



POSITIVE  
TECHNOLOGIES

# NTA: почему анализ трафика необходим в SOC

Владимир Бенгин

[ptsecurity.com](http://ptsecurity.com)

# Предотвратить проникновение в сеть

PT

**Firewall**

**IPS**

**NGFW**

**WAF**

**Email GW**

**Web GW**

**Pentest**

# Предотвратить проникновение в сеть больше не удастся

PT

Firewall

IPS

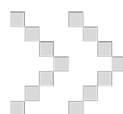
NGFW

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

Анализ сетевого трафика

**NTA**

**SOC  
Visibility  
Triad**

Gartner 2019

**SIEM**

**EDR**

Анализ активности и на узлах

Журналы систем и средств защиты

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

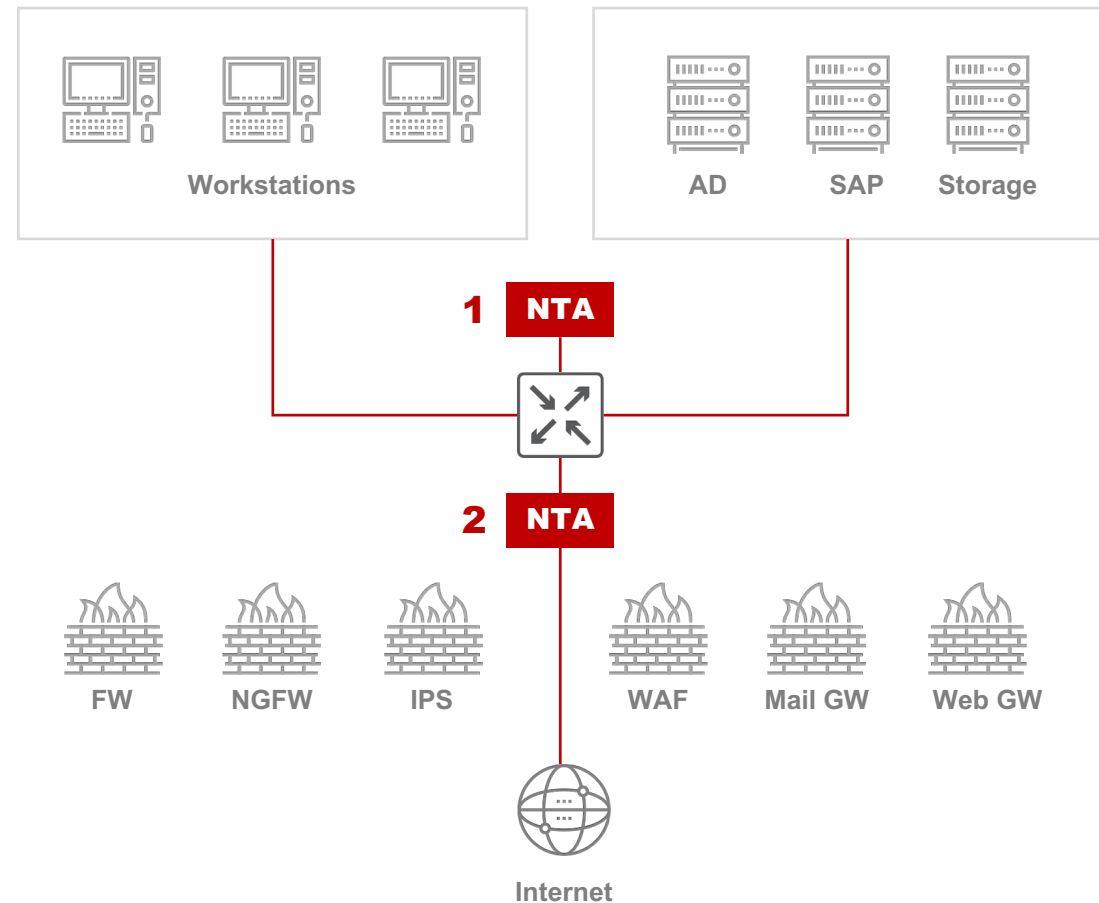
Market Guide for Network Traffic Analysis, Gartner, 2019

**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

# Где внедрять и что можно выявлять при помощи NTA

- **Горизонтальное перемещение**
  - Эксплуатация уязвимостей
  - Хакерский инструментарий
  - Распространение вредоносных
- **Внутренний злоумышленник**
- **Эксфильтрация данных**
- **Коммуникации с серверами злоумышленников**
  
- **Расследование**
- **Сетевой комплаенс**



# Что можно поймать

PT

## 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%**

### Атаки по названиям

Название атаки	Количество атак
ATTACK [PTsecurity] Metasploit MS17-010 ETERNALBLUE Exploitat...	19
REMOTE [PTsecurity] Malicious Remote Desktop Connection (Laten...	16
ATTACK AD [PTsecurity] NetSess enumeration user hosts	10
ATTACK AD [PTsecurity] Malicious DCSync. KRBTGT Ticket Stealing...	4
ATTACK AD [PTsecurity] Possible MS-RPRN abuse. Hash or Ticket t...	4

## SMB, Kerberos, NTLM, RPC ...

Не суммируй,  
100% не выйдет!

# Описание, классификация, рекомендации

The screenshot shows the PT NAD interface with a timeline of attacks. A callout box titled "Тактики и техники ATT&CK" lists "Defense Evasion" and "DCShadow". Below it, a detailed card for the "ATTAACK AD [PTsecurity] DCShadow Replication Attempt" attack provides the following information:

Время атаки	09.08.2019 10:45:05
Имя	ATTAACK AD [PTsecurity] DCShadow Replication Attempt - DRSUAPL_REPLICA_ADD from non-DC
Опасность	Высокая
SID	10002558
Ревизия	1
Класс	Attempted Administrator Privilege Gain
Атакующий узел	192.168.235.143
Атакуемый узел	192.168.235.146

**Описание и рекомендации**

**Описание:** Атака DCShadow, позволяющая скрыть вредоносную активность от SIEM-систем путем имитации работы сервера контроллера домена.

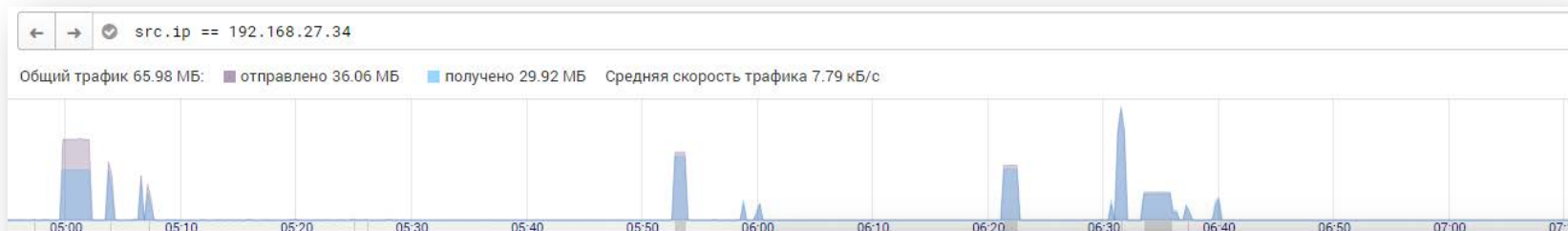
**Рекомендации:** Данный факт указывает на компрометацию сети Active Directory и наличие у злоумышленника привилегированного доступа к домену, например учетных данных администратора домена. Убедитесь, что данные операции не относятся к легитимным процессам, и устраните злоумышленника из сети. Из-за наличия у злоумышленника повышенных привилегий необходимо сбросить пароли пользователей и учетных записей служб, а пароль krbtgt необходимо сбросить дважды.

**См. также:** [blog.alsid.eu/dcshadow-explained-4510f52fc19d](http://blog.alsid.eu/dcshadow-explained-4510f52fc19d)  
[github.com/ptresearch/AttackDetection](https://github.com/ptresearch/AttackDetection)

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



Показано 95 строк — Отмечена 1 строка

!	Начало	Конец	Транспорт	Протокол	IP-адрес отправителя
■	01.10.2019 06:53:31	01.10.2019 06:53:31	tcp	smb	192.168.27.34
■	01.10.2019 06:45:39	01.10.2019 06:45:39	tcp	smb	192.168.27.34
■	01.10.2019 06:43:51	01.10.2019 06:43:51	tcp	smb	192.168.27.34
■	01.10.2019 06:41:46	01.10.2019 06:41:47	tcp	smb	192.168.27.34
■	01.10.2019 06:40:53	01.10.2019 06:40:53	tcp	smb	192.168.27.34
■	01.10.2019 06:40:12	01.10.2019 06:40:14			
■	01.10.2019 06:40:08	01.10.2019 06:40:09			
■	01.10.2019 06:39:42	01.10.2019 06:39:43			
■	01.10.2019 06:39:33	01.10.2019 06:39:33			
■	01.10.2019 06:39:21	01.10.2019 06:39:21			

### Общие сведения

Протоколы smb, tcp  
Начало 01 октября 2019, 07:09:12  
Конец 01 октября 2019, 07:59:35  
Длительность 50 минут 22 секунды  
Отправлено 15 кБ, 112 пакетов  
Получено 14 кБ, 104 пакета  
Отправитель 192.168.27.34:19260  
00:22:90:FE:25:B6  
Windows: 7 or 8

### Атаки

- ET POLICY SMB2 NT Create AndX Request For an Executable File  
Potentially Bad Traffic
  - ATTACK [PTsecurity] SMB2 Create PSEXESVC.EXE  
A Suspicious Filename was Detected
  - ATTACK AD [PTsecurity] SMB ADMIN\$ Share Access Denied  
Attempted Administrator Privilege Gain
- [Еще 1 атака](#)

### Общие сведения

Протоколы smb, tcp  
Начало 4 апреля 2019, 19:18:37  
Конец 4 апреля 2019, 19:19:16  
Длительность 39 секунд  
Отправлено 66 кБ, 656 пакетов  
Получено 10,62 МБ, 6 978 пакетов  
Отправитель 10.0.185.11:52848  
00:50:56:A6:63:5C  
Windows: 7 or 8  
Получатель 10.0.185.17:445  
dc\_nonamebank.nonamebank.com  
00:50:56:A6:48:2E  
Windows: 7 or 8

### Файлы

**BIN** ntds.dit 10,2 МБ  
↓ /

# Расследование



src.ip == 192.168.27.34

Общий трафик 65.98 МБ: отправлено 36.06 МБ получено 29.92 МБ Средняя скорость трафика 7.79 кБ/с

Показано 95 строк — Отмечена 1 строка

!	Начало	Конец	Транспорт	Протокол	IP-адрес отправителя
■	01.10.2019 06:53:31	01.10.2019 06:53:31	tcp	smb	192.168.27.34
■	01.10.2019 06:45:39	01.10.2019 06:45:39	tcp	smb	192.168.27.34
■	01.10.2019 06:43:51	01.10.2019 06:43:51	tcp	smb	192.168.27.34
■	01.10.2019 06:41:46	01.10.2019 06:41:47	tcp	smb	192.168.27.34

Общие сведения

Протоколы smb, tcp

Начало 01 октября 2019, 07:09:12

Конец 01 октября 2019, 07:59:35

Длительность 50 минут 22 секунды

Отправлено 15 кБ, 112 пакетов

Получено 14 кБ, 104 пакета

Отправитель 192.168.27.34:19260

Атаки

Показано 5000 строк из 91346 — Отмечено 6 строк

!	Репу...	Начало	Конец	Хранилище	Транспорт	Протокол	IP-адрес отправителя	Порт отпра...	Домен отправителя	IP-адрес получателя	П
■		18.11.2019 13:47:55	18.11.2019 13:52:17		udp	dns	192.168.85.100	63601	www.nonamebank.com	8.8.8.8	5
■		18.11.2019 13:48:17	18.11.2019 13:51:40		udp	dns	192.168.85.100	64235	www.nonamebank.com	8.8.8.8	5
■		18.11.2019 13:48:40	18.11.2019 13:54:23		tcp	ldap	192.168.85.100	44594	exchange.nonamebank.com	192.168.85.1	3
■		18.11.2019 13:49:25	18.11.2019 13:52:56		udp	ldap	192.168.85.100	44880	proxy.nonamebank.com	192.168.85.1	3
■		18.11.2019 13:50:03	18.11.2019 13:51:21		udp	nbns	192.168.85.100	137		192.168.85.100	1
■		18.11.2019 13:50:41	18.11.2019 13:51:22		tcp	dcerpc	192.168.85.1	56862	api.nonamebank.com	192.168.85.1	49666
■		18.11.2019 13:50:41	18.11.2019 13:52:35		tcp	dcerpc	192.168.85.1	59184	api.nonamebank.com	192.168.85.1	49686
■		18.11.2019 13:50:59	18.11.2019 13:51:33		udp	nbns	192.168.85.100	137	api.nonamebank.com	192.168.85.100	137
■		18.11.2019 13:51:02	18.11.2019 13:51:36		udp	nbns	192.168.85.100	137		192.168.85.100	137

Расшифровать...

Дамп:

- отправить в хранилище...
- скачать в формате rsar...

Данные о сессиях:

- скачать в формате JSON
- скачать в формате CSV

Скачать извлеченные файлы...

Зарегистрировать инцидент

С выбранными

Расшифровать...

Дамп:

отправить в хранилище...

скачать в формате rsar...

Данные о сессиях:

скачать в формате JSON

скачать в формате CSV

Скачать извлеченные файлы...

6 кБ 2 кБ

9 кБ 23 кБ

6 кБ 0 Б

2 кБ 0 Б

dc.nonamebank.nonamebank.com  
00:50:56:A6:48:2E  
Windows: 7 or 8

# Нарушение регламентов ИБ



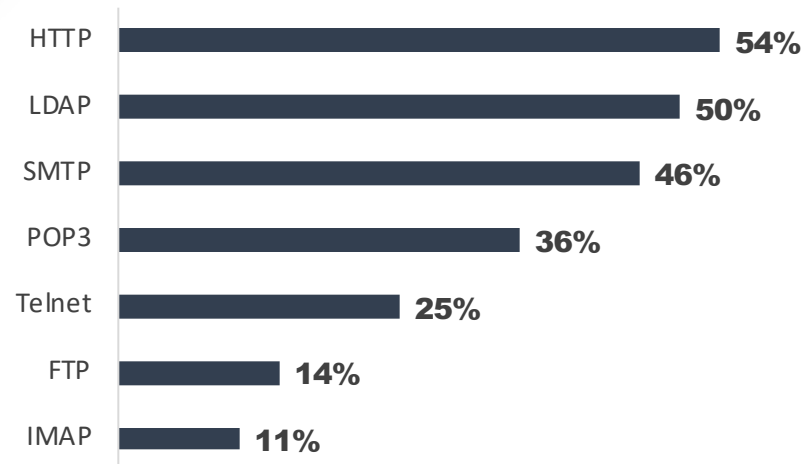
Пары "логин – пароль" по числу сессий

Логин	Пароль	Количество сессий
administrator	admin	57
service	1qaz!@WSX	51
smakarova@company.com	Qwerty123	25
aivanov@company.com	1qaz!@WSX	12
imironov@company.com	Qwerty123	9
vc-admin@company.com	1qaz!@WSX	3
cisco	123456	3
zabbix	zabbix	3

Нарушения регламентов ИБ встречалось нами в 96% случаев

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

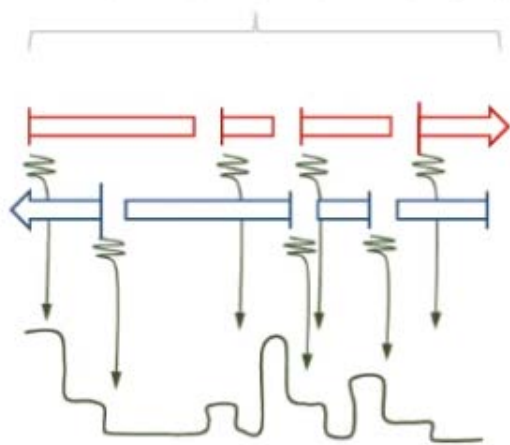
Незащищенные протоколы передачи чувствительных данных



# Наблюдение за внешним трафиком



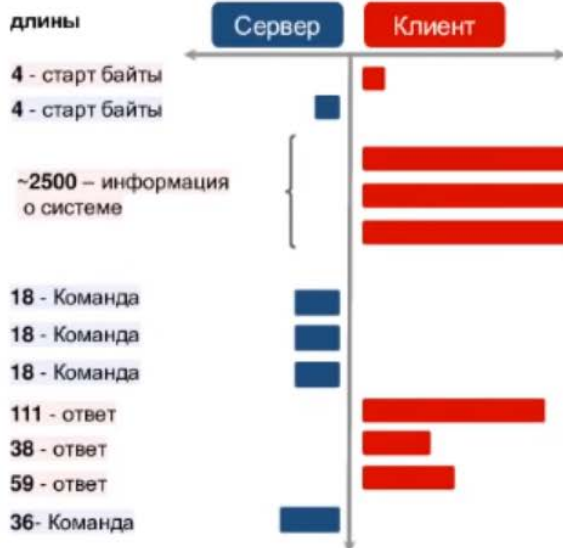
Сообщения (TCP, TLS, HTTP, any ...)



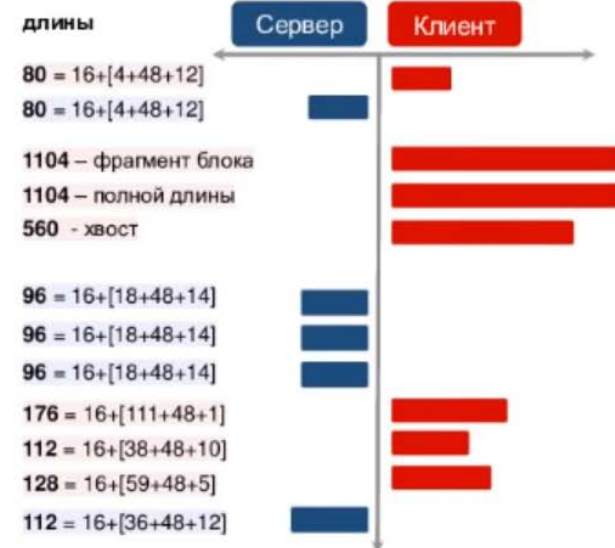
Побочный канал



## Открытый



## Зашифрованный



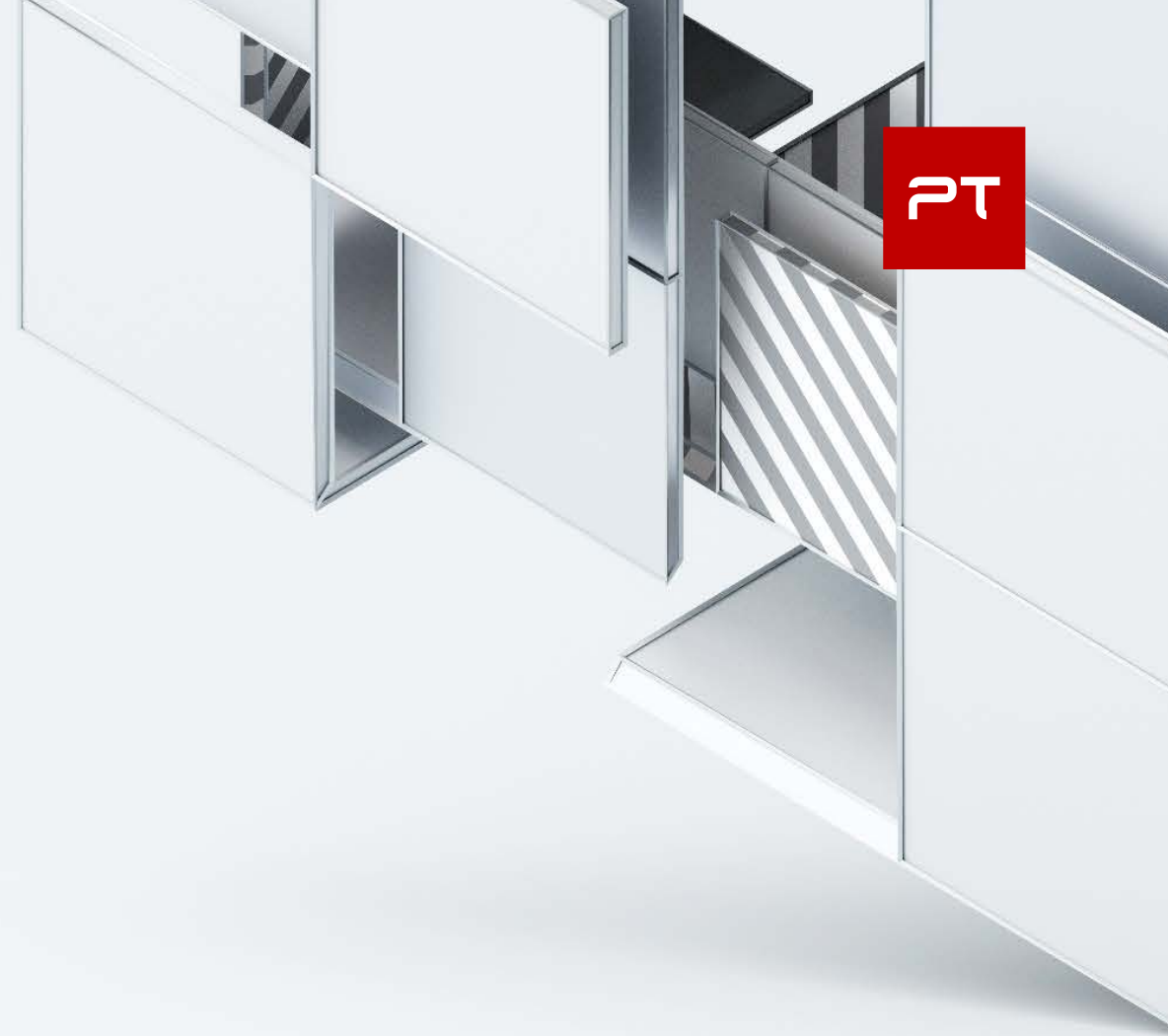
# Почему NTA это здорово

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

