NTA: почему анализ трафика необходим в SOC

Владимир Бенгин

ptsecurity.com

Предотвратить проникновение в сеть

- **Firewall**
- **IPS**
- **NGFW**
- **WAF**
- **Email GW**
- **Web GW**
- **Pentest**

Предотвратить проникновение в сеть **больше не удается**

- **Firewall**
- **IPS**
- **NGFW**
- **WAF**
- **Email GW**
- **Web GW**
- **Pentest**

в 92% проектов

по тестированию на проникновению, проведенных в 2018 году, наши специалисты смогли преодолеть сетевой периметр и получить доступ к ресурсам ЛВС*

в 50% компаний

злоумышленник может преодолеть сетевой периметр за один шаг*

206 дней

среднее время незаметного присутствия злоумышленников в инфраструктуре**

* Уязвимости корпоративных информационных систем, 2019, Positive Technologies
** 2019 Cost of a Data Breach Report, Ponemon institute

Средства мониторинга инфраструктуры

Многие клиенты Gartner рассказали, что NTA инструменты выявили подозрительную активность в трафике, которую пропустили периметровые решения

Market Guide for Network Traffic Analysis, Gartner, 2019

NTA входит в топ технологий для выявления угроз, работой которых довольны в SOC

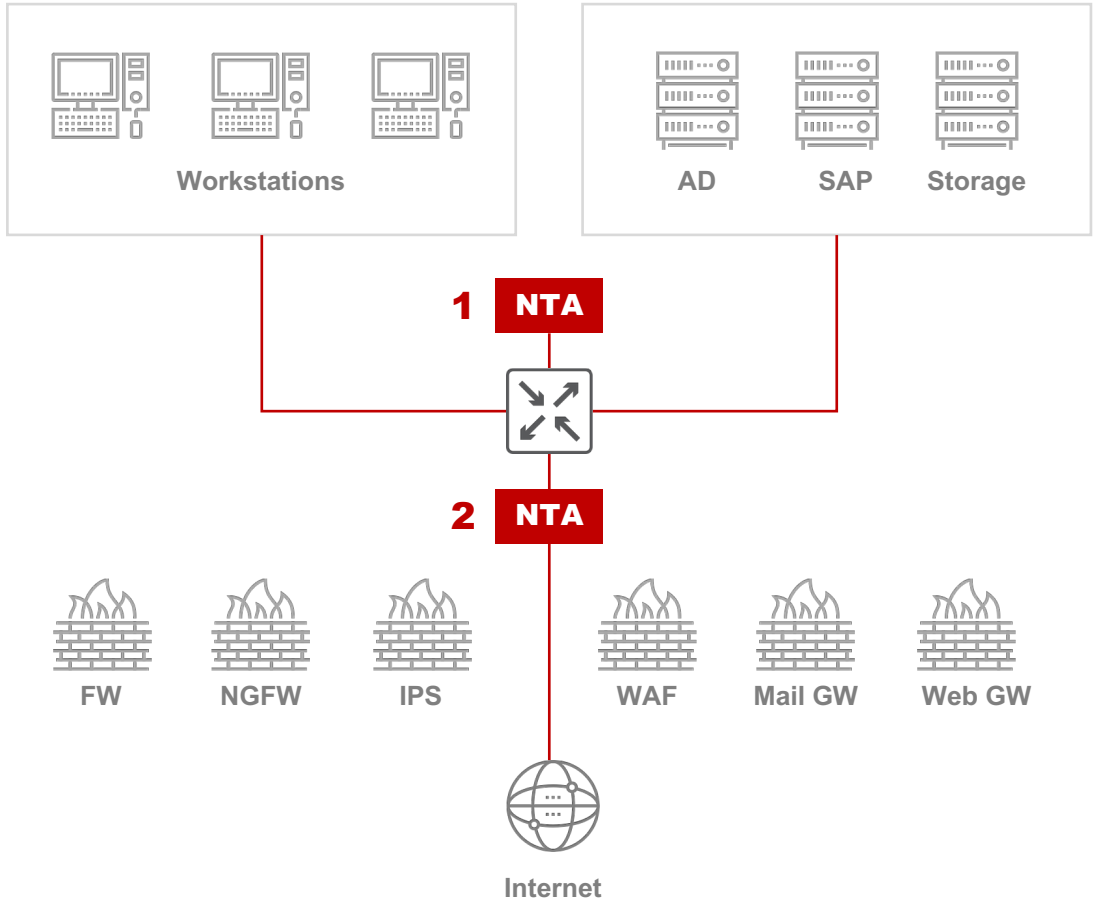
Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey, SANS Institute 2019

NTA — Network Traffic Analysis

Где внедрять и что можно выявлять при помощи NTA

- **Горизонтальное перемещение**
  - Эксплуатация уязвимостей
  - Хакерский инструментарий
  - Распространение вредоносов
- **Внутренний злоумышленник**
- **Эксфильтрация данных**
- **Коммуникации с серверами злоумышленников**

- **Расследование**
- **Сетевой комплаенс**



Что можно поймать

Результаты пилотирования PT NAD в 2019 году

Сканирование внутренней сети
39%

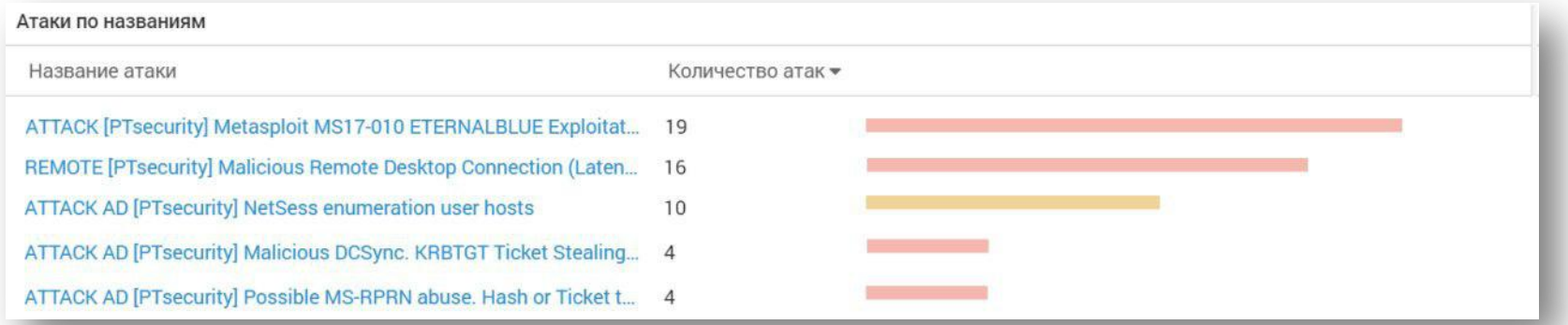
Запуск инструментов для проведения атак
25%

Попытки эксплуатации уязвимостей в ПО
25%

Получение данных с контроллера домена
21%

Сбор информации об активных сетевых сессиях
21%

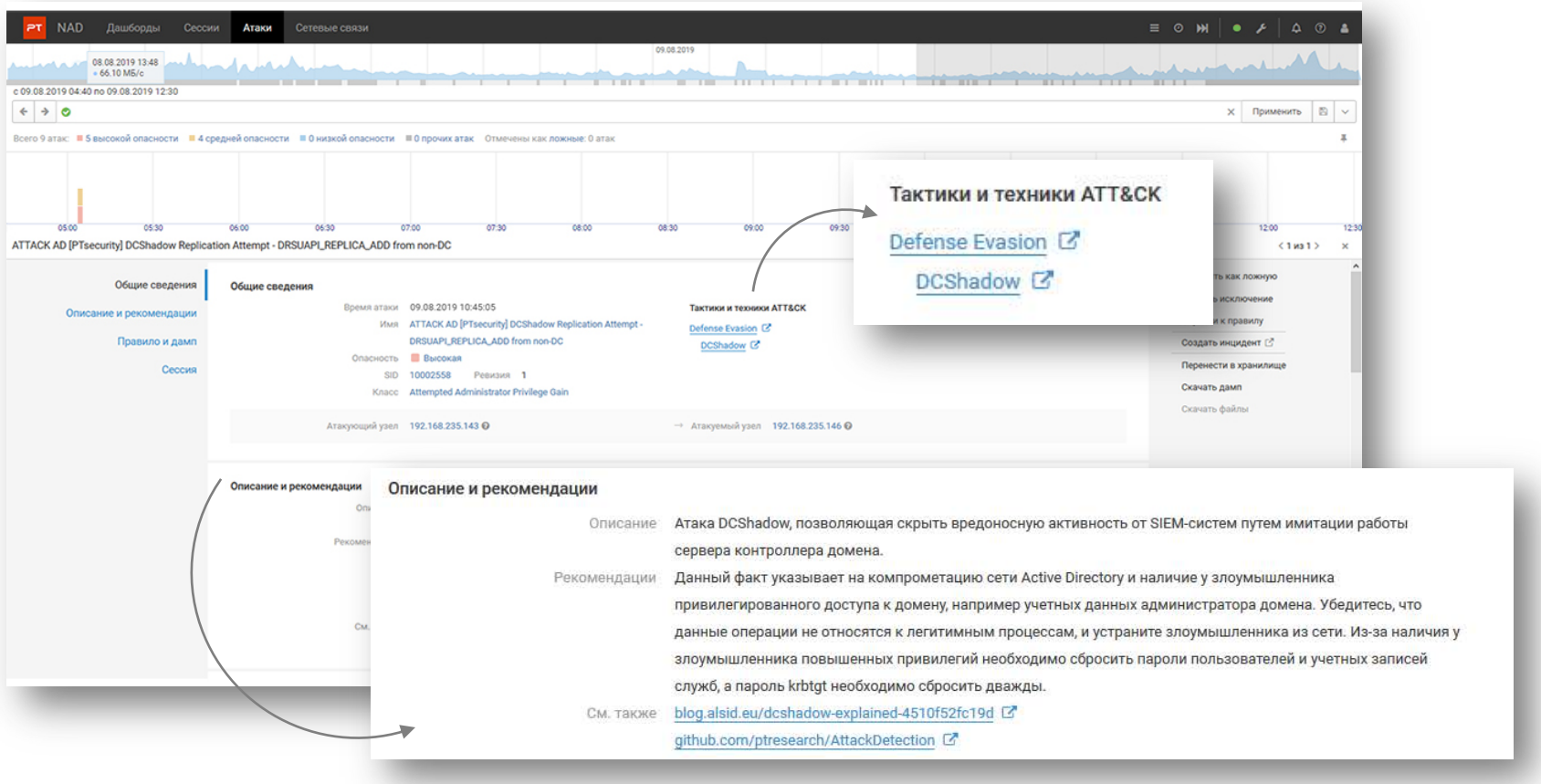
Попытки удаленного запуска службы или процесса
14%



SMB, Kerberos, NTLM, RPC …

Не суммируй,
100% не выйдет!

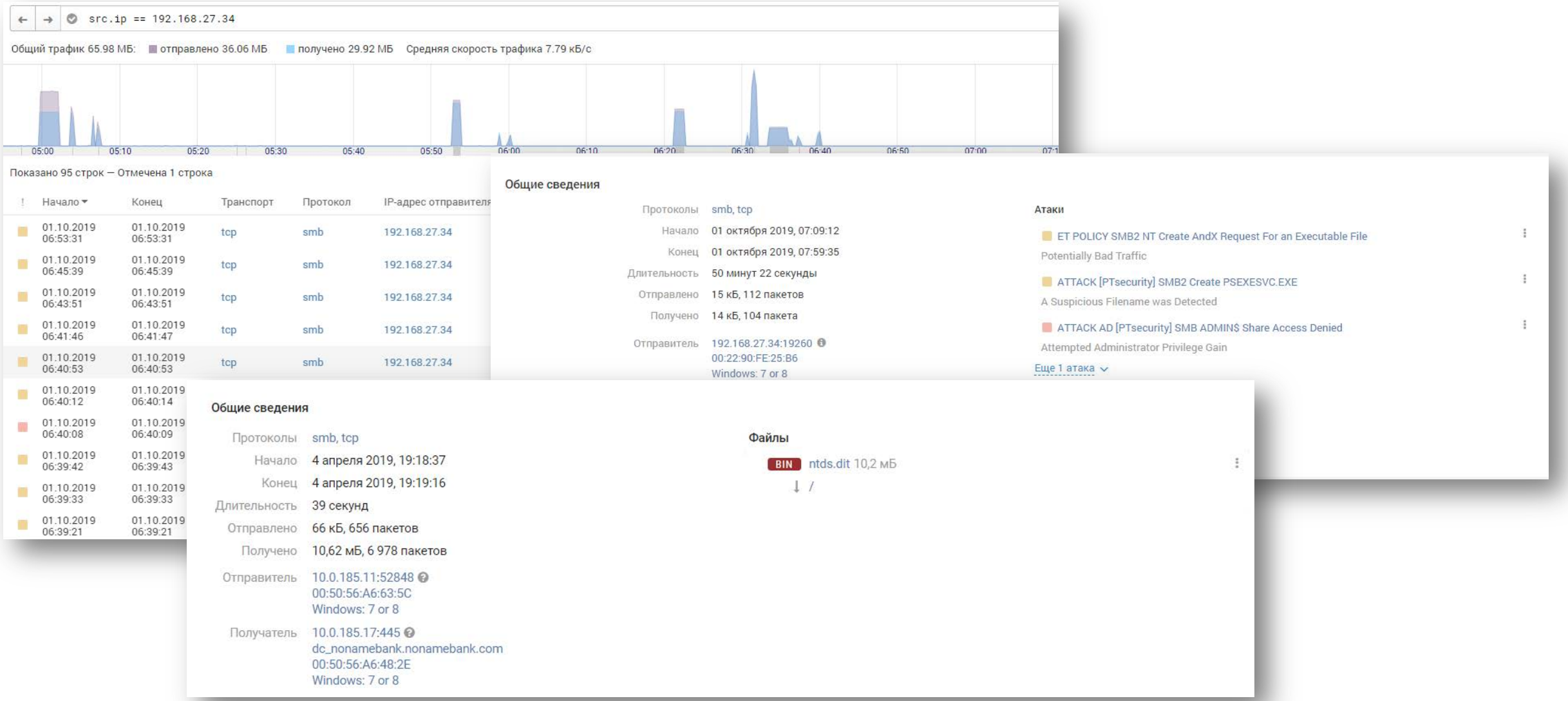
Описание, классификация, рекомендации



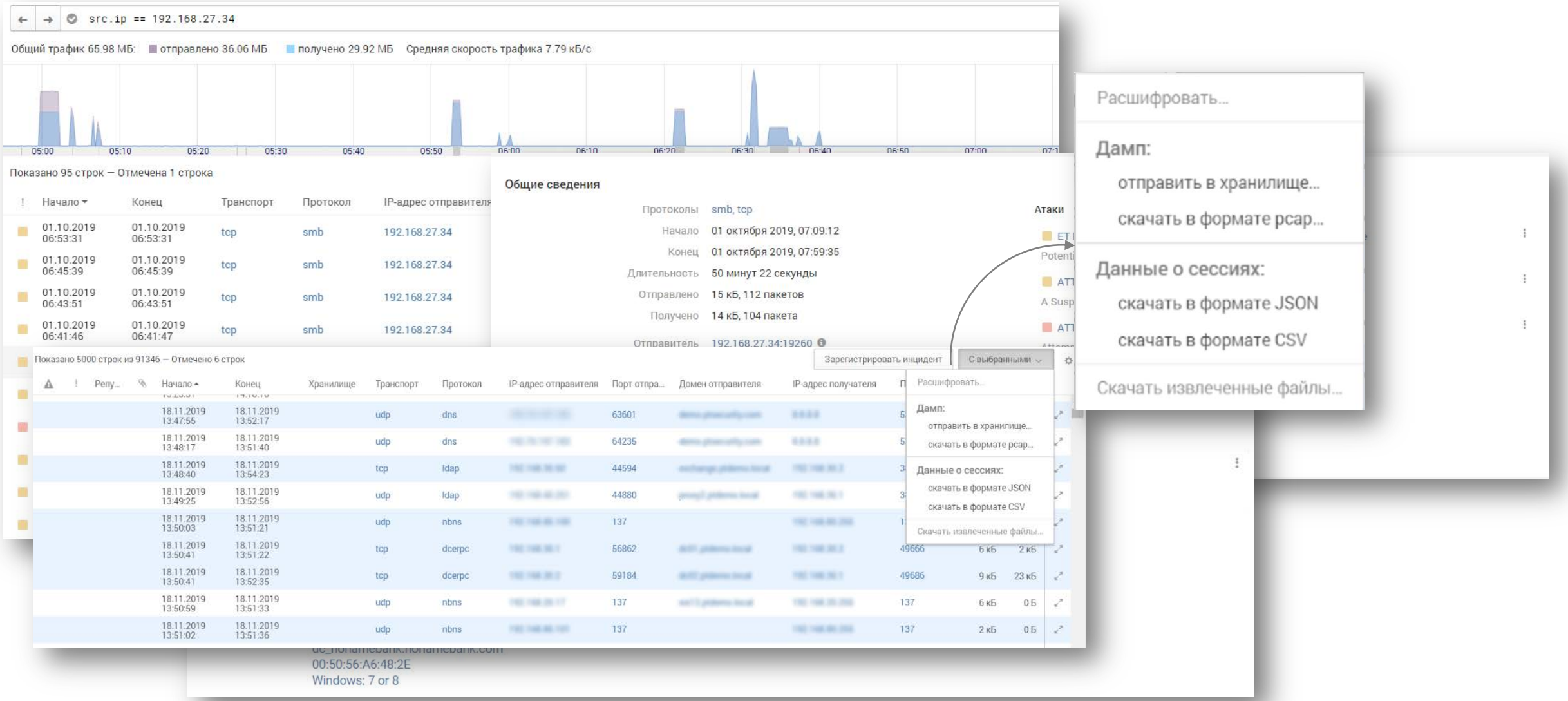
В карточке атаки отображаются данные об использованных тактиках и техниках по матрице ATT&CK.

Это помогает понять, на какой стадии атаки находятся злоумышленники и быстрее определить компенсирующие меры.

Расследование



Расследование



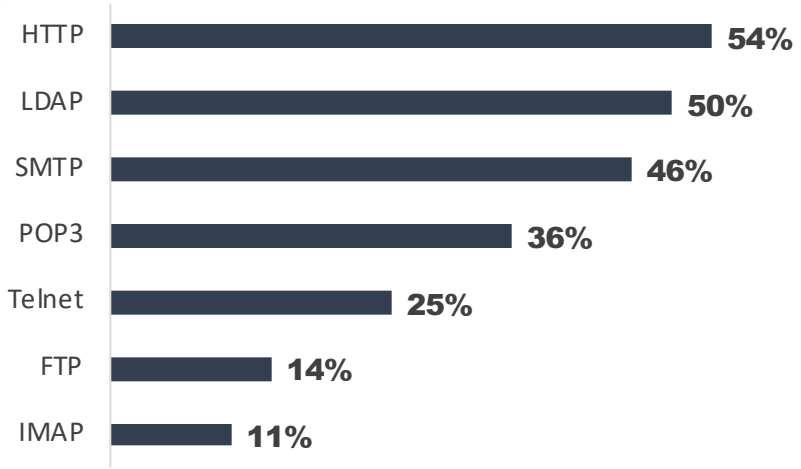
Нарушение регламентов ИБ

Пары "логин – пароль" по числу сессий

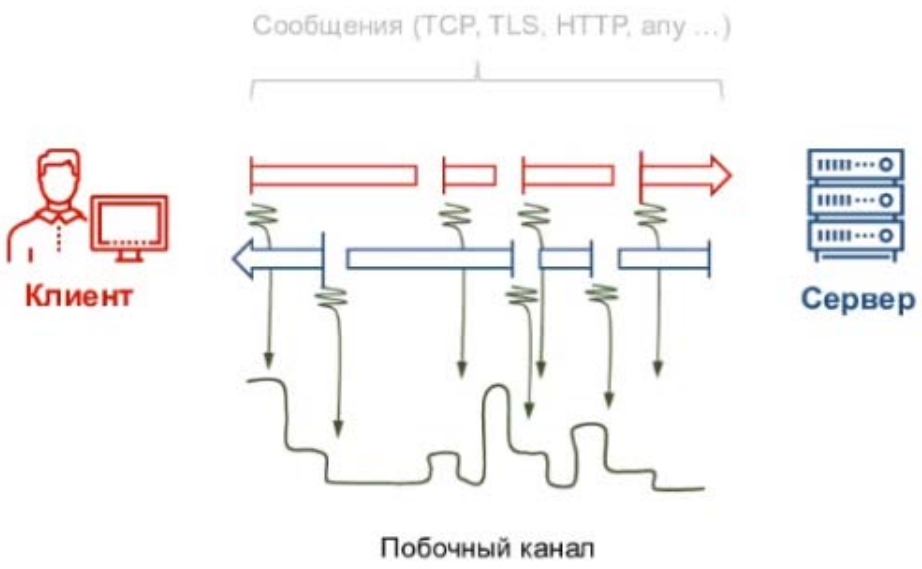
Логин	Пароль	Количество сессий
administrator	[redacted]	57
service	[redacted]	51
smakarova@[redacted].com	[redacted]	25
aivanov@[redacted].com	[redacted]	12
imironov@[redacted].com	[redacted]	9
vc-admin@[redacted].com	[redacted]	3
cisco	[redacted]	3
zabbix	zabbix	3

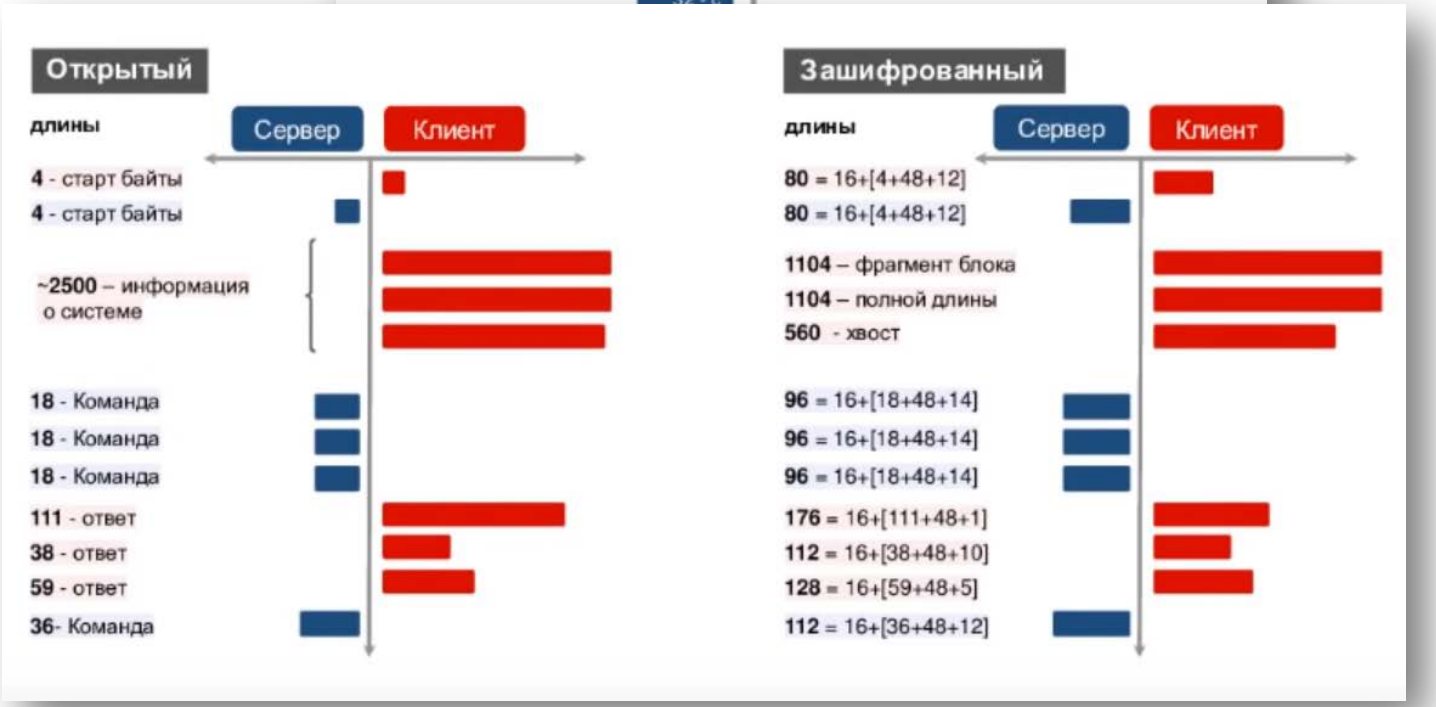
Нарушения регламентов ИБ встречалось нами в 96% случаев

Самый распространенный пример — передача паролей и других данных в открытом виде

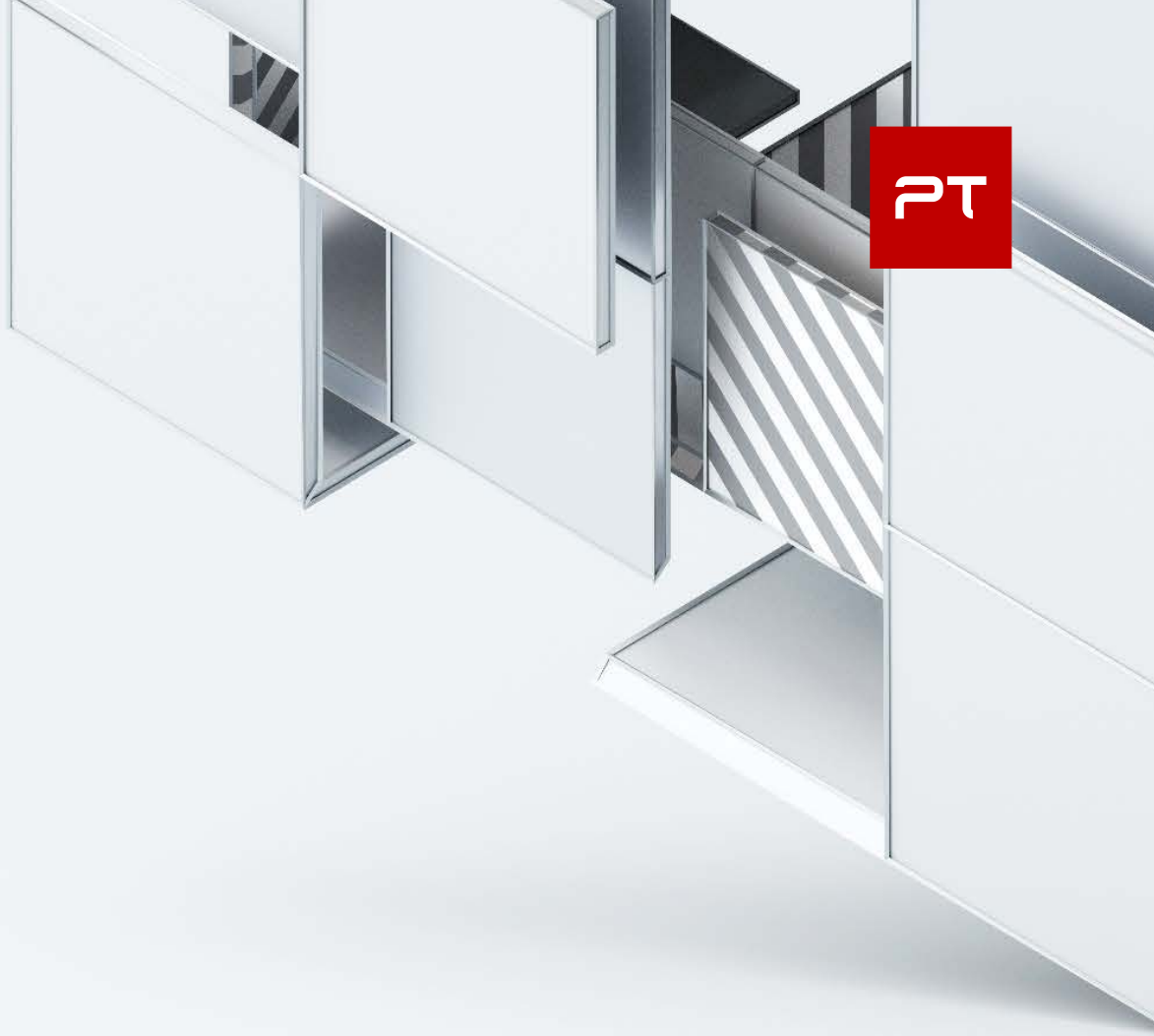


Наблюдение за внешним трафиком





Почему NTA это здорово



Видит активность злоумышленников во внутреннем трафике

Легко внедряется и приносит Результат сразу после внедрения

Усиливает любой SOC. Видит то чего не видят EDR и SIEM

Не может быть отключен злоумышленником

Почему NTA это здорово

Видит активность злоумышленников во внутреннем трафике

Легко внедряется и приносит Результат сразу после внедрения

Усиливает любой SOC. Видит то чего не видят EDR и SIEM

Не может быть отключен злоумышленником

А еще

Может использоваться для:

- Расследования атак
- Threat Hunting
- Наведения порядка в сети


NITA