

PT NAD 10.2

НОВЫЕ ВОЗМОЖНОСТИ ВЫЯВЛЕНИЯ
киберугроз с помощью анализа
трафика



Наталья Казанькова
старший менеджер
по продуктовому маркетингу



Кирилл Черкинский
Менеджер по продвижению
продуктов и поддержке продаж

Программа вебинара



1

Как в РФ компании защищаются от целевых атак? **РЕЗУЛЬТАТЫ ОПРОСА**

2

ОБЗОР PT NAD 10.2:

- детект большего количества угроз
- автоопределение роли и типа сетевого узла
- переход на DPDK
- кое-что еще

3

Маппинг PT NAD на матрицу **MITRE ATT&CK**

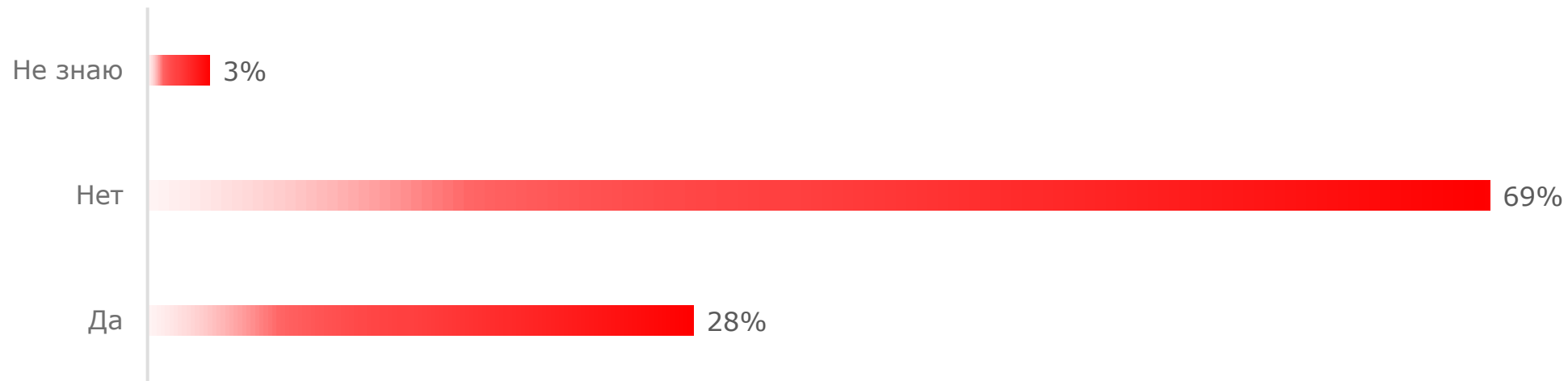
Как в России компании защищаются от целевых атак?

Результаты опроса

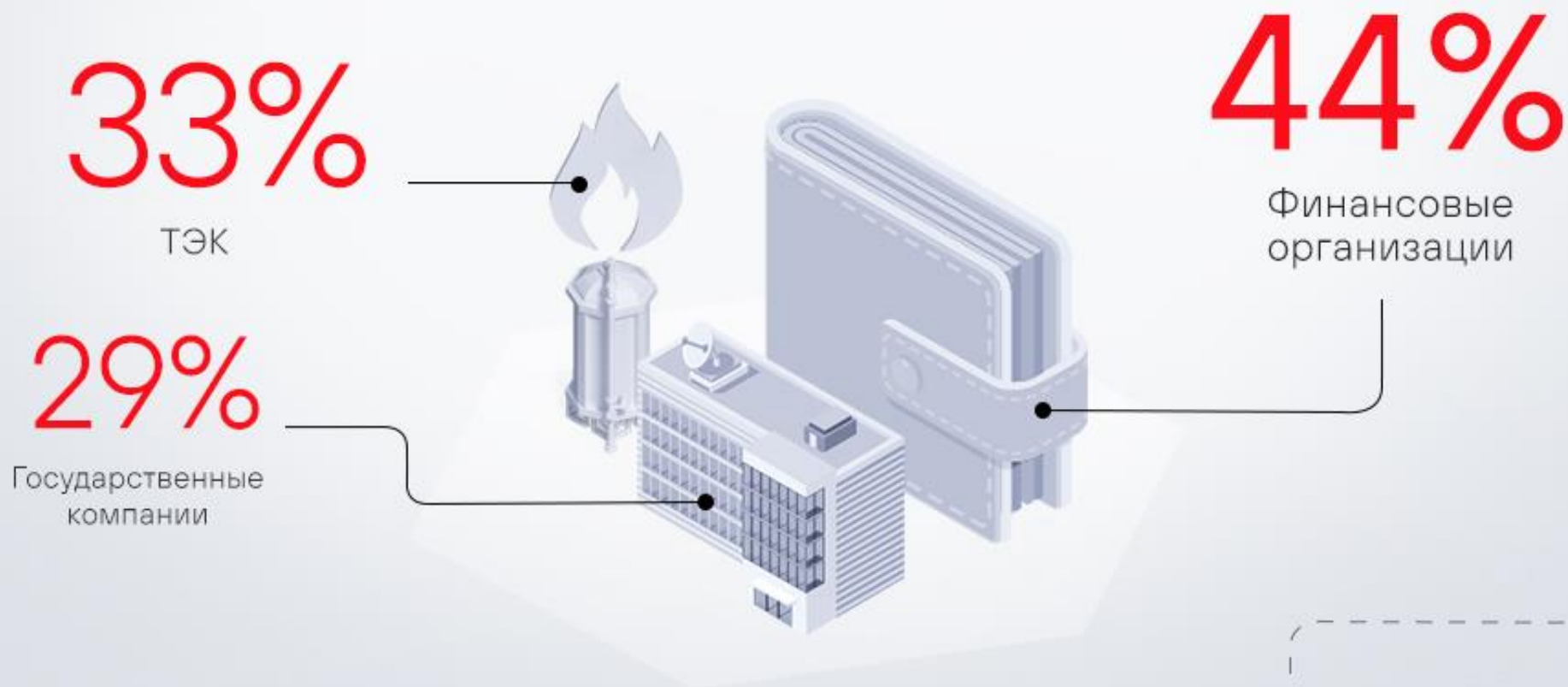


Кого уже атаковали?

СТАНОВИЛАСЬ ЛИ ВАША КОМПАНИЯ КОГДА-ЛИБО ЖЕРТВОЙ ЦЕЛЕВОЙ ИЛИ АРТ-АТАКИ?



Кого уже атаковали?



С какими последствиями кибератак сталкивалась ваша компания?



Защита от кибератак: сейчас и потом

**Какие системы ИБ
уже используются
в российских
компаниях / будут
использоваться
в течение 1-3 лет**

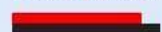


Согласно результатам опроса, проведенного
Positive Technologies

Комплексные решения для защиты от целевых атак (anti-APT) 15% / 26%



EDR 14% / 16%



SIEM 34% / 23%



Sandbox 28% / 22%



NGFW 41% / 18%



Network traffic analysis (NTA, NDR) 27% / 27%



WAF 32% / 13%



IDS/IPS 55% / 21%



Антивирус 89% / 22%



Другое 1,2% / 3,2%



NTA пока использует только
каждая четвертая компания
(27%)

Еще столько же компаний
планирует начать в течение
1-3 лет

Выводы

- Треть компаний когда-либо подвергалась целевой атаке, многие столкнулись с серьезными последствиями.
- В основном компании используют базовые средства защиты, у некоторых нет даже антивирусов. Лишь 10% респондентов имеют специализированные комплексные решения для защиты от целевых атак.
- Хорошие новости: арсенал средств выявления атак расширяется, у большинства компаний скоро будет NTA.

Полный отчет тут: ptsecurity.com/ru-ru/research/analytics/kak-rossijskie-kompanii-zashchishchayutsya-ot-celevyh-atak/

PT Network Attack Discovery 10.2

Лента активностей



Positive Technologies

ptsecurity.com



Активности для ленты

**ВЕРСИЯ
10.1**

Неизв. DHCP-сервер

Словарные пароли

Польз. уведомления

Ретроспектива

Новые активности для ленты

ВЕРСИЯ 10.1

Неизв. DHCP-сервер

Словарные пароли

Польз. уведомления

Ретроспектива

NEW!

АКТИВНОСТЬ ВРЕДОНОСНОГО ПО

Malware

Adware

Ransomware

Miner

NEW!

УДАЛЕННОЕ УПРАВЛЕНИЕ

AeroAdmin

Ammy Admin

AnyDesk

LiteManager

RMS

TeamViewer

PsExec

PowerShell

NEW!

УЧЕТНЫЕ ДАННЫЕ В ОТКРЫТОМ ВИДЕ

FTP

HTTP

LDAP

Mail

NEW

РАЗНОЕ

Tor

Scanners

Kali Linux OS

Burp Suite

Torrents

Telnet

LLMNR

NetBios

NEW!

VPN & PROXY

Socks5

PPTP VPN tunnel

OpenVPN

friGate Proxy

Hola VPN

PT Network Attack Discovery 10.2



Контроль сетевых узлов



Типы и роли узлов

ТИПЫ:

- Рабочие станции
- Серверы
- Мобильные устройства
- Принтеры
- Сетевые устройства

РОЛИ:

- | | | |
|---------------------|-----------------------|------------------------------|
| ■ Веб-сервер | ■ Сервер базы данных | ■ DHCP-сервер |
| ■ Виртуализация | ■ Сервер приложений | ■ DNS-сервер |
| ■ Контроллер домена | ■ Система мониторинга | ■ VPN |
| ■ Маршрутизатор | ■ Служба AAA | ■ WSUS |
| ■ Почтовый сервер | ■ Служба каталогов | ■ Антивирусный сервер |
| ■ Прокси-сервер | ■ Файловая служба | ■ Беспроводная точка доступа |

- Определяем автоматически
- Пока не определяем

PT Network Attack Discovery 10.2

НОВЫЕ ВОЗМОЖНОСТИ DPI



Positive Technologies

ptsecurity.com



Новые возможности DPI

ОБНАРУЖЕНИЕ АТАК СКАНИРОВАНИЯ, ФЛУДА И DDOS

- PT NAD теперь создает одну запись сессии с объединенной информацией
- Защита от переполнения базы данных
- Повышение стабильности работы сенсора

The screenshot displays the PT NAD interface with the following elements:

- Top Bar:** Shows the session ID `10.0.213.20 → 53 251 IP-адрес`.
- Left Sidebar:** Contains tabs for **Общие сведения** (General) and **Расширенные сведения** (Advanced).
- Main Content Area:**
 - Общая информация (General Information):**
 - Протоколы: tcp
 - Начало: 30 сентября 2021, 12:00:13
 - Конец: 30 сентября 2021, 12:06:16
 - Длительность: 6 минут 3 секунды
 - Отправлено: 33 МБ, 544 808 пакетов
 - Получено: 9 КБ, 146 пакетов
 - Отправитель: H17200
 - Получатели: 53 251 IP-адрес
 - 5 портов: 22 – 443
 - Сессий: 526 291 (1450 в секунду)
 - Особенность обработки сессии (Session Processing Feature):** MULTI_FLOW: Сессии объединены на основании общих признаков.
 - Атаки (Attacks):**
 - [ANOMALY] [PTsecurity] TCP SYN scan FINISHED
 - Unknown Traffic
 - [ANOMALY] [PTsecurity] TCP SYN scan
 - Unknown Traffic
- Right Sidebar:** Contains actions: **Зарегистрировать инцидент**, **Отправить в хранилище**, **Скачать дампы**, **Скачать файлы**, and **Скопировать ссылку**.

Новые возможности DPI

РАЗБОР ПРОТОКОЛОВ ПРИ ПОТЕРЯХ ДАННЫХ В СОЕДИНЕНИЯХ:

Разбор соединения продолжается даже при потере данных (применимо к HTTP, FTP, DCE/RPC, SMTP, POP3, IMAP)

НОВЫЕ ПРОТОКОЛЫ:

ОПРЕДЕЛЕНИЕ:

- Elasticsearch
- Printer-ps (Raw PostScript TCP Printing)

РАЗБОР:

- MySQL
- Oracle TNS
- PostgreSQL

MySQL

Server version 5.7.24
Database AIWEDB
User alednyov

Client attributes

_os Win32
_client_name libmysql
_pid 14844
_thread 10628
_platform AMD64
_client_version 5.7.11

Oracle TNS

Application name apache2@we-oracle-php (TNS V1-V3)
Database WTST
User system
Connection string (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=10.0.212.186)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=WTST)(CID=(PROGRAM=apache2)(HOST=we-oracle-php)(USER=www-data))))

Parameters

AUTH_MACHINE we-oracle-php
AUTH_SID www-data
SESSION_CLIENT_DRIVER_NAME PHP OCI8 2.0.10
AUTH_SC_SERVER_HOST we-orcl-11
AUTH_SC_DBUNIQUE_NAME WTST
AUTH_SC_INSTANCE_NAME wtst
AUTH_SC_SERVICE_NAME WTST

PostgreSQL

Application name pgAdmin 4 - DB:KnowledgeBase
Server version 12.2 (Debian 12.2-2.pgdg100+1)
Database KnowledgeBase
User pt_system
Superuser true

Новые возможности DPI

ЗАХВАТ ТРАФИКА ПРИ ПОМОЩИ DPDK

- Высокая скорость обработки без потерь
- Эффективная утилизация всех аппаратных ресурсов

АВТОМАТИЧЕСКАЯ ПРИВЯЗКА ЯДЕР CPU К ПОТОКАМ PT DPI

- Теперь можно настроить привязку в автоматическом режиме
- В том числе для DPDK

ПОДДЕРЖКА СЕТЕВЫХ КАРТ NVIDIA MELLANOX

- Сенсор теперь может работать с сетевыми картами NVIDIA Mellanox

PT Network Attack Discovery 10.2

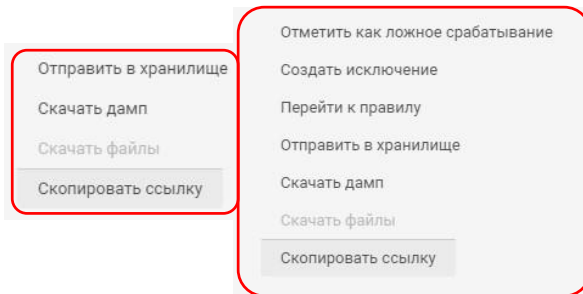
Другие улучшения



Другие улучшения версии 10.2

ССЫЛКИ НА КАРТОЧКИ СЕССИЙ И АТАК

- Ссылка на карточки сессий и атак формируется в адресной строке
- Возможность скопировать ссылку в карточке



API ДЛЯ ПРОСМОТРА РЕПУТАЦИОННЫХ СПИСКОВ

- Доработали API для упрощения работы с динамическими репутационными списками

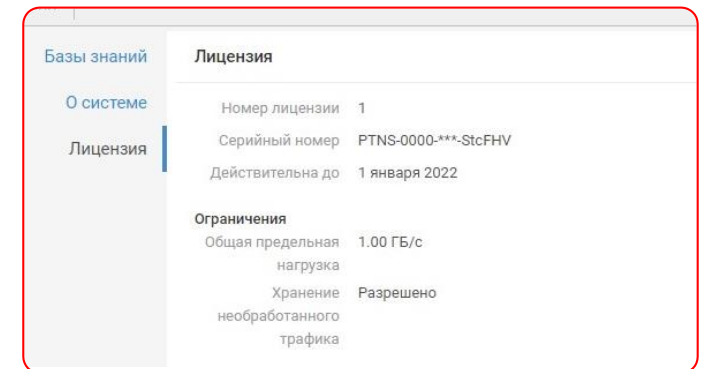
```
GET /api/v2/replists/dynamic/<external_key>
```

ФИЛЬТРАЦИЯ СПИСКА АТАК

- Дубликаты и попадающие в исключения атаки больше не отправляются в MaxPatrol SIEM

УПРАВЛЕНИЕ ЛИЦЕНЗИЕЙ В ИНТЕРФЕЙСЕ

- Просмотр данных о лицензии в UI
- Возможность добавить или изменить лицензию в UI
- Уведомление о проблемах с лицензией



PT Network Attack Discovery

и MITRE ATT&CK



Кто знает про MITRE ATT&CK?

Поставьте + в чат, если пользуетесь матрицей MITRE ATT&CK

MITRE ATT&CK

База знаний, разработанная и поддерживаемая компанией MITRE на основе анализа реальных АРТ-атак. Это структурированный в виде наглядной таблицы список тактик, для каждой из которых указаны возможные техники.

<https://attack.mitre.org/>

ATT&CK Matrix for Enterprise								
<div> <div>layout: side ▾</div> <div>show sub-techniques</div> <div>hide sub-techniques</div> </div>								
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques	15 techniques	29 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (6)	Create Account (3)	Domain Policy Modification (2)	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Escape to Host	Execution Guardrails (1)	Modify Authentication Process (4)	Container and Resource Discovery
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Event Triggered Execution (15)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery
Search Victim-Owned Websites			System Services (2)	Exploitation for Privilege Escalation	Hijack Execution Flow (11)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Discovery
			User Execution (3)	External Remote Services		Hide Artifacts (9)	Steal Application	Group Policy Discovery
			Windows Management Instrumentation	Hijack		Hijack Execution Flow (11)		Network Service Scanning

MITRE ATT&CK

База знаний, разработанная и поддерживаемая компанией MITRE на основе анализа реальных АРТ-атак. Это структурированный в виде наглядной таблицы список тактик, для каждой из которых указаны возможные техники.

<https://attack.mitre.org/>

ATT&CK Matrix for Enterprise

Тактики, цели, задачи атакующих

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	BITS Jobs	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (15)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (6)	Create Account (3)	Domain Policy Modification (2)	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Domain Policy Modification (2)	Execution Guardrails (1)	Modify Authentication Process (4)	Container and Resource Discovery
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Escape to Host	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery
Search Victim-Owned Websites			System Services (2)	Exploitation for Privilege Escalation	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Discovery
			User Execution (3)	External Remote Services	Hijack Execution Flow (11)	Hide Artifacts (9)	Steal Application	Group Policy Discovery
			Windows Management Instrumentation	Hijack		Hijack Execution Flow (11)		Network Service Scanning

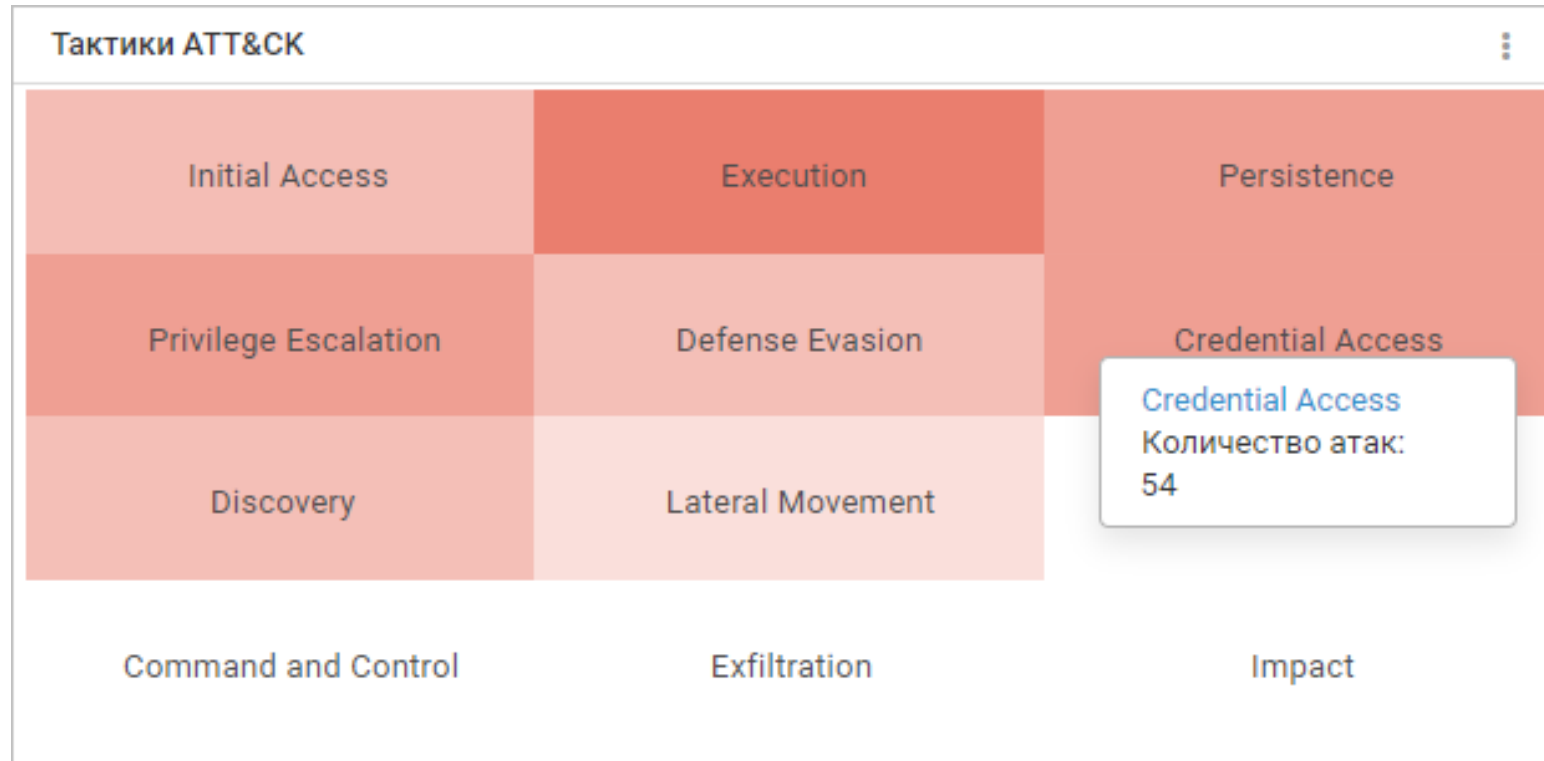
Техники, конкретные действия атакующих

Зачем нужна ATT&CK?

Общие сведения	
Обнаружена	30.11.2019 00:54:26
Название	ATTACK [PTsecurity] Exim 4.87 < 4.91 RCE via LPE (CVE-2019-10149)
Опасность	Высокая
SID	10004894 Ревизия 1
Класс	Attempted Administrator Privilege Gain
<div> <div> Атакующий узел 4.0.10.6 [AS3356 Level 3 Parent, LLC] (US) США </div> <div> → Атакуемый узел 92.243.167.182 mx-01.child-invlrbl.com [AS15582 OJSC Comcor] (RU) Россия, Moscow </div> </div>	
Тактики и техники ATT&CK	
Initial Access Exploit Public-Facing Application	
Описание и рекомендации	
Описание	Эксплуатация уязвимости в Exim (CVE-2019-10149), которая позволяет злоумышленникам, действующим удаленно, повысить уровень своих привилегий и выполнить произвольный код в системе.
Рекомендации	Проверить версию Exim, обновить если нужно. Версии начиная с 4.92 не подвержены уязвимости.
См. также	CVE-2019-10149 github.com/dhn/exploits/tree/master/CVE-2019-10149

Карточка атаки в PT NAD

Зачем нужна ATT&СК?



Тепловая карта на дашборде РТ NAD

Популярность ATT&CK в России

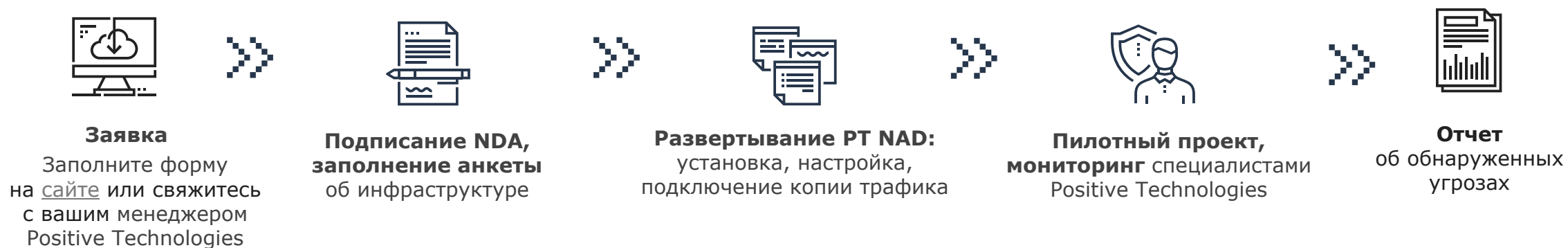
**ИСПОЛЬЗУЕТЕ ЛИ ВЫ В ПРОЦЕССЕ МОНИТОРИНГА,
РЕАГИРОВАНИЯ И РАССЛЕДОВАНИЯ АТАК МАТРИЦУ
MITRE ATT&CK?**



67% опрошенных
либо уже пользуются
данными матрицы,
либо планируют
начать

<https://mitre.ptsecurity.com/>

Как провести пилот PT NAD



≈ 4 недели

ПИЛОТ:

ptsecurity.com/ru-ru/products/network-attack-discovery/#free-demo



В 100% компаний выявлены нарушения регламентов ИБ, в 90% — подозрительная активность

ptsecurity.com/ru-ru/research/analytics/top-ugroz-ib-v-korporativnyh-setyah-2021/



Полезные ссылки



Задать вопрос, следить
за новостями PT NAD:
t.me/PTNADChat

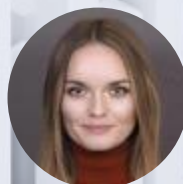
Маппинг PT NAD на ATT&CK:
mitre.ptsecurity.com

Как компании защищаются
от целевых атак:
[отчет по итогам
исследования](#)

Обновить версию:
support.ptsecurity.com

ПИЛОТ:

ptsecurity.com/ru-ru/products/network-attack-discovery/#free-demo



Наталия Казанькова
старший менеджер
по продуктовому маркетингу



Кирилл Черкинский
менеджер по продвижению
продуктов и поддержке продаж
Kcherkinskiy@ptsecurity.com