VB-Trend 2019

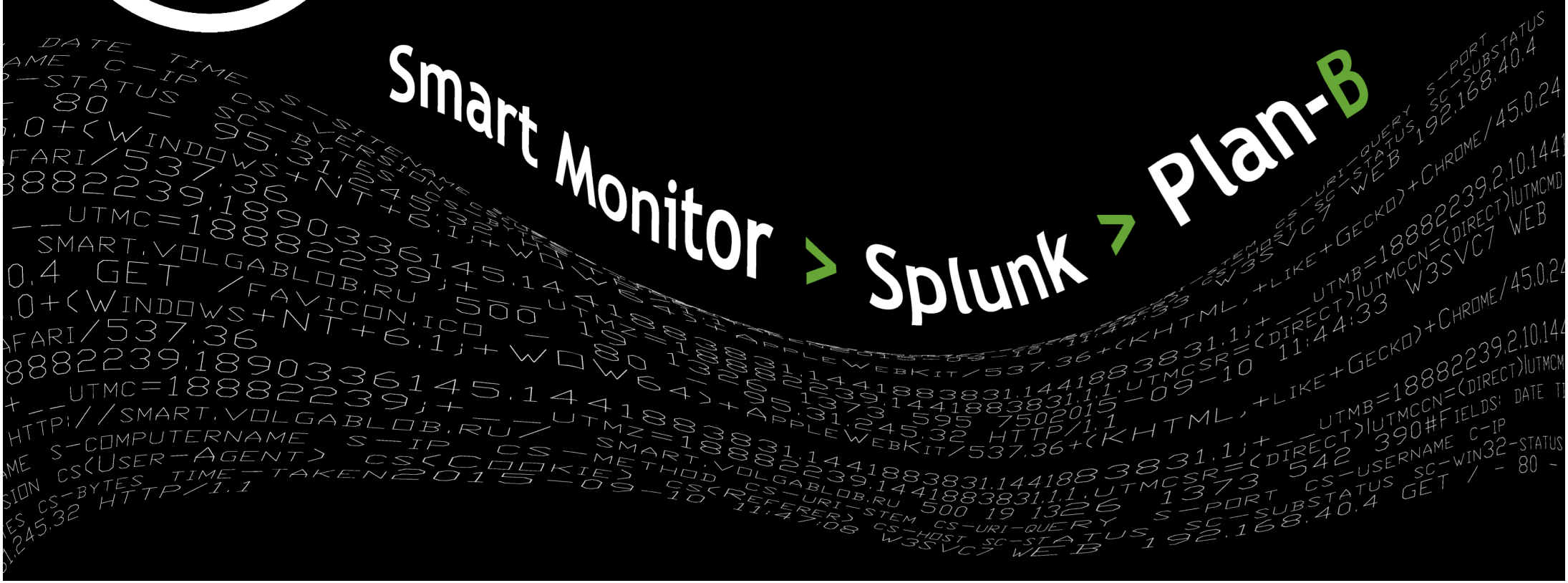
plan>b

VolgaBlob

Новый взгляд на автоматизацию оценки соответствия

Первое российское применения стандарта OSCAL

Smart Monitor > Splunk > Plan-B



Цели

- Автоматизация процессов оценки соответствия
- Привязка к требований к инфраструктуре с применением ресурсно-сервисных моделей
- Минимизация ошибок « человеческого фактора» оценки

OSCAL – стандарт для стандартов

VB-Trend 2019 plan>b VolgaBlob

Функция: Предоставление стандартов ИБ в машиночитаемом формате

Назначение: Автоматизация оценки соответствия различным требованиям ИБ

Преимущества: Гибкая настройка, быстрое внедрение

NIST
National Institute of Standards and Technology

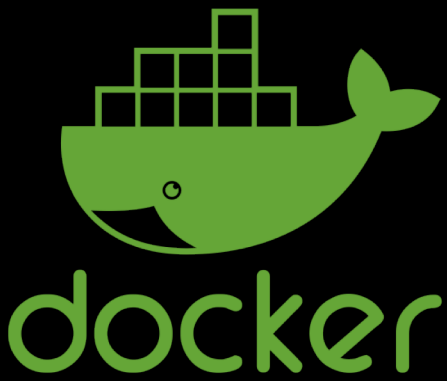
OSCAL: Применение

Федеральная программа управления рисками и авторизацией

Автоматизация оценки мер информационной безопасности поставщиков облачных услуг

Docker Enterprise

Автоматизация оценки соответствия для строго регулируемых инфраструктур



Архитектура OSCAL

VB-Trend 2019
plan>b
VolgaBlob

Каталог – представление в нотации OSCAL определенного стандарта ИБ.

Профиль – представление наборов контролей для систем различного уровня критичности или конкретных программ оценки безопасности.

Контроль – описание меры защиты, разработанный для соответствия набору определенных требований безопасности.

Структуры данных: Каталог [metadata]

VB-Trend 2019 plan>b VolgaBlob

```
"catalog": {
   "id": "uuid-47fdefdb-dc1a-4040-9f27-b517a16b06d2",
   "metadata": {
     "title": "NIST Special Publication 800-53…",
     "last-modified": "2019-09-23T14:19:17.649-04:00",
     "version": "2015-01-22",
     "oscal-version": "1.0.0-milestone1",
     "properties": {
       "keywords": "Assurance, computer security, FISMA…"
     },
     "links": [
       {
         "href": "#resource-pdf-sp-800-53r4",
         "rel": "alternate",
         "text": "NIST publication (PDF)"
       },
        …
     ],
     "roles": [
       {
         "id": "creator",
         "title": "Document creator"
       },
        …
],
```

Информация о стандарте

Ссылки на публикации

Указатели на создателей каталога

Структуры данных: Каталог [back-metter]

VB-Trend 2019 plan>b VolgaBlob

```
"back-matter": {
      "citations": [
        {
          "id": "ref001",
          "targets": "http://www.gpo.gov/fdsys/granule/CFR-2012-title5-vol2/CFR-
2012-title5-vol2-sec731-106/content-detail.html",
          "title": "5 C.F.R. 731.106"
        },
        ...
      ],
      "resources": [
        {
          "id": "resource-pdf-sp-800-53r4",
          "rlinks": {
            "href":
"https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf",
            "media-type": "application/pdf"
          }
        },
        ...
      ]
    }
```

Коллекция ссылок на ресурсы, связанных с публикацией

Структуры данных: Каталог

```
"groups": [
    {
      "id": "ac",
      "class": "family",
      "title": "Access Control",
      "controls": [
        {
          "id": "ac-1",
          "class": "SP800-53",
          "title": "Access Control Policy and Procedures",
          "parts": [
            {
              "id": "ac-1_smt",
              "name": "statement",
              "prose": "The organization:",
              "parts": [
                {
                  "id": "ac-1_smt.a",
                  "name": "item",
                  "properties": {
                    "label": "a."
                  },
                  "prose": "Develops, documents, and disseminates to {{ ac-1_prm_1 }}:"
```

Семейство контролей
группа контролей, отвечающая различным областям ИБ

Контроль
Контроль безопасности
(набор предъявляемых действий)

Требование
действие исполняемое в рамках контроля

Публикация каталога

FAMILY: ACCESS CONTROL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

   1. Access control policy [*Assignment: organization-defined frequency*]; and

   2. Access control procedures [*Assignment: organization-defined frequency*].

Профиль

```
{
  "profile": {
    "id": "uuid-13172679-d468-4a88-8d7f-3afdeffedff8",
    "metadata": {
      "title": "NIST Special Publication 800-53 Revision 4 LOW IMPACT BASELINE",
       ...
    },
    "imports": {
      "href": "#catalog",
      "include": {
        "id-selectors": [
          {
            "control-id": "ac-1"
          },
          ...
        ]
      }
    },
    "modify": {
      "alterations": [
        {
          "control-id": "ac-1",
          "additions": {
            "position": "starting",
            "properties": {
              "priority": "P1"
            }
          }
        }
        ...
      ]
    },
    "back-matter": {
      "resources": {
        "id": "catalog",
        "desc": "NIST Special Publication 800-53 Revision 4: Security and ...",
        …
```

Информация о профиле

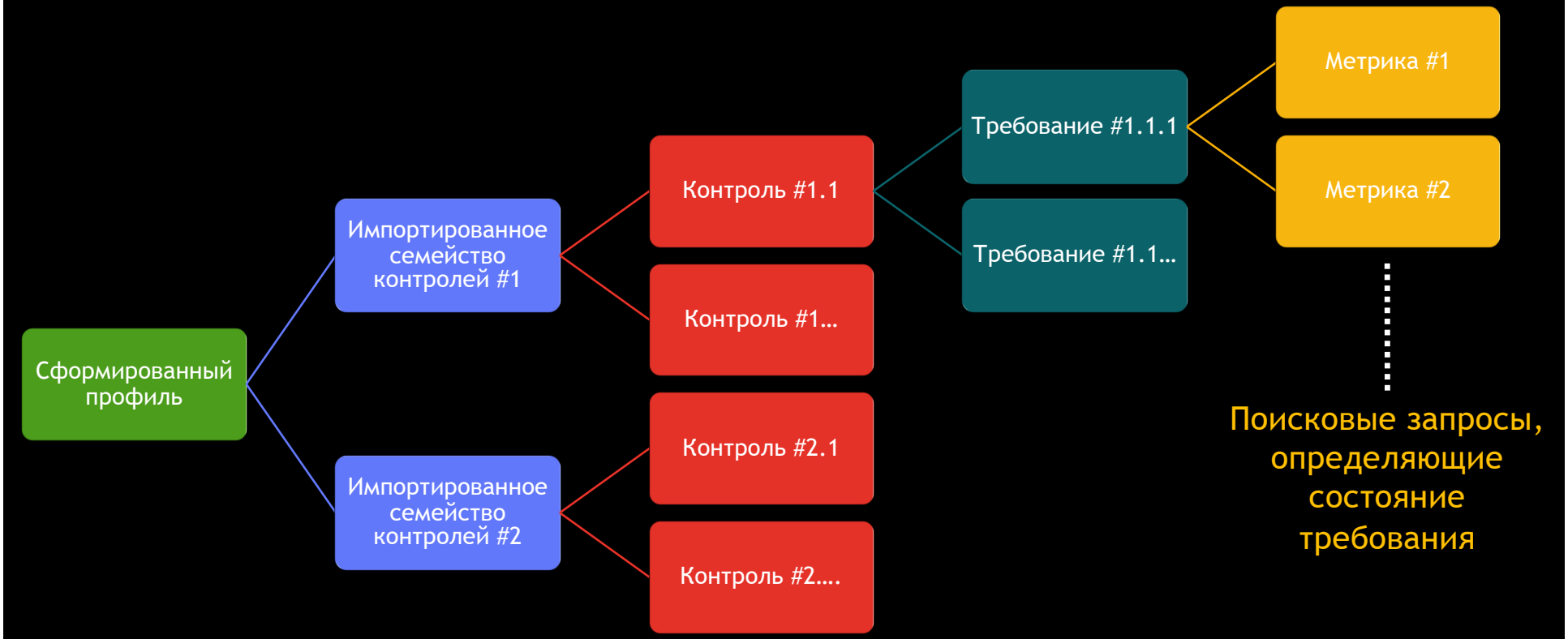
Импортирование необходимых контролей

Изменение параметров контролей

Ссылки на требуемые каталоги

VB-Trend 2019 plan>b VolgaBlob

Архитектура решения



Демо: OSCAL на платформе Smart Monitor

Результаты расследования

1. Конвертированы профили NIST в ресурсно-сервисные модели
2. Реализован профиль на базе контроля NIST с необходимыми контролями
3. Реализована оценка соответствия на базе стандарта ГОСТ Р 57580.1-2017
4. Выявлены проблемные объекты инфраструктуры, которые повлияли на общее состояние модели соответствия

Состояние проекта

- ✓ Реализовать систему соответствия на базе SmartMonitor с использованием нотации OSCAL
- ✓ Реализовать ресурсно-сервисные модели на базе Российского стандарта ГОСТ Р 57580.1-2017
- ❑ Реализовать модели для востребованных стандартов ИБ на рынке:
  1. ISO/IEC 27001
  2. N 152-ФЗ
  3. PCI DSS
  4. …

Опрос

VB-Trend 2019 plan>b VolgaBlob

Оценку на соответствие какому стандарту ИБ стоило бы автоматизировать в **первую очередь**?

- ❑ Стандарты серии **ISO 2700x** (Системы менеджмента информационной безопасности)
- ❑ Требования по защите персональных данных (ФЗ-152)
- ❑ Стандарт безопасности данных индустрии платежных карт **(PCI DSS)**
- ❑ Безопасность финансовых (банковских) операций **(ГОСТ Р 57580.2-2018)**
- ❑ Свой вариант

Поделитесь мнением, пожалуйста!

Результат

VB-Trend 2019 plan>b VolgaBlob

✓ Автоматизация процессов оценки соответствия

Использование профилей и каталогов OSCAL для формирование объективной модели соответствия

✓ Автоматизация создания ресурсно-сервисных моделей

Формирование ресурсно-сервисных моделей, используя конвертацию профилей OSCAL

✓ Минимизация человеческого фактора оценки

Использование систем регистрации и анализа машинных данных для оценки соответствия требованиям ИБ

Спасибо за внимание!

Вопросы?

VB-Trend 2019

plan>b

VolgaBlob