

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)**
Кафедра комплексной информационной безопасности
электронно-вычислительных систем (КИБЭВС)

**Разработка программного обеспечения для проверки
политик разграничения доступа к программным
интерфейсам**

Отчёт по производственной практике

Студент гр.777
Иванов И.И.

Руководитель практики
от предприятия
Старший инженер по качеству
С.Е. Солдатов

Руководитель практики
ассистент каф. КИБЭВС
А.И. Гуляев

Томск 2017

Информация о предприятии

- 15 лет на рынке
- Офисы в России,
Великобритании, Чехии
и других странах
- Портал SecurityLab.ru
- Научно-практический
форум Positive Hack
Days

POSITIVE TECHNOLOGIES

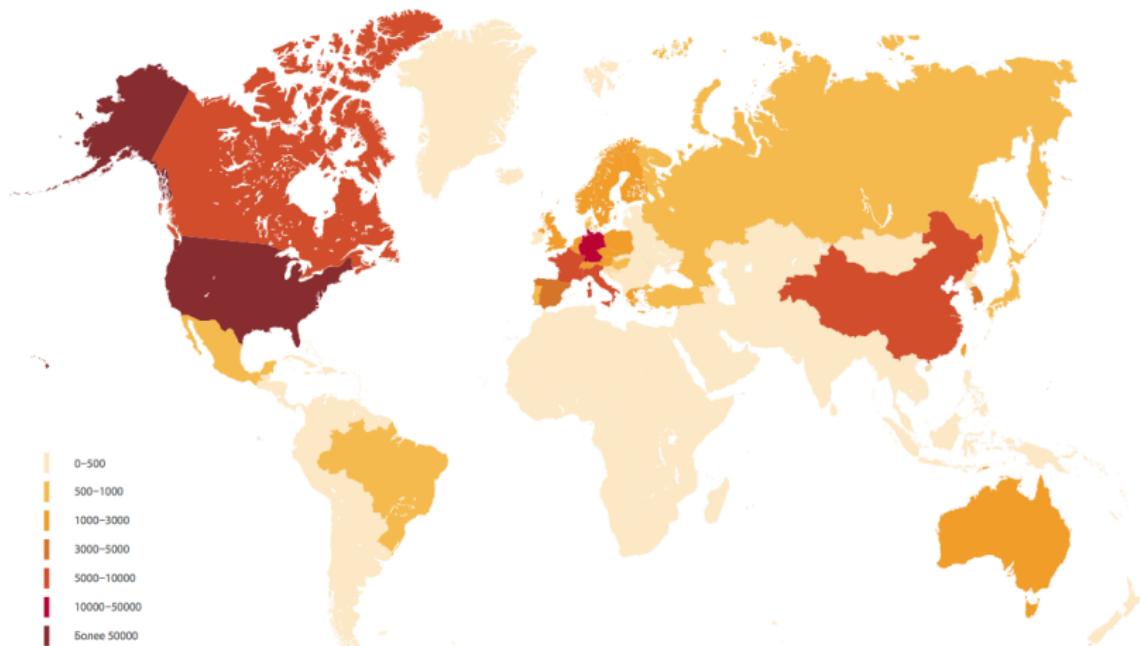
Информация о предприятии. Продукты

- MaxPatrol 8
- MaxPatrol SIEM
- PT Application Firewall
- PT Application Inspector
- PT MultiScanner
- XSpider
- PT ISIM

POSITIVE TECHNOLOGIES

Безопасность АСУ ТП

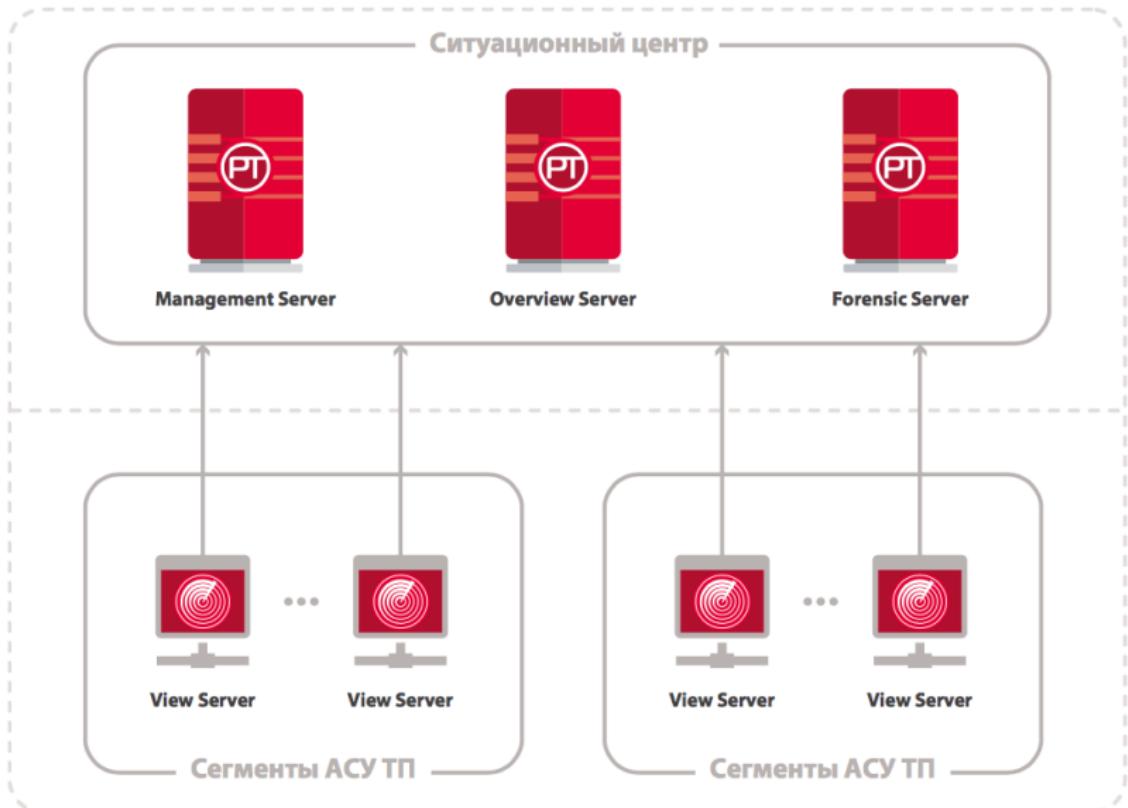
Количество компонентов АСУ ТП, доступных в сети
Интернет



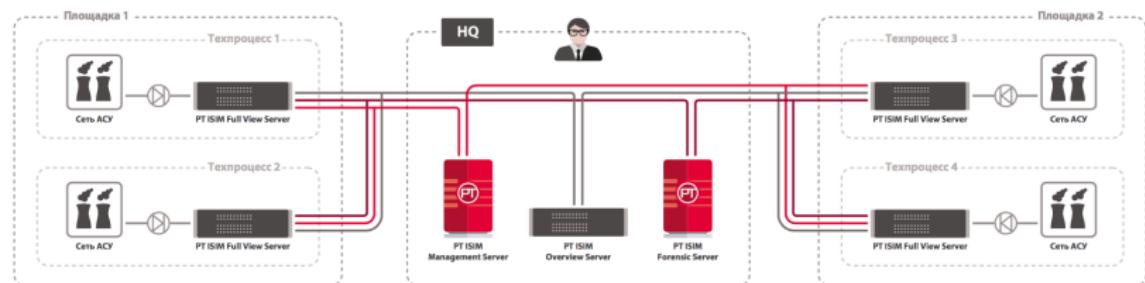
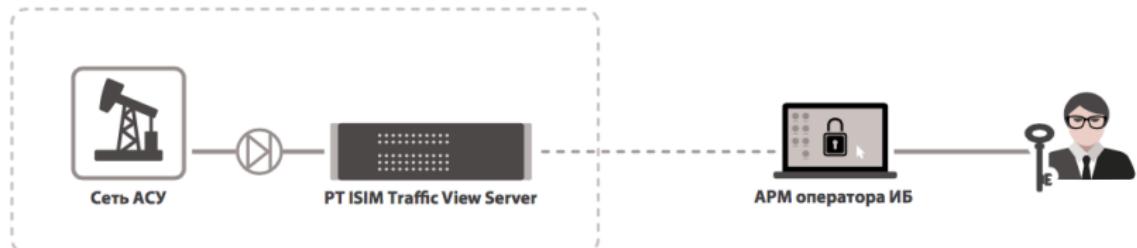
- Система управления инцидентами кибербезопасности
- Анализ копии трафика промышленной сети
- Выявление внутренних и внешних угроз



РТ ISIM. Компоненты



РТ ISIM. Примеры внедрения



Подходы к тестированию

- Функциональное тестирование
- Нагрузочное тестирование
- Стress-тестирование
- Компонентное тестирование
- Интеграционное тестирование
- Smoke-тестирование
- Регрессионное тестирование

Py.test

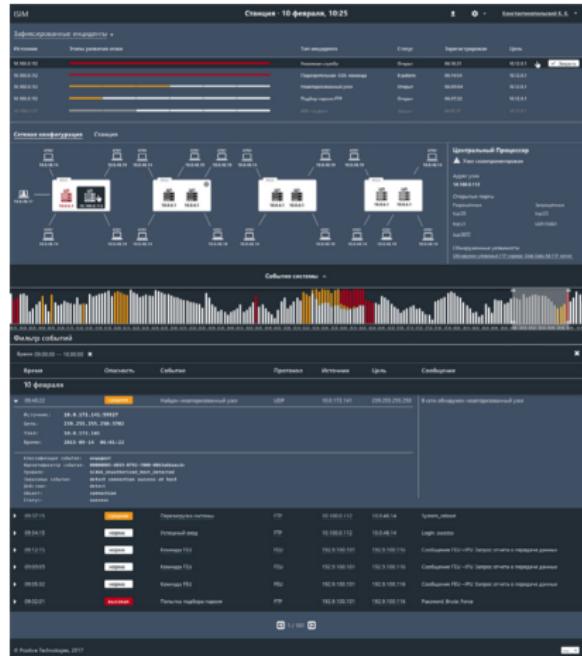
- Набор библиотек для автоматизации тестирования
- Подробный отчёт
- Параметризация тестов
- Метки для маркировки тестов
- Большое количество дополнительных модулей



pytest

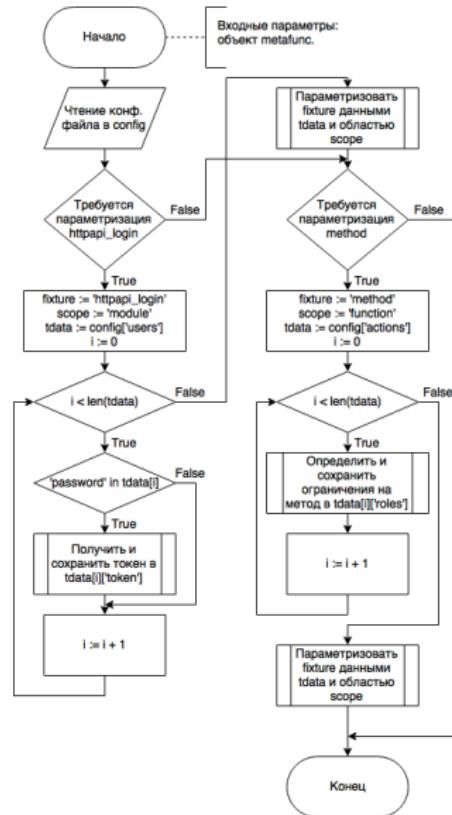
Httpapi

- Предоставляет интерфейс для доступа к компонентам PT ISIM
- Используется клиентской частью
- Используется другими серверами PT ISIM
- Работает при помощи методов HTTP
- Оперирует данными в формате JSON



Параметризация

- Количество методов httpapi не постоянно
- Пользователи и группы изменяются в процессе разработки
- Требуется отчёт о каждой проверке каждого метода httpapi для каждого пользователя



Конфигурационный файл

- Роли пользователей
- Пользователи
- Методы httpapi
- Ограничения методов

```
{  
    "method": "users.AllUsersHandler.get",  
    "description": "action_get_users",  
    "http_method": "get",  
    "url": "/users"  
},  
{  
    "method": "users.AllUsersHandler.post",  
    "description": "action_add_user",  
    "http_method": "post",  
    "url": "/users"  
},
```

```
"roles": [  
    {"_id": 0, "name": "anyone"},  
    {"_id": 1, "name": "anonymous"},  
    {"name": "operator"},  
    {"name": "iss"},  
    {"name": "administrator"}  
],
```

```
{  
    "login": "operator",  
    "name": "Operator",  
    "email": "operator@example.com",  
    "blocked": false,  
    "password": "████████",  
    "pin": "████████",  
    "roles": [  
        {"name": "operator"}  
    ]  
},
```

Описание программы

- Сопоставление методов httpapi с ограничениями прав
- Параметризация входных данных
- Тестирование методов httpapi

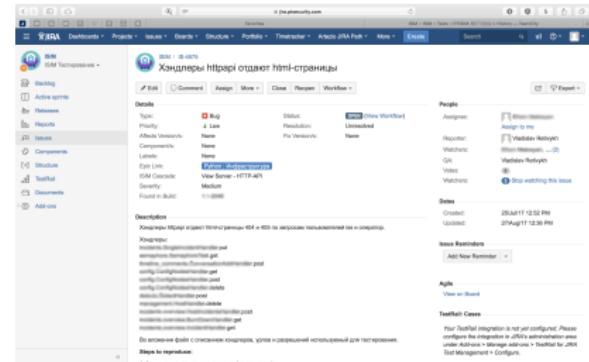


Работа программы

- Информация о работе программы в stdout
 - Определение некорректных ответов httpapi
 - Определение избыточных прав неавторизованного пользователя
 - Определение уже сделанных проверок в рамках других тестов

Результаты работы программы

- Получение html-страниц вместо документов JSON
 - Наличие недопустимых прав у неавторизованного пользователя
 - Отсутствие необходимых прав у ряда пользователей
 - Информирование разработчиков обо всех найденных ошибках при помощи JIRA



Непрерывная интеграция

- Интеграция в уже существующий набор автотестов
 - Непрерывная интеграция при помощи сервера TeamCity
 - Автоматическая проверка прав доступа для каждой новой сборки PT ISIM

Результаты

- Проведён анализ конфигурационных файлов РТ ISIM
- Разработано ПО для проверки политик разграничения доступа к программным интерфейсам
- Разработанное ПО интегрировано в существующую систему автотестов
- Выявлено 74 несоответствия фактических прав эталонным

Заключение

- Изучена СУИК РТ ISIM
- Получены навыки тестирования коммерческого ПО
- Получены навыки работы с py.test
- Разработанное в рамках практики ПО включено в процесс разработки РТ ISIM