nmap-ccv3s.org/cc/v1">
  <cf-element id="fai-audit-gen">
    <title>
      The TSF shall be able to generate an audit record of the following auditable events:
    </title>
    <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>
    <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>
  </cf-element>
</cf-component>
```

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

The screenshot displays the SFR Catalog application interface. On the left is a 'Filter' sidebar with sections for 'Threats & Assumptions' (13 options), 'Objectives' (7 options), 'SFRs' (10 options, including 'FAU\_GEN.1'), and 'PPs' (3 options, including 'CC Part 2 [2022]' and 'Mobile Device [3.3]'). A 'CLEAR ALL FILTERS' button is at the bottom of the sidebar. The main area is titled 'Results' and contains two panels. The left panel, 'CC Part 2 [2022]', shows 'FAU\_GEN.1' with a description of security audit data generation and a 'view to' button. The right panel, 'Mobile Device [3.3]', shows 'FAU\_GEN.1' with a description of audit data generation and a 'view to' button. Both panels include a 'view to' button with a magnifying glass icon.

**SFR Catalog**

**Filter**

**Threats & Assumptions**

Select Threat/Assumption

Threat/Assumption Options: 13

**Objectives**

Select Objective

Objective Options: 7

**SFRs**

Search for

Selected SFR

FAU\_GEN.1

SFR Options: 10

**PPs**

Selected PP

CC Part 2 [2022]

Mobile Device [3.3]

PP Options: 3

**CLEAR ALL FILTERS**

**Results**

**CC Part 2 [2022]**

**FAU\_GEN.1**

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

**Mobile Device [3.3]**

**FAU\_GEN.1**

String XML

**view to**

```
<cf-component cc-id="fau_gen.1" name="Audit Data Generation" xmlns="https://niap-csrc.org/cc/v1">
  <cf-element id="fai-audit-gen">
    <title>
      The TSF shall be able to generate an audit record of the following auditable
      events:
    </title>
    <htm:bn 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>
    </htm:ol>
  </cf-element>
</cf-component>
```

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

The screenshot displays the SFR Catalog application interface. On the left, there is a sidebar with filter options under the heading "Filter". The filters include "Threats & Assumptions" (Select Threat/Assumption, Threat/Assumption Options: 13), "Objectives" (Select Objective, Objective Options: 7), "SFRs" (Search By: TSF, Mitigation, SFR Control; Search SFR: FAU\_GEN.1; SFR Options: 368), and "PPs" (Select PP: CC Part 2 [2022], Mobile Device [3.3]; PP Options: 3). A "CLEAR ALL FILTERS" button is at the bottom of the sidebar.

The main area is titled "Results" and shows two columns: "CC Part 2 [2022]" and "Mobile Device [3.3]". The "Mobile Device [3.3]" column is active, showing "FAU\_GEN.1" with a magnifying glass icon. A modal window is open over the "FAU\_GEN.1" entry, titled "TD: 0724". The modal contains the following text:

Publication Date: 2023-02-24  
SFR Components: FAU\_GEN.1

Text:

FAU\_GEN.1.1 in PP\_MDPE\_V3.3 is updated as follows, with yellow highlight indicating format changes to add indices/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 event in Table 3. (assignment: other auditable events derived from this Protection Profile); no additional auditable events)]**

The modal also includes a "CLOSE" button at the bottom right. The background shows XML code snippets, including "Audit Data Generation" and "create an audit record of the following auditable".

**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."**

