Петров С.В.

IDS&PKI

PKI. Практическая безопасность

POSITIVE TECHNOLOGIES

ptsecurity.ru

POSITIVE TECHNOLOGIES

PKI надежно построен и защищен

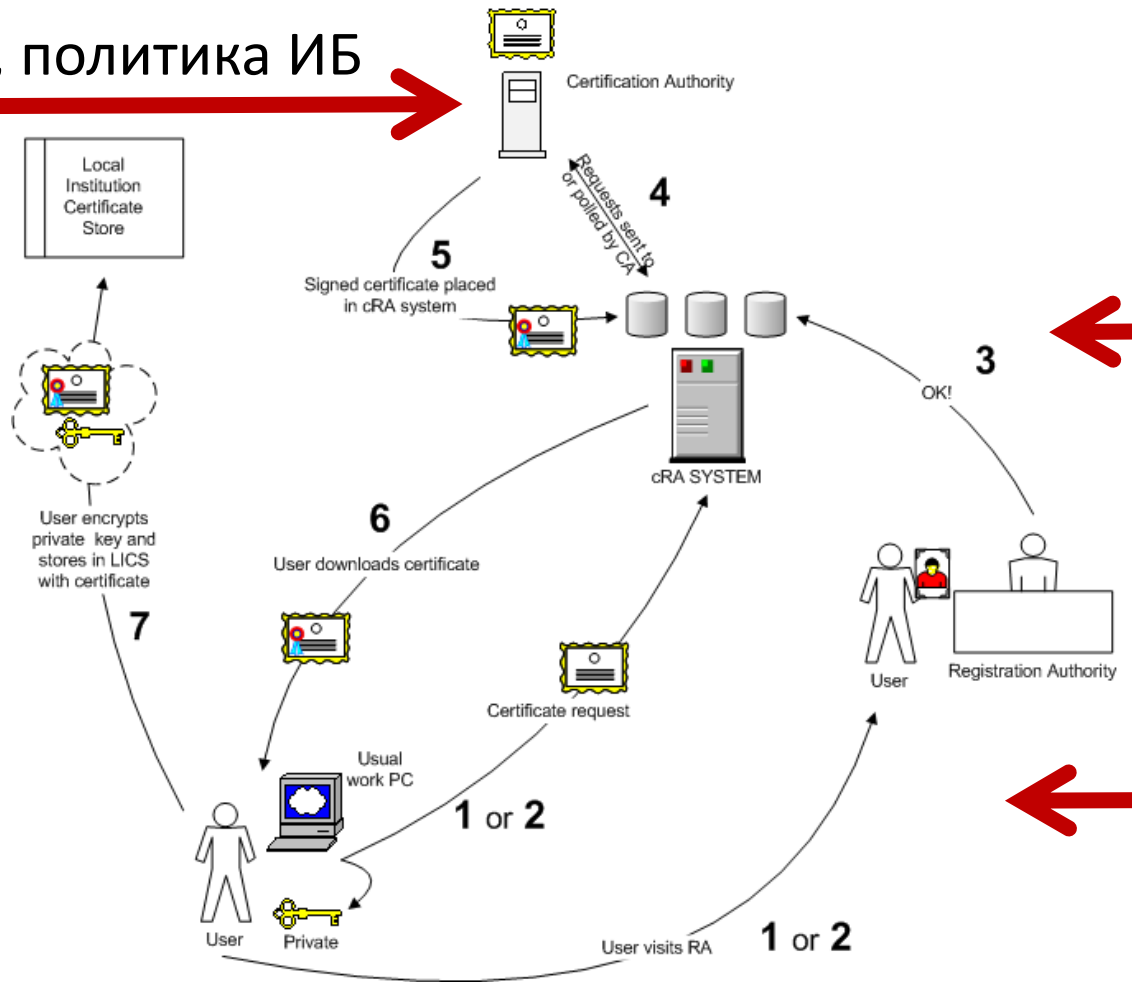
- ФЗ-63
- Положения 795, 796
- X.842
- Сертифицированные криптопровайдеры КС1 КС2
- Аттестованные и аккредитованные УЦ
- DMZ, СЗИ НСД, токены, регламенты…

PKI. Жизненный цикл компонентов с PKI

POSITIVE TECHNOLOGIES

DMZ

Настройки, политика ИБ



Патчи, обновления

Прошивки

Internet

Пакеты — Встраивание в качестве ядер

- OpenSSL
- Bouncycastle
- GnuTLS

Протоколы — Примерный стек

- TSP RFC3161
- OCSP RFC6960
- DVCS RFC3029
- HTTP, FTP, TFTP, SNMP, DHCP, LLMNR, NBNS, TLS, SSH, Telnet etc

Системное ПО — Неотъемлемая часть

- ОС Windows
- ОС/прошивки FW, коммутаторов, оборудования

Криптоядра — Интерфейсы и решения

- CSP
- JCP
- CryptoAPI, PKCS#11, CNG

PKI. Анализ компонентов PKI

POSITIVE TECHNOLOGIES

PKI. Примеры CVE в пакетах PKI

POSITIVE TECHNOLOGIES

CVE-2016-2180

The TS_OBJ_print_bio function in crypto/ts/ts_lib.c in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation in **OpenSSL** through 1.0.2h allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted time-stamp file that is mishandled by the "openssl ts" command.

CVE-2013-0166

OpenSSL before 0.9.8y, 1.0.0 before 1.0.0k, and 1.0.1 before 1.0.1d does not properly perform signature verification for OCSP responses, which allows remote OCSP servers to cause a denial of service (NULL pointer dereference and application crash) via an invalid key.

CVE-2012-0441

The ASN.1 decoder in the QuickDER decoder in Mozilla Network Security Services (**NSS**) before 3.13.4, as used in Firefox 4.x through 12.0, Firefox ESR 10.x before 10.0.5, Thunderbird 5.0 through 12.0, Thunderbird ESR 10.x before 10.0.5, and SeaMonkey before 2.10, allows remote attackers to cause a denial of service (application crash) via a zero-length item, as demonstrated by (1) a zero-length basic constraint or (2) a zero-length field in an OCSP response.

CISCO ASA, Apple iOS,
CISCO IOS, GnuTLS

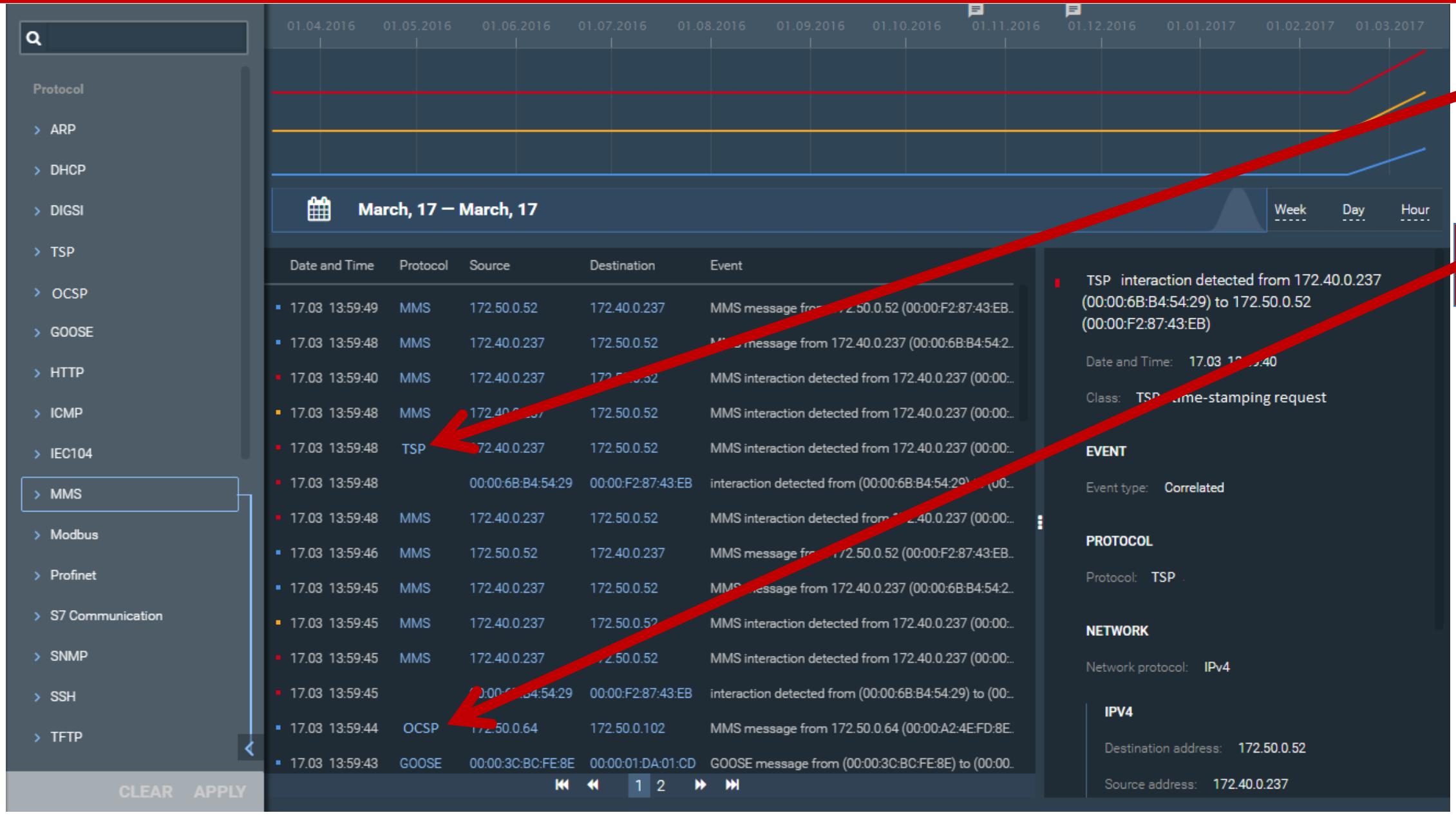
PKI. Работающие системы не проверялись на прочность

POSITIVE TECHNOLOGIES

- Нет аудита PKI
- Нет пентестов PKI
- Не исследуются работающие PKI-проекты
- Не ведется реестр PKI-уязвимостей и патчей для них. Или мы не знаем.

PKI. События в PKI-трафике

POSITIVE TECHNOLOGIES



TSP

OSCP

FTP

DHCP

PKI. Этапы разбора трафика

POSITIVE TECHNOLOGIES

Передаётся в сети:

```
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
```

Частичный разбор:

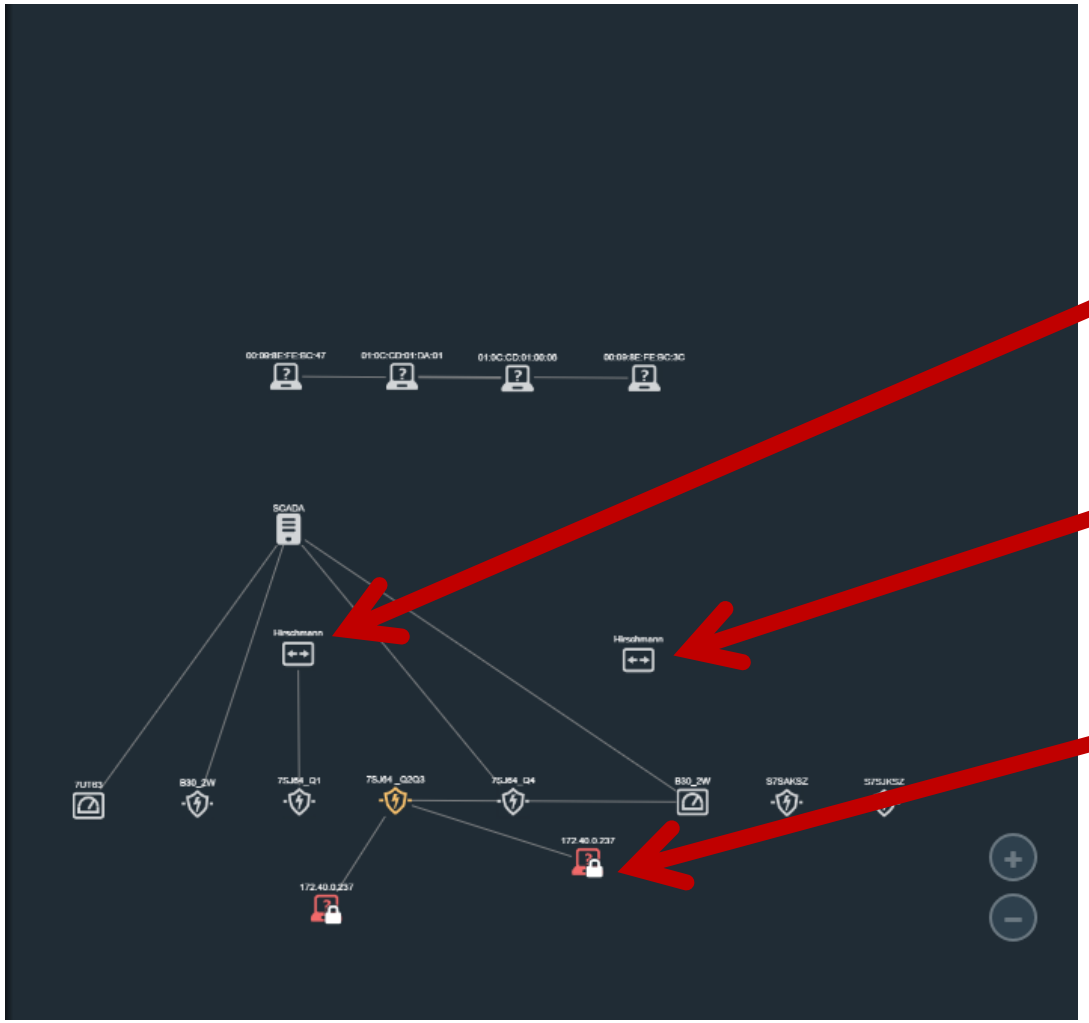
Протокол: TSP3161, Тип информационного объекта: TimeStampResp , причина передачи: 11, объект информации 25 в состояние 0, отправитель: 172.50.0.52, получатель: 172.50.0.72

“Умный” разбор:

Сообщение TSP3161 от 172.50.0.52 на 172.50.0.72: «Ответ TSA сервера на запрос метки времени: успешно»

PKI. Топология защищаемой сети

POSITIVE TECHNOLOGIES



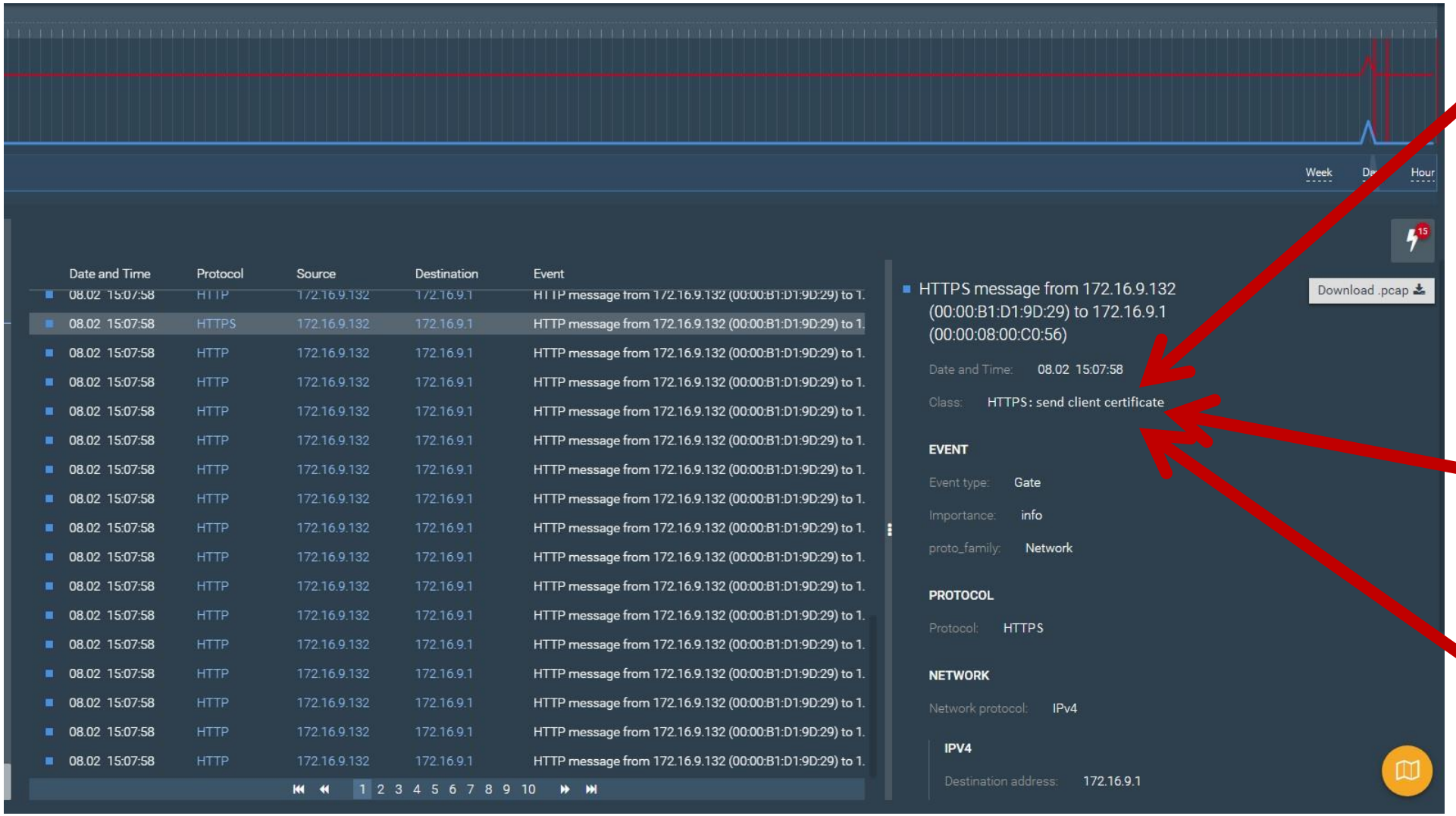
OCSP-сервер

TSP-сервер

Неавторизованный хост

PKI. Проверка на соответствие РД в реальном времени

POSITIVE TECHNOLOGIES



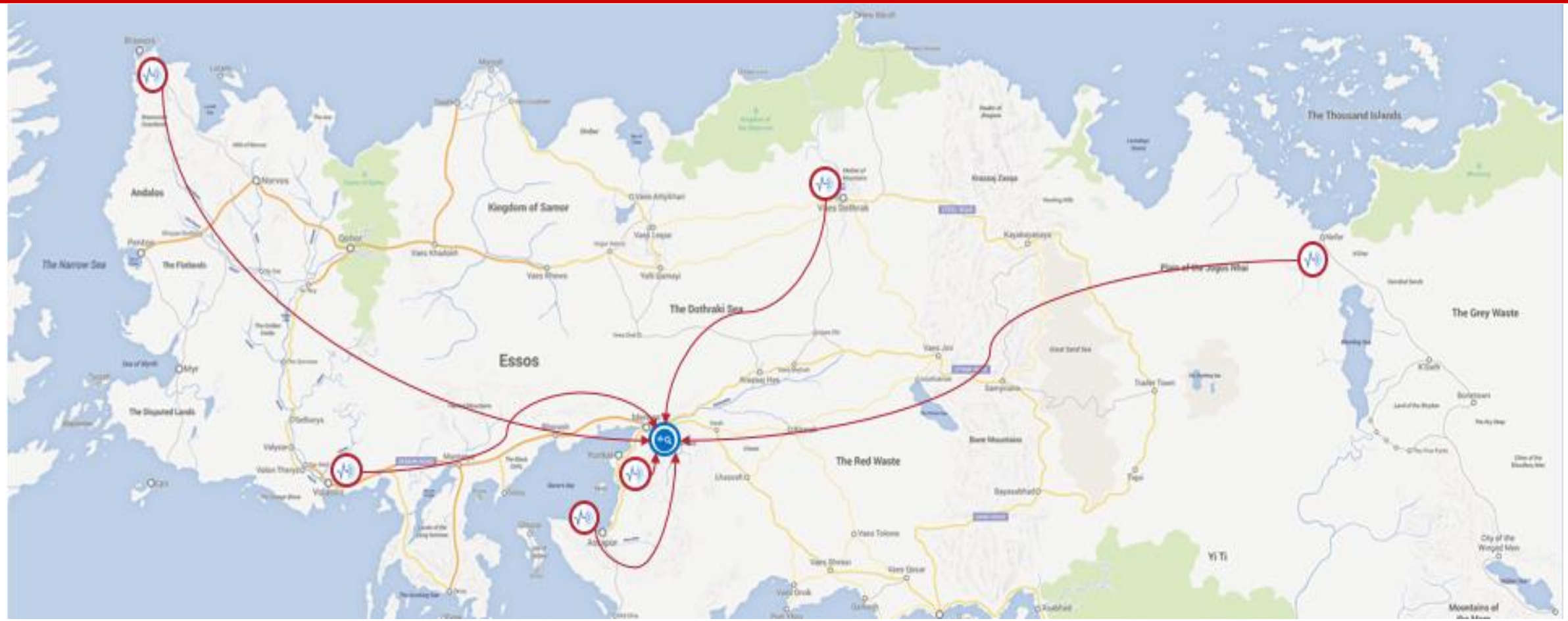
Приказ ФСБ № 795
Требования к совокупности полей квалифицированного сертификата, к порядку расположения полей

Приказ ФСБ № 796
Классификация атаки в соответствии с положением

NIST-тесты:
4.4.18 Invalid Long Serial Number Test18

PKI. Информация с IDS в SOC

POSITIVE TECHNOLOGIES



- Информация о состоянии удалённых объектов стекается в SOC
- Возможность удалённого управления объектами (обновления продукта и внесение новых детектов)
- Возможность удалённого расследования и ведения инцидентов
- Возможности получения оперативной информации о киберзащищённости на местах

PKI. IDS для PKI как сервис X.842

POSITIVE TECHNOLOGIES

- \+ X.842: 7.7.7 Incident Reporting and Alert Management Service
- \+ Обнаружение вторжений и оповещение в реальном времени
- \+ Гарантия изоляции от корпоративной сети на физическом уровне, используется гальваническая развязка с сетью
- \+ Создание набора базовых PKI-событий, моделирование системы доверия
- \+ Аудит на соответствие требованиям РД в реальном времени

Спасибо!

POSITIVE TECHNOLOGIES

ptsecurity.ru