Cyber Security Toolbox

User Manual

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

Table of contents

Table of figures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

1 Introduction

The SPHINX Cyber Security Toolbox (CST) component enables SPHINX users to select the security services that best match their needs, to use within the SPHINX ecosystem. It allows users to *plug* cybersecurity services into their existing connectivity services and configure/adapt them according to their security needs. In this respect, and upon receiving the users' requests through a cybersecurity tailored questionnaire, CST jointly examines the available security functions/services that are part of the Toolbox and produces a suggestion based on the available cybersecurity services. Moreover, the CST lists all the available attack patterns that exist within the SPHINX environment by utilizing the Knowledge Base (KB), along with the course(s) of action for every attack pattern, should they exist.

1.1.1 Installation/Deployment

1.1.1.1 Prerequisites and hardware

- Minimum Requirements
  - CPU: 1-2Cores
  - RAM: 256MB
  - GPU: Not needed
  - SPACE: 150 MB

1.1.1.2 Deployment with Docker

The CST can be deployed on docker-compose. The deployment YAML is provided in the component's GIT repository.

1.1.1.3 Deployment with Kubernetes

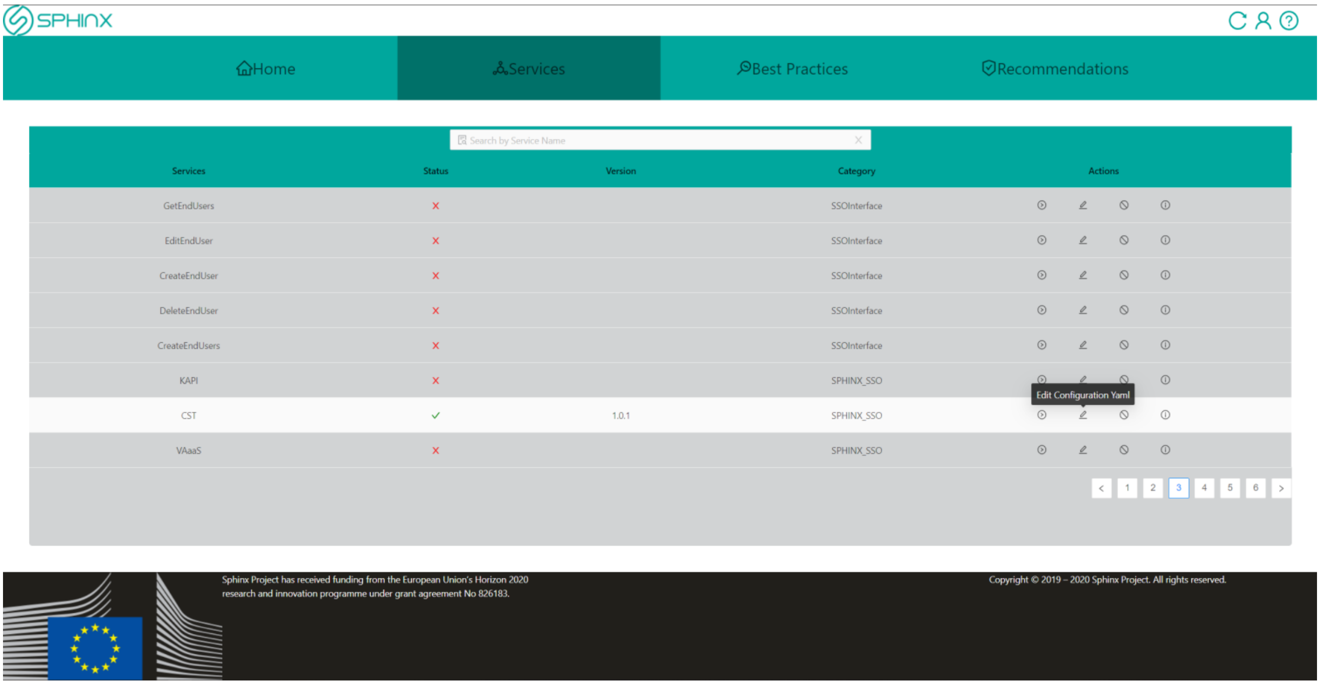
The CST can be deployed on docker-compose. The deployment YAML is provided in the component's GIT repository.

1.1.2 Operation and Maintenance

The basic examples illustrate the interaction between the Service Manager (SM) and CST by depicting all the existing services and relevant information about them, while also utilizing the functionalities integrated to CST in order to edit/deploy/delete a service from the Common Integration Platform (CIP).

1.1.2.1 Basic Examples

For the 1st **basic example**, the listing of all of the cybersecurity services that exist within the SM is displayed to the "**Services"** component that is found in the horizontal top bar. For the test case, select one of the listed services and from the "**actions"** column select the **2nd** one that will allow us to preview and edit the YAML deployment file (Figure 1).



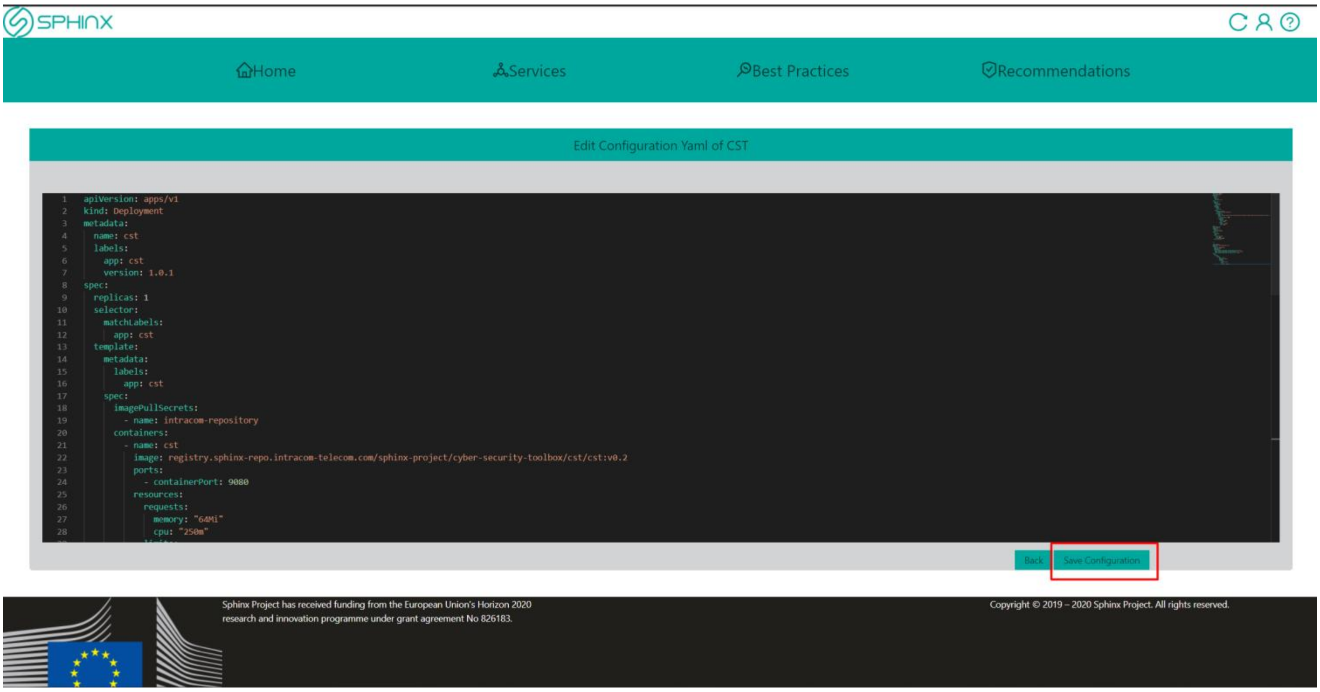
Services	Status	Version	Category	Actions
GetEndUsers	✗		SSOInterface	
EditEndUser	✗		SSOInterface	
CreateEndUser	✗		SSOInterface	
DeleteEndUser	✗		SSOInterface	
CreateEndUsers	✗		SSOInterface	
KAPI	✗		SPHINX_SSO	
CST	✓	1.0.1	SPHINX_SSO	
VAaaS	✗		SPHINX_SSO	

Sphinx Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183.

Copyright © 2019 – 2020 Sphinx Project. All rights reserved.

Figure 1 Edit Configuration YAML

To save the configuration click the "**Save Configuration"** button (Figure 2).



Edit Configuration Yaml of CST

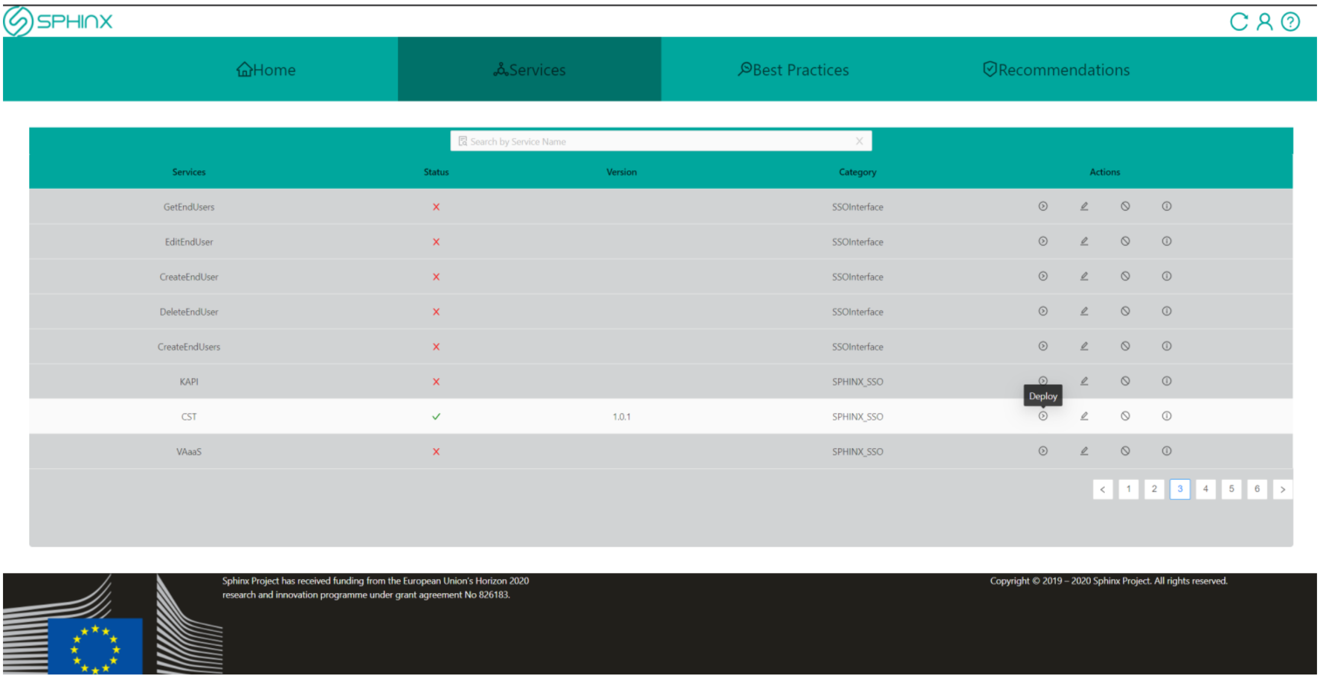
```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: cst
  labels:
    app: cst
    version: 1.0.1
spec:
  replicas: 1
  selector:
    matchLabels:
      app: cst
  template:
    metadata:
      labels:
        app: cst
    spec:
      imagePullSecrets:
        - name: intracom-repository
      containers:
        - name: cst
          image: registry.sphinx-repo.intracom-telecom.com/sphinx-project/cyber-security-toolbox/cst/cst:v0.2
          ports:
            - containerPort: 9080
          resources:
            requests:
              memory: "64Mi"
              cpu: "250m"
```

Sphinx Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183.

Copyright © 2019 – 2020 Sphinx Project. All rights reserved.

Figure 2 Save Configuration

A pop-up appears in the top middle of the screen to alert the user regarding the success or failure of the process. By clicking the "**Back"** button a redirection back to the "**Services"** tab is initiated. From the "**actions"** column select the **1st** one to be redirected to the CIP deployment component (Figure 3).



Services	Status	Version	Category	Actions
GetEndUsers	✗		SSOInterface	⊙ ✎ ⊘ ⓘ
EditEndUser	✗		SSOInterface	⊙ ✎ ⊘ ⓘ
CreateEndUser	✗		SSOInterface	⊙ ✎ ⊘ ⓘ
DeleteEndUser	✗		SSOInterface	⊙ ✎ ⊘ ⓘ
CreateEndUsers	✗		SSOInterface	⊙ ✎ ⊘ ⓘ
KAPI	✗		SPHINX_SSO	⊙ ✎ ⊘ ⓘ
CST	✓	1.0.1	SPHINX_SSO	⊙ ✎ ⊘ ⓘ
VAaaS	✗		SPHINX_SSO	⊙ ✎ ⊘ ⓘ

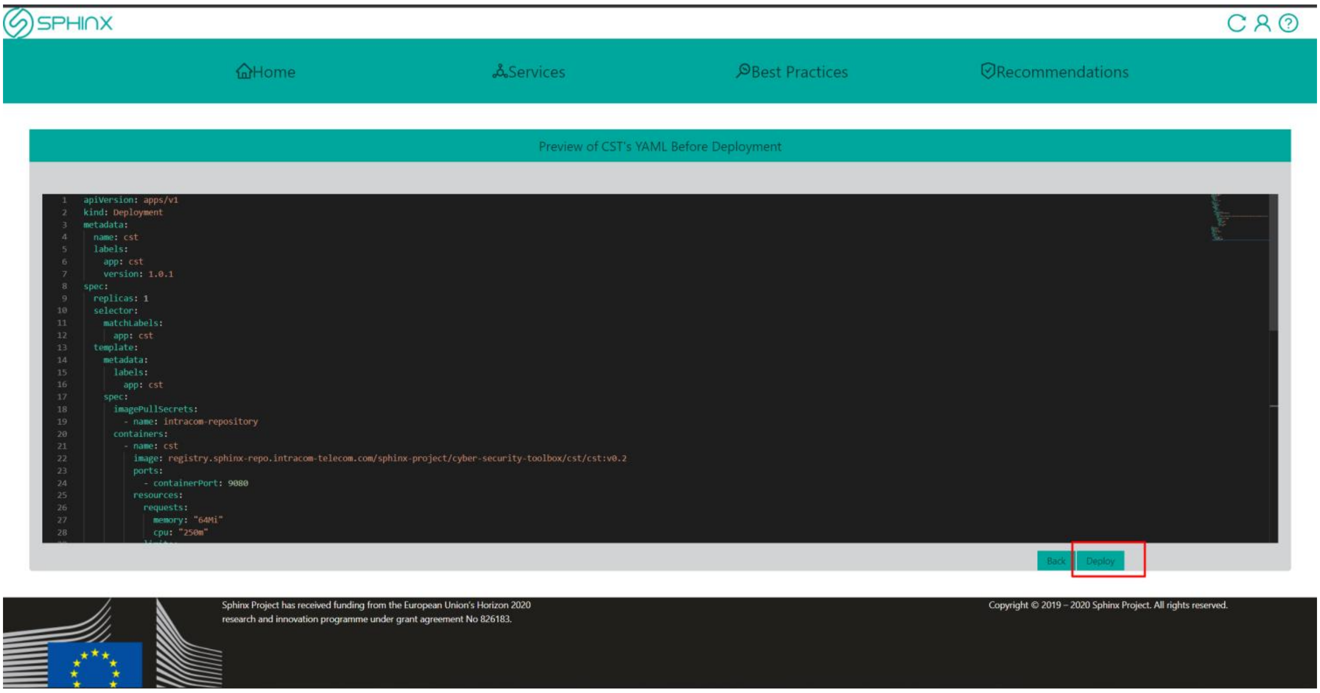
< 1 2 3 4 5 6 >

Sphinx Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183.

Copyright © 2019 – 2020 Sphinx Project. All rights reserved.

Figure 3 **Deploy Button**

There the user is able to preview the saved YAML file but not edit it. By pressing the "**Deploy**" button the deployment of the service to the CIP is initiated (Figure 4).



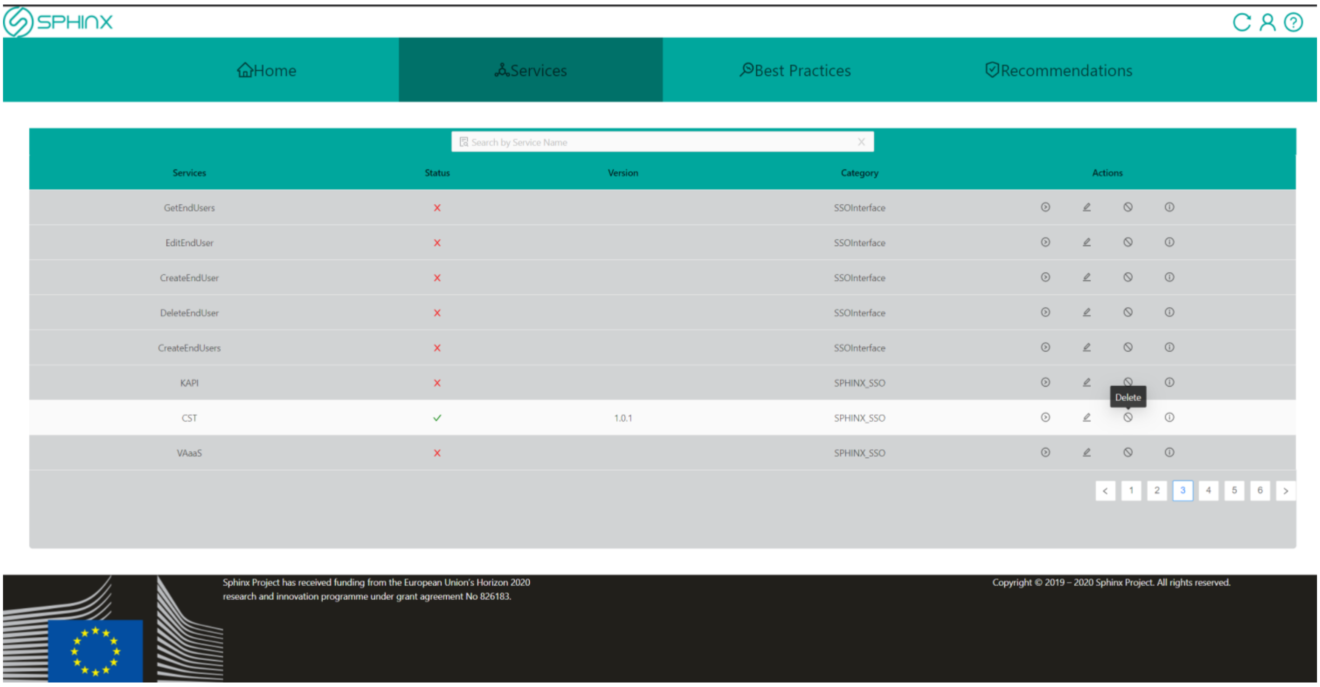
Preview of CST's YAML Before Deployment

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: cst
  labels:
    app: cst
    version: 1.0.1
spec:
  replicas: 1
  selector:
    matchLabels:
      app: cst
  template:
    metadata:
      labels:
        app: cst
    spec:
      imagePullSecrets:
        - name: intracom-repository
      containers:
        - name: cst
          image: registry.sphinx-repo.intracom-telecom.com/sphinx-project/cyber-security-toolbox/cst/cst:v0.2
          ports:
            - containerPort: 9080
          resources:
            requests:
              memory: "64Mi"
              cpu: "250m"
```

Sphinx Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183.

Copyright © 2019 – 2020 Sphinx Project. All rights reserved.

Figure 4 **Deploy**



Services	Status	Version	Category	Actions
GetEndUsers	✗		SSOInterface	
EditEndUser	✗		SSOInterface	
CreateEndUser	✗		SSOInterface	
DeleteEndUser	✗		SSOInterface	
CreateEndUsers	✗		SSOInterface	
KAPI	✗		SPHINX_SSO	
CST	✓	1.0.1	SPHINX_SSO	
VAaaS	✗		SPHINX_SSO	

Sphinx Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183.

Copyright © 2019 – 2020 Sphinx Project. All rights reserved.

Figure 5 **Delete Deployment**

By clicking it a confirmation pop will appear, by clicking **“OK”** the request for deletion is send is. A pop-up appears in the top middle of the screen to alert us regarding the success or failure of the deletion.

1.1.2.2 Links with other Components

Link with the Service Manager: The service manager is tasked with providing the list of the cybersecurity services that are depicted in the CST component. Moreover, the SM is responsible for storing the YAML configuration files of the services, providing information regarding each service, and also providing the stored YAML back to the CST.

Link with the Knowledge Base: The Knowledge Base provides CST with attack patterns that have amassed, a detailed description of each attack pattern, and course(s) of action regarding each attack pattern. The CST is tasked with the illustration of the data in a user-friendly way.

Link with the Common Integration Platform (CIP): Through CST the user can interact with the CIP. The dashboard provides the means for the user to deploy, delete, check the version, check the status, and get information regarding the existing services.

1.1.2.3 Outcomes

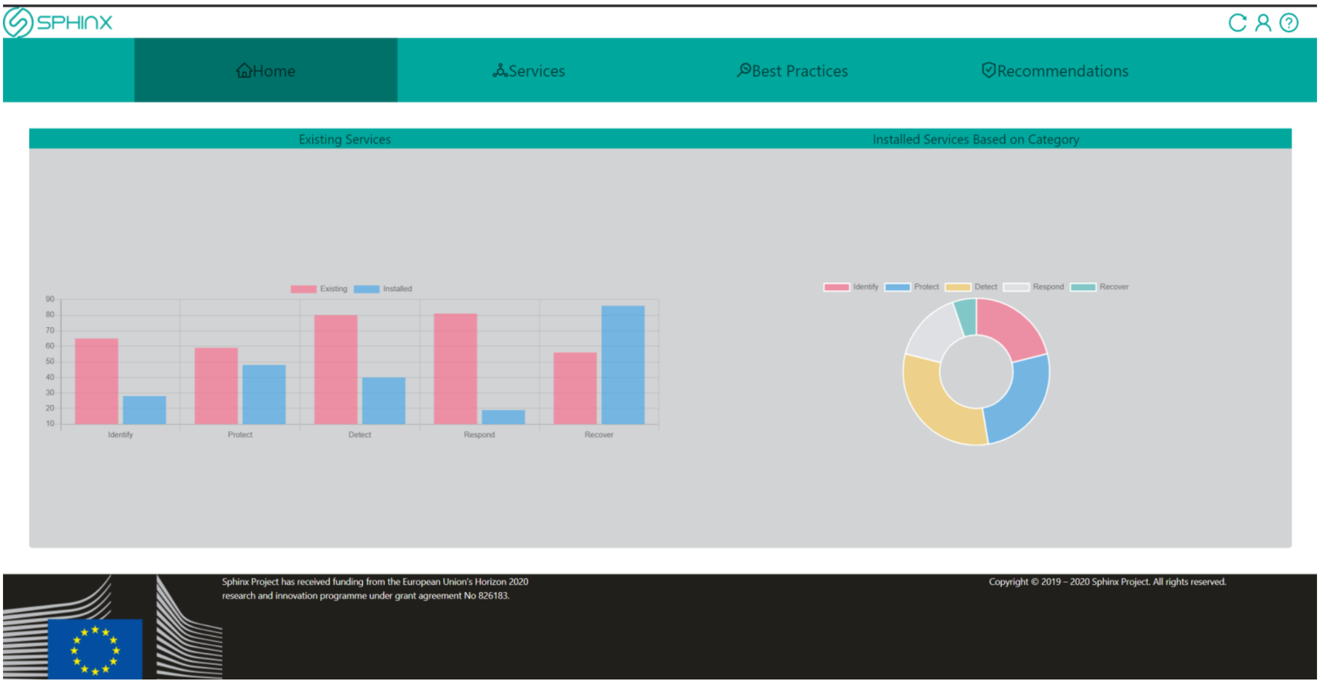
For the 1st **case example,** we expect a successful deployment of the service in the CIP. The deployment status and version of the service can then be seen in the **“Service”** tab (Figure 2). For the 2nd **case example, we** expect the successful deletion of the deployment from the CIP. The deployment status marked as X can then be seen in the **“Service”** tab (Figure 2).

1.1.2.4 Maintenance

N/A

1.1.3 Application UI presentation

Figure 1 depicts the Home tab of the CST, wherein users can see Existing services within the SPHINX ecosystem categorized based on the cyber-security lifecycle steps, and the amount of active/installed services based on these categories.

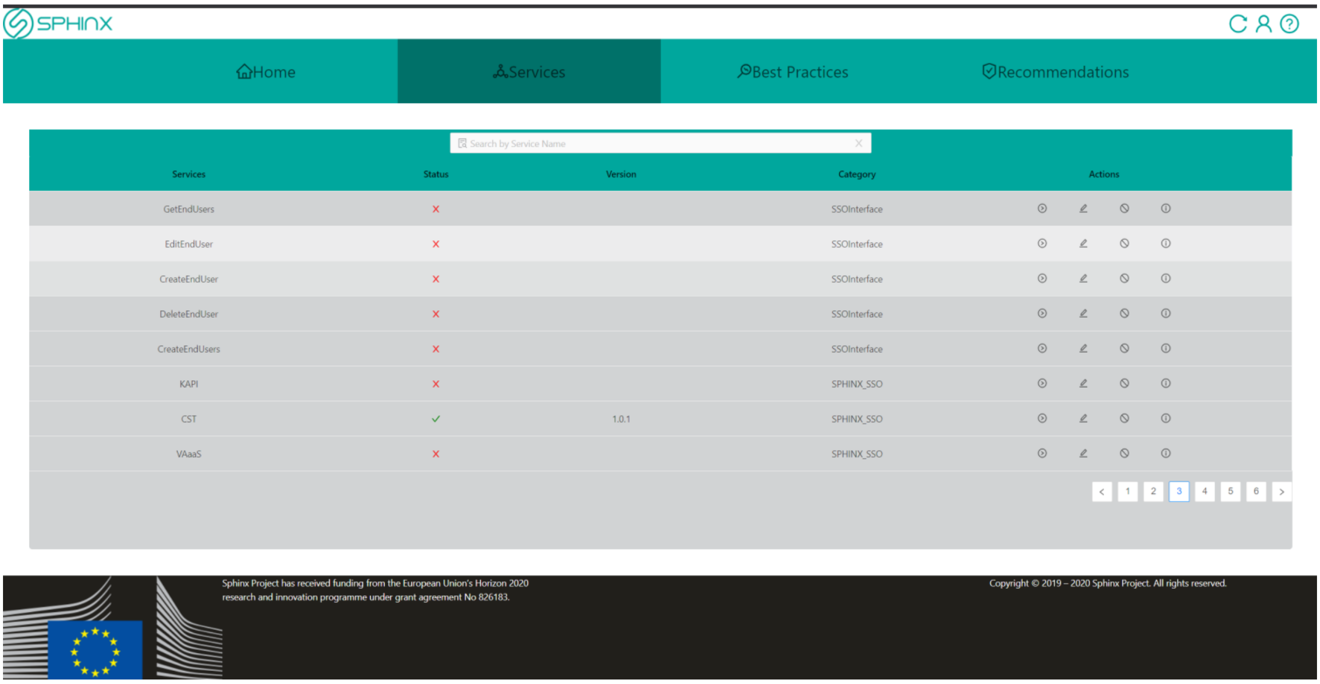


Sphinx Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183.

Copyright © 2019 – 2020 Sphinx Project. All rights reserved.

Figure 6 **Home tab**

The Services tab, allows the user to scroll through all of the existing services, their status, version, category, and interacts with them through the actions bar (Deploy the service, edit configuration file of the service, delete the service from the CIP, and information regarding the service). The Service tab is depicted in Figure 2.



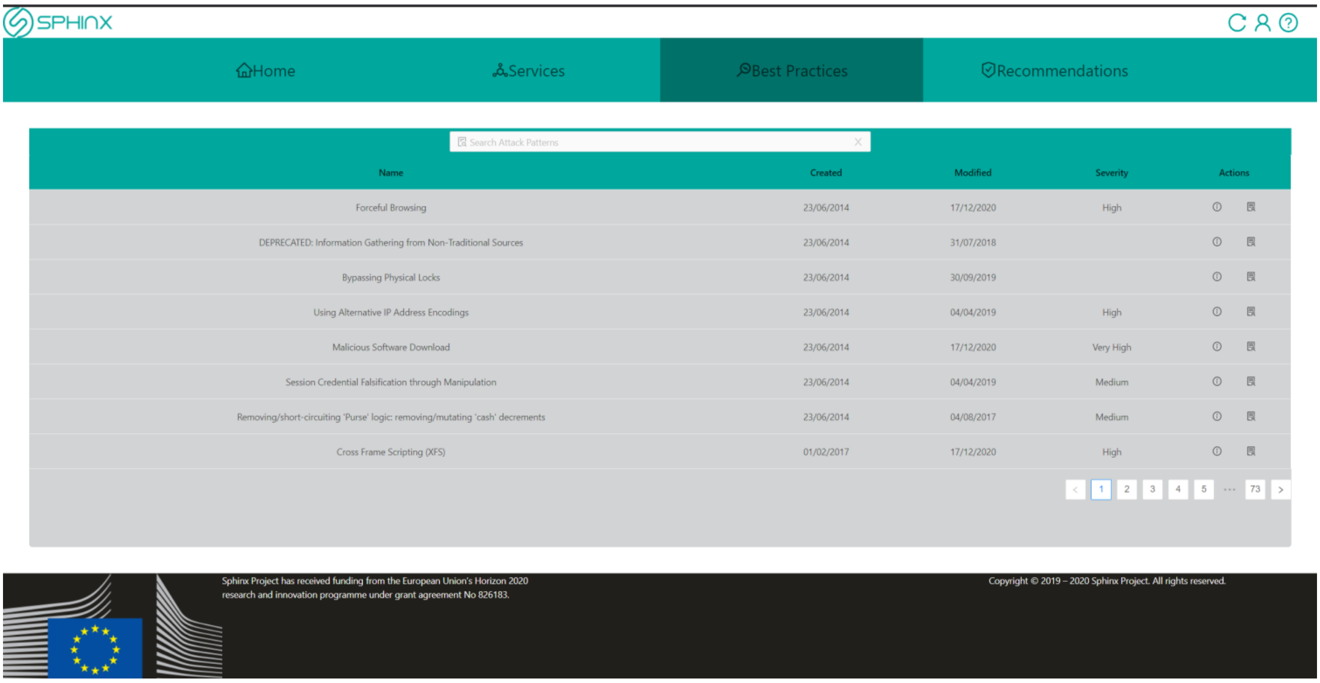
Services	Status	Version	Category	Actions
GetEndUsers	✗		SSOInterface	⊙ ✎ ⊘ ⓘ
EditEndUser	✗		SSOInterface	⊙ ✎ ⊘ ⓘ
CreateEndUser	✗		SSOInterface	⊙ ✎ ⊘ ⓘ
DeleteEndUser	✗		SSOInterface	⊙ ✎ ⊘ ⓘ
CreateEndUsers	✗		SSOInterface	⊙ ✎ ⊘ ⓘ
KAPI	✗		SPHINX_SSO	⊙ ✎ ⊘ ⓘ
CST	✓	1.0.1	SPHINX_SSO	⊙ ✎ ⊘ ⓘ
VAaaS	✗		SPHINX_SSO	⊙ ✎ ⊘ ⓘ

Sphinx Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183.

Copyright © 2019 – 2020 Sphinx Project. All rights reserved.

Figure 7 **Services Tab**

The Best Practices tab contains the amassed knowledge of the SPHINX ecosystem. Within this section, the user can scroll through numerous attack patterns and collect information regarding each attack pattern (date created, when was last modified, severity of the attack pattern, description of the attack pattern, and course(s) of action listed for each specific attack pattern). The Best Practices tab is depicted in Figure 3.



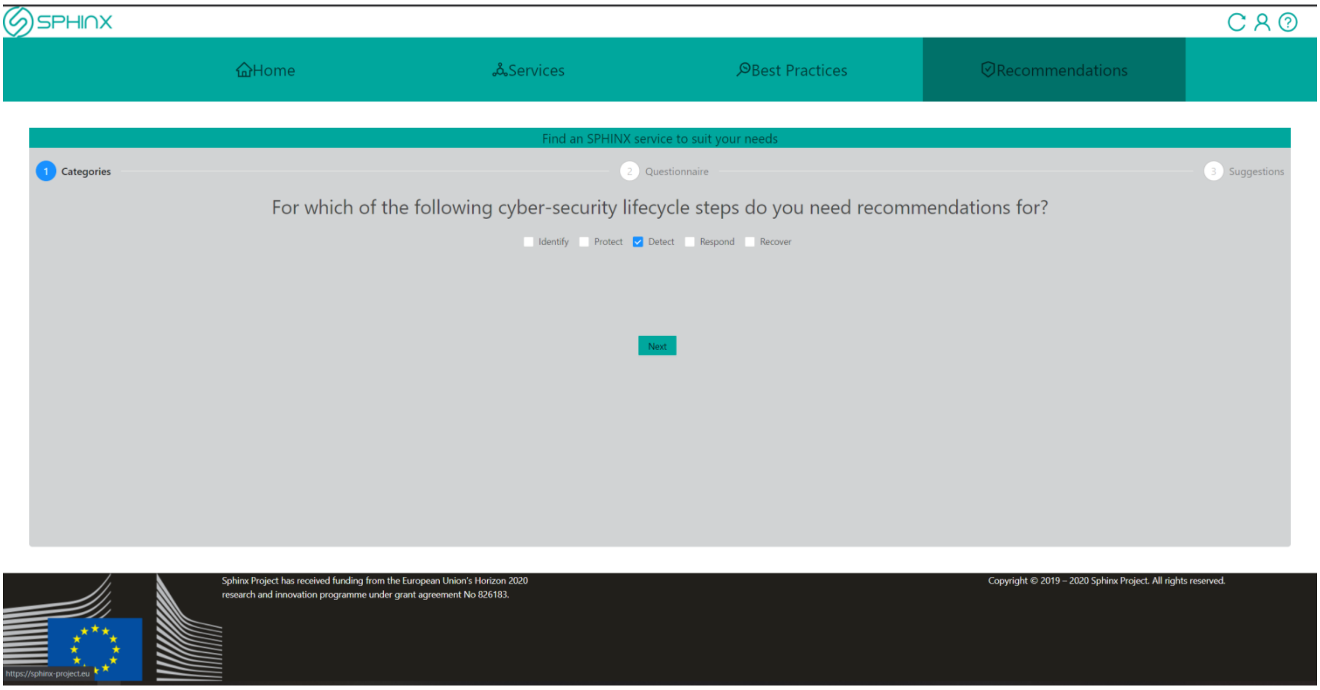
Name	Created	Modified	Severity	Actions
Forceful Browsing	23/06/2014	17/12/2020	High	ⓘ
DEPRECATED: Information Gathering from Non-Traditional Sources	23/06/2014	31/07/2018		ⓘ
Bypassing Physical Locks	23/06/2014	30/09/2019		ⓘ
Using Alternative IP Address Encodings	23/06/2014	04/04/2019	High	ⓘ
Malicious Software Download	23/06/2014	17/12/2020	Very High	ⓘ
Session Credential Falsification through Manipulation	23/06/2014	04/04/2019	Medium	ⓘ
Removing/short-circuiting 'Purse' logic: removing/mutating 'cash' decrements	23/06/2014	04/08/2017	Medium	ⓘ
Cross Frame Scripting (XFS)	01/02/2017	17/12/2020	High	ⓘ

Sphinx Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183.

Copyright © 2019 – 2020 Sphinx Project. All rights reserved.

Figure 8 **Best Practices Tab**

Through the Recommendations tab, users can get suggestions about cybersecurity services that they can install into their ecosystem through a questionnaire. It's a 3 steps process, wherein in the 1st step, users are prompted to choose one or more of the 5 existing cybersecurity categories, based on their selection the 2nd step presents them with more specific questions linked to services, leading to the suggested service in step 3. The Recommendations tab is illustrated below in Figure 4.



Find an SPHINX service to suit your needs

1 Categories — 2 Questionnaire — 3 Suggestions

For which of the following cyber-security lifecycle steps do you need recommendations for?

□ Identify □ Protect ☑ Detect □ Respond □ Recover

Sphinx Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183.

Copyright © 2019 – 2020 Sphinx Project. All rights reserved.

Figure 9 **Recommendations tab**