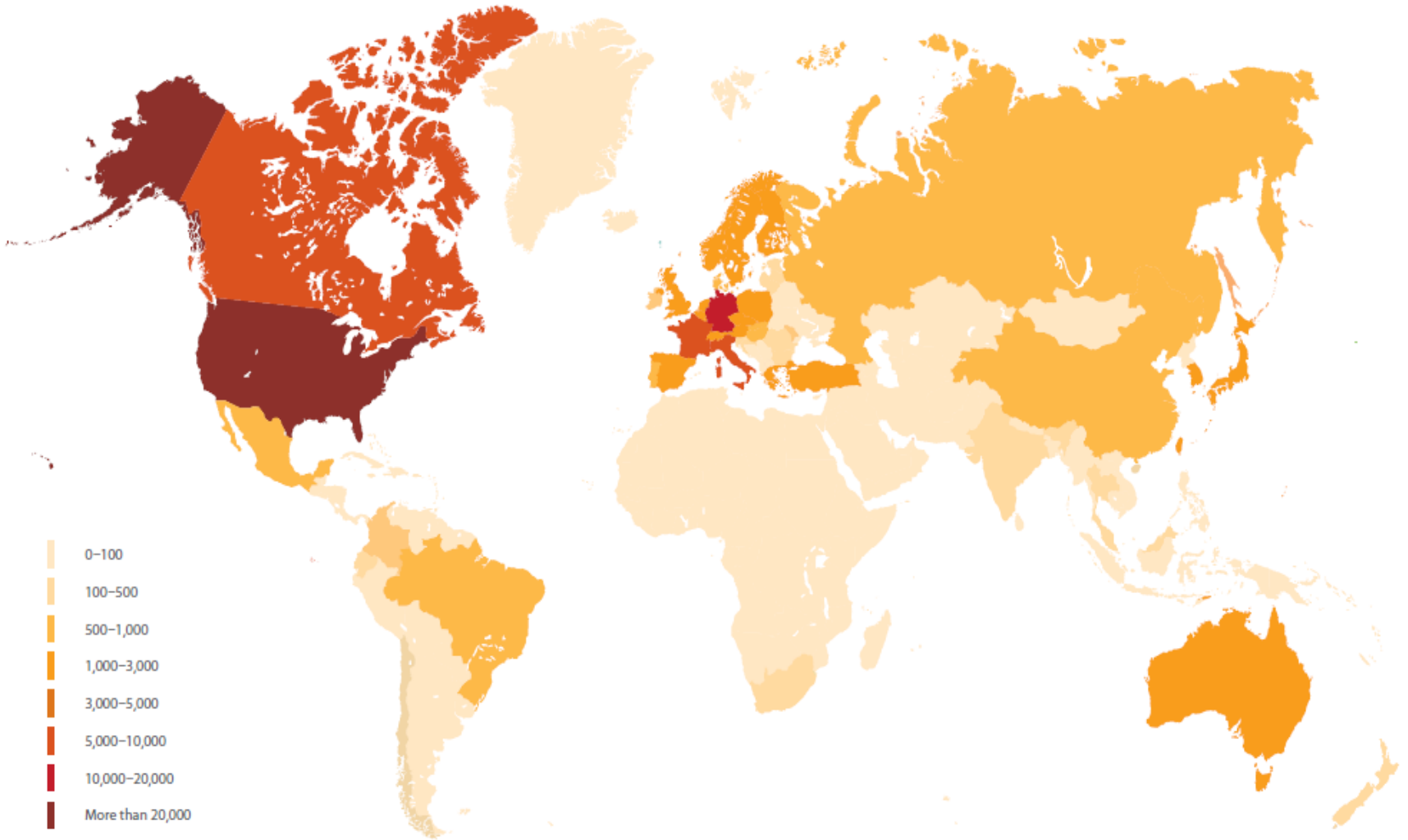
JET CONFERENCE

01/06/2017

PT ISIM и не только

Дмитрий Даренский

POSITIVE TECHNOLOGIES

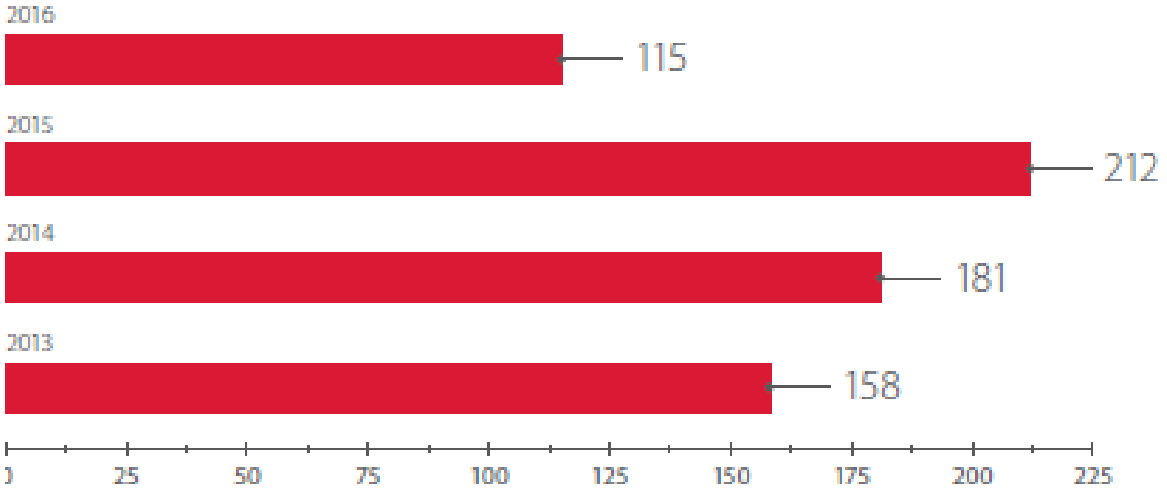


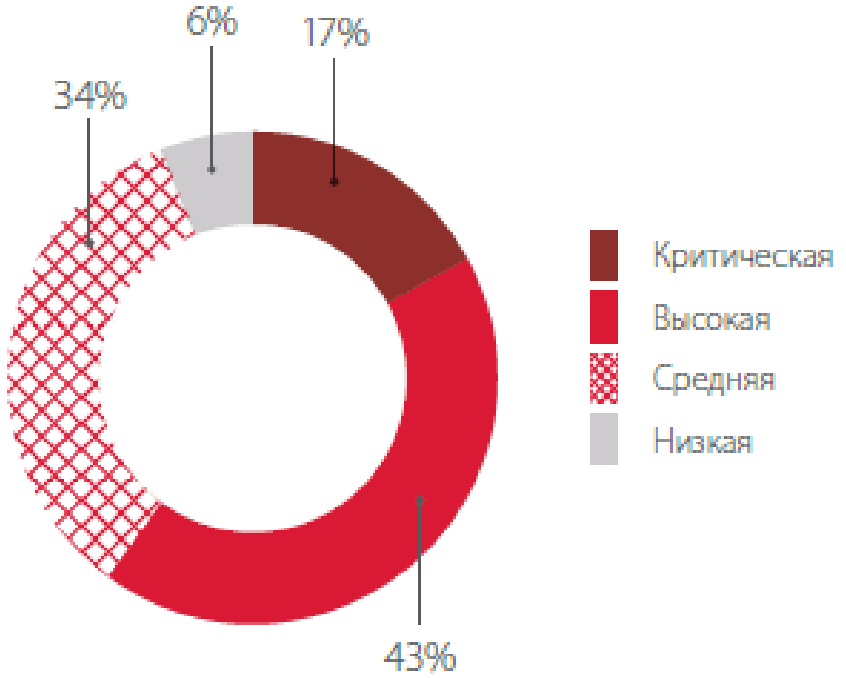
В 2016 Более 160 000 компонентов АСУ ТП оказались подключенными к Интернет

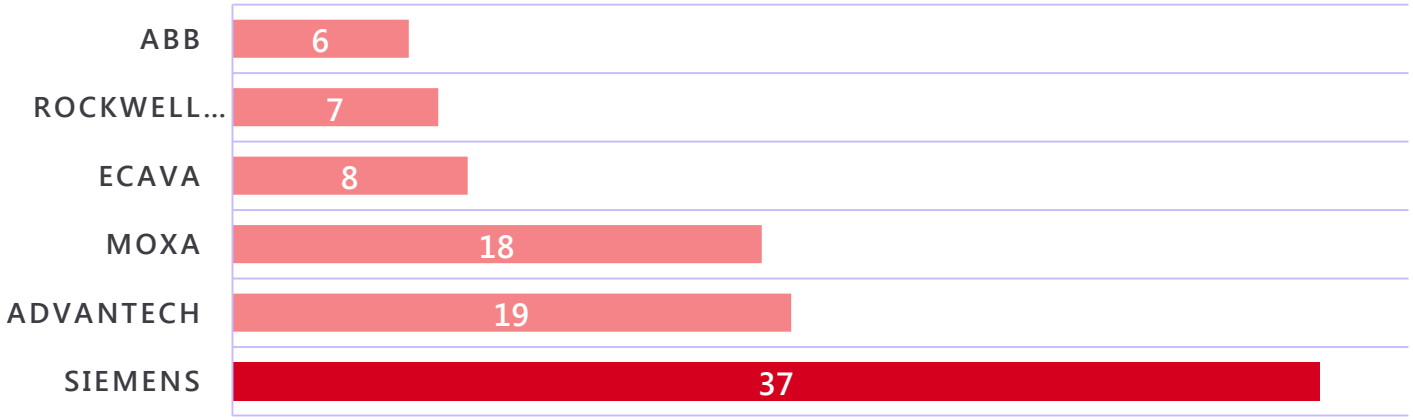
— 4515 компонентов (3% от общего числа) применяются в области энергетики

— 38 580 (24%) относятся к области автоматизации зданий.

Источник: аналитический отчет Positive Technologies «Безопасность АСУ ТП. Итоги 2016 года»







Источник: аналитический отчет Positive Technologies «Безопасность АСУ ТП. Итоги 2016 года»

JET CONFERENCE

Большинство АСУ ТП (и всё что под ними подразумевается)

НЕ УМЕЮТ КОНТРОЛИРОВАТЬ ПОВЕДЕНИЕ КОМПОНЕНТОВ В СВОЕЙ СЕТИ

НЕ ОТЛИЧАЮТ СВОИ СЕТЕВЫЕ КОМПОНЕНТЫ ОТ ПОСТОРОННИХ

НЕ ОТЛИЧАЮТ СВОЙ ТРАФИК ОТ ПОСТОРОННЕГО

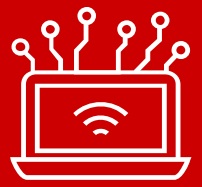
НЕ ВЫЯВЛЯЮТ АТАКИ НА СВОИ КОМПОНЕНТЫ И СЕТЕВЫЕ ПРОТОКОЛЫ

НЕ ВЫЯВЛЯЮТ ЭКСПЛУАТАЦИЮ СВОИХ УЯЗВИМОСТЕЙ

НЕ АНЛИЗИРУЮТ И НЕ РАССЛЕДУЮТ ИНЦИДЕНТЫ КИБЕРБЕЗОПАСНОСТИ

Без влияния на технологический процесс и сеть

- Обнаружение нелигитимной активности в сети
- Выявление атак на устройства и протоколы
- Выявление атак на нарушение логики работы системы
- Выявление эксплуатации уязвимостей
- Возможность проведения расследований



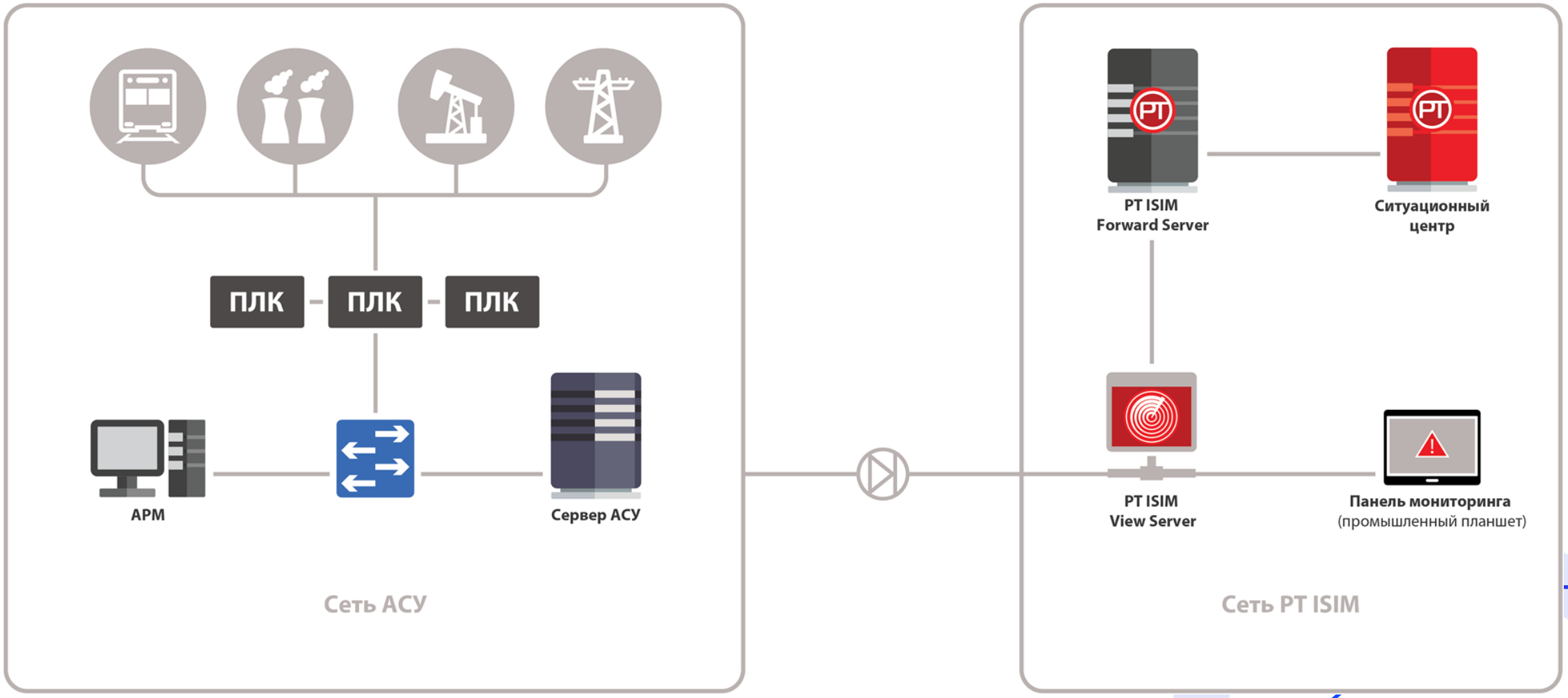
Внешние угрозы

Внутренние угрозы

Ошибки конфигурации

- Превентивное обнаружение действий злоумышленника
- Контроль действий сотрудников и подрядчиков
- Контроль сетевого окружения
- Проведение расследований
- Контроль доступа к удаленной прошивке
- Своевременное информирование об инцидентах
- Анализ инцидентов и оценка их последствий
- Помощь в планировании мер защиты
- Выполнение требований регулирующих организаций

Подключение к SPAN или Mirroring port коммутатора технологической сети через дата диод.



Исходный трафик

```
0000 23 12 14 00 0f 00 f4 01 00 fe 33 00 64 a1 2c 0c 92 05 10 f5 01 00 00 34 00 64 a1 2c 0c 92 05 10
0020 f6 01 00 07 34 00 64 a1 2c 0c 92 05 10 f7 01 00 12 06 00 64 a1 2c 0c 92 05 10 f8 01 00 15 06 00
0040 64 a1 2c 0c 92 05 10 f9 01 00 14 06 00 64 a1 2c 0c 92 05 10 fa 01 00 d2 00 00 64 a1 2c 0c 92 05
0060 10 fb 01 00 d3 00 00 64 a1 2c 0c 92 05 10 fc 01 00 d3 00 00 64 a1 2c 0c 92 05 10 fd 01 00 ff ff
0080 00 64 a1 2c 0c 92 05 10 fe 01 00 ff ff 00 64 a1 2c 0c 92 05 10 ff 01 00 ff ff 00 64 a1 2c 0c 92
00a0 05 10 00 02 00 d2 00 00 64 a1 2c 0c 92 05 10 01 02 00 d3 00 00 64 a1 2c 0c 92 05 10 02 02 00 d3
00c0 00 00 64 a1 2c 0c 92 05 10 03 02 00 e8 03 00 64 a1 2c 0c 92 05 10 04 02 00 e8 03 00 64 a1 2c 0c
```

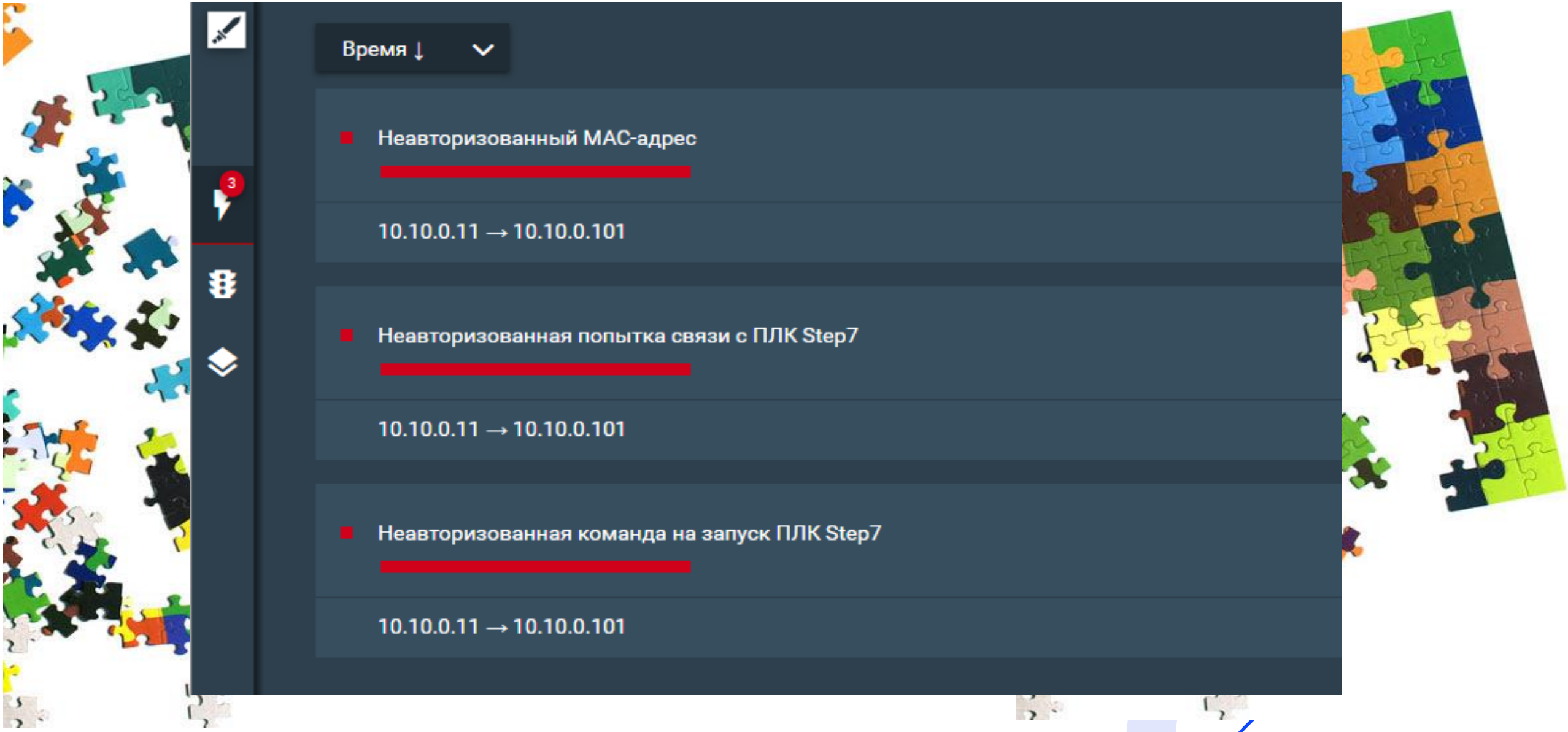
Частичная обработка событий

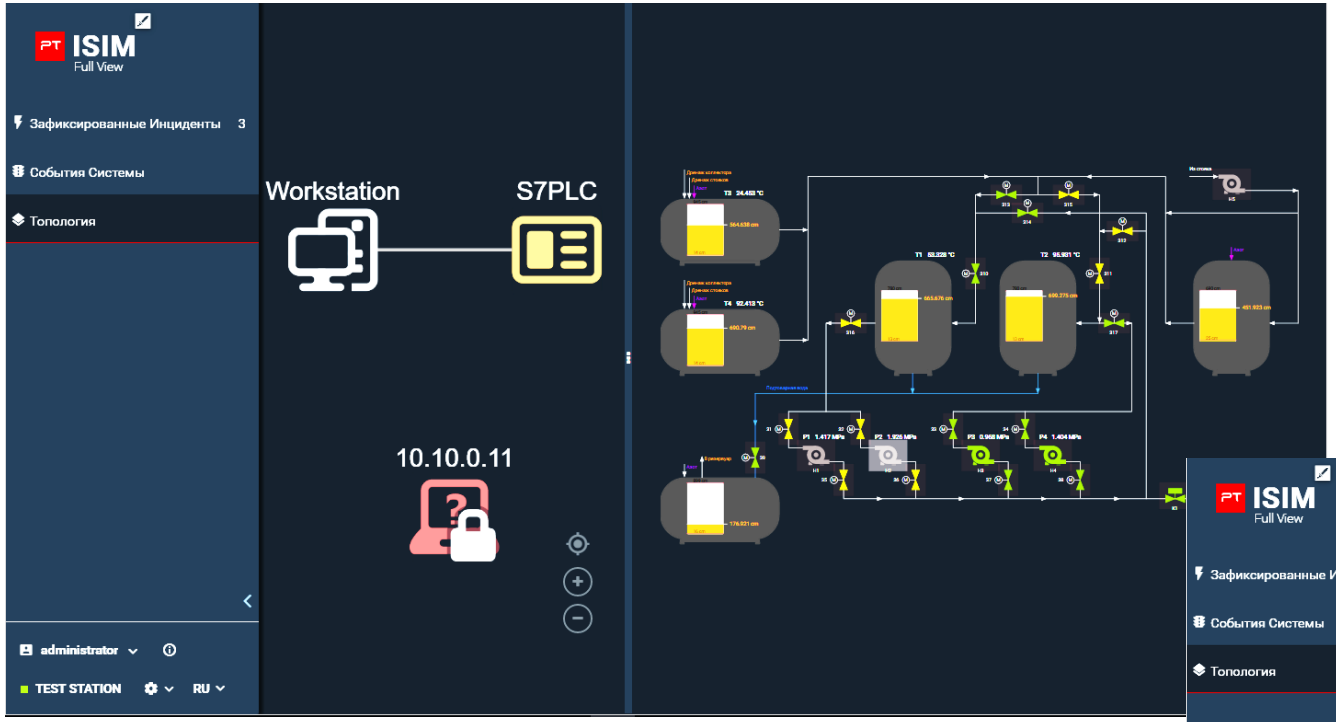
Протокол: IEC104, **Тип информационного объекта: T1_M_SP_NA_1,**
причина передачи: 11, объект информации 25 в состояние 0,
отправитель: 172.50.0.52, получатель: 172.50.0.72

Интеллектуальная обработка событий в трафике

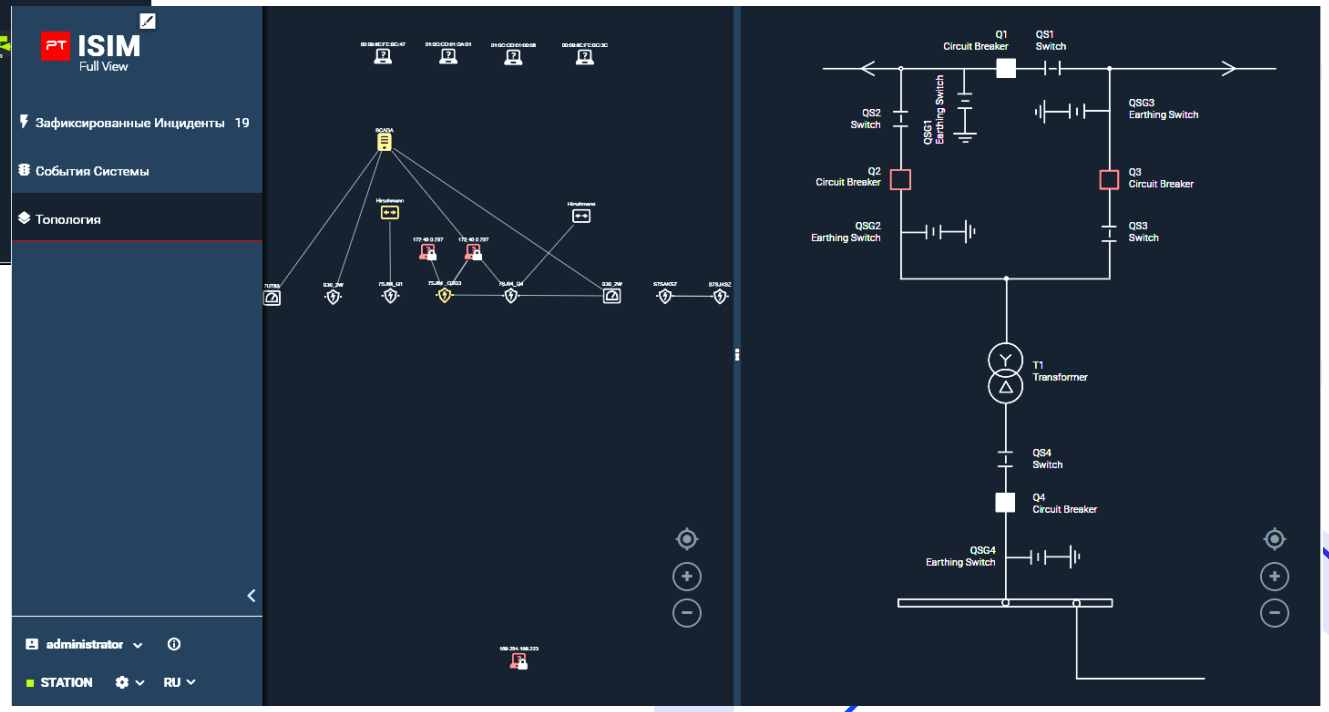
Сообщение IEC104 от 172.50.0.52 на 172.50.0.72:

«Заземляющий нож QSG2: отключен»





1. Цепочки атак
2. Атаки на сетевой карте
3. Атаки на технологической карте



1. Карта объектов сети и их состояние
2. Карта технологического процесса
3. Отображение состояния участков АСУ

JET CONFERENCE

ПИЛОТИРОВАНИЕ

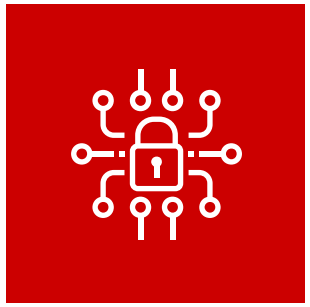
ПРОЕКТИРОВАНИЕ

ПРОЕКТЫ ВНЕДРЕНИЯ

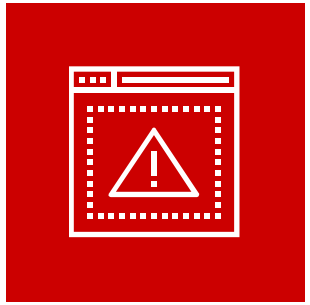
КОГДА ДОГАДЫВАЛСЯ,
ЧТО ВСЁ НЕ ОЧЕНЬ ХОРОШО

НО ПОНЯТИЯ НЕ ИМЕЛ,
НА СКОЛЬКО «НЕ ОЧЕНЬ»

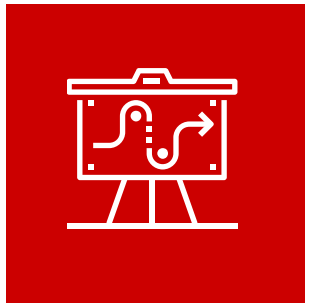
- «Изолированные» сети АСУ ТП такими не являются
- «Изолированная» сеть не равно «незараженная»
- Сегментация сети АСУ ТП только на бумаге
- Трафик всей сети ходит через удаленный объект
- Большинство уязвимостей в сети – результат проектирования и внедрения
- Эксплуатация уязвимостей авторизованными компонентами
- Эксплуатация уязвимых сетевых протоколов (SNMP v.1)
- Неразбериха с подключенными устройствами



- Обнаружение простых и сложных атак
- Контроль сетевого окружения
- Контроль изменений конфигурационных настроек
- Выявление сетевых аномалий
- Контроль сетевого взаимодействия
- Выявление попыток эксплуатации уязвимостей



- Информирование и отчетность на всех уровнях
- Возможность проведения расследований инцидентов
- Масштабируемая решение с широким возможностями интеграции



- Поддержка принятия решений
- Соответствие требованиям регуляторов

POSITIVE TECHNOLOGIES

JET CONFERENCE

01/06/2017

Дмитрий Даренский

Спасибо за внимание!