Offensive Security

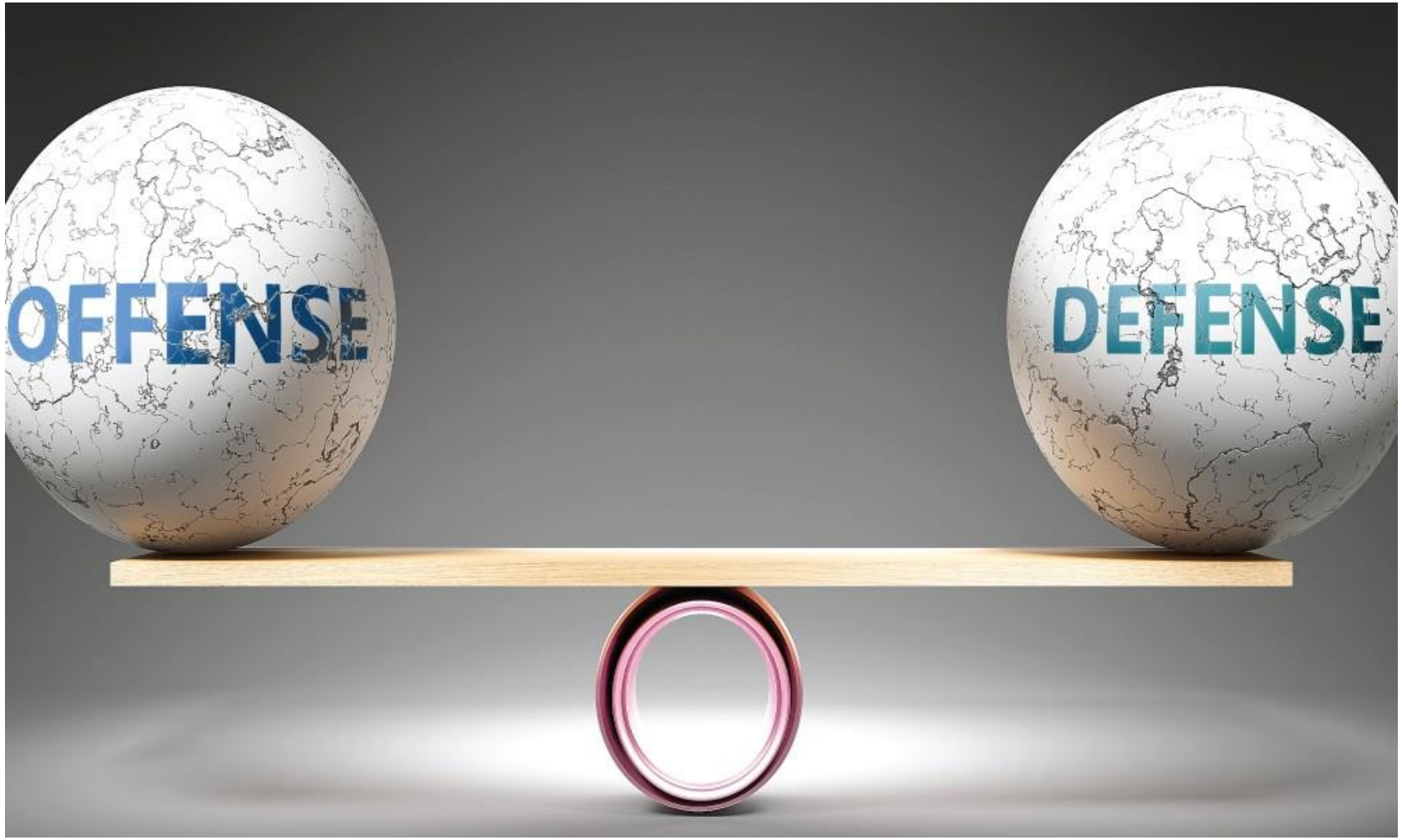
Penetration Testing

Кто я

- Пентестер в Positive Technologies
- Участник команды экспертов PT SWARM
- Обладатель сертификатов OSCP, OSEP

- https://t.me/ashvets0v

Offensive & Defensive

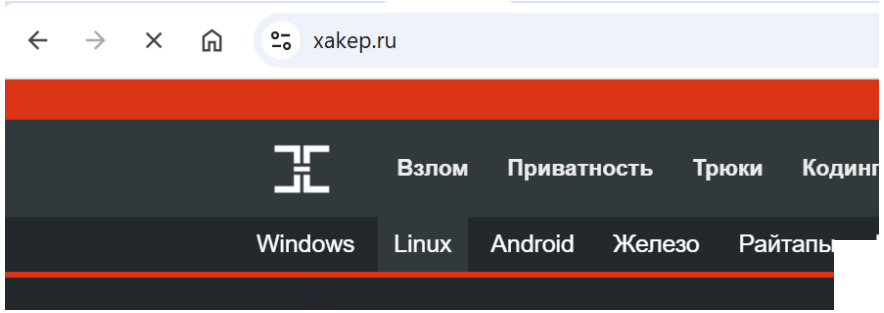


Виды offensive

Black Hat
Hacking

Виды offensive

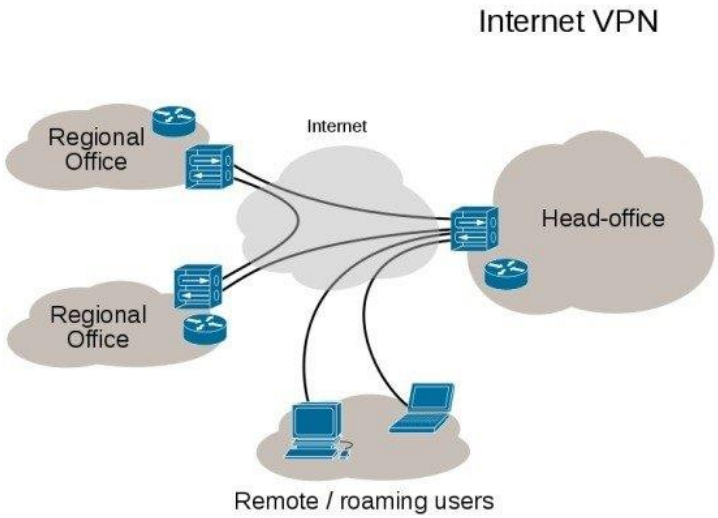
Веб-приложения



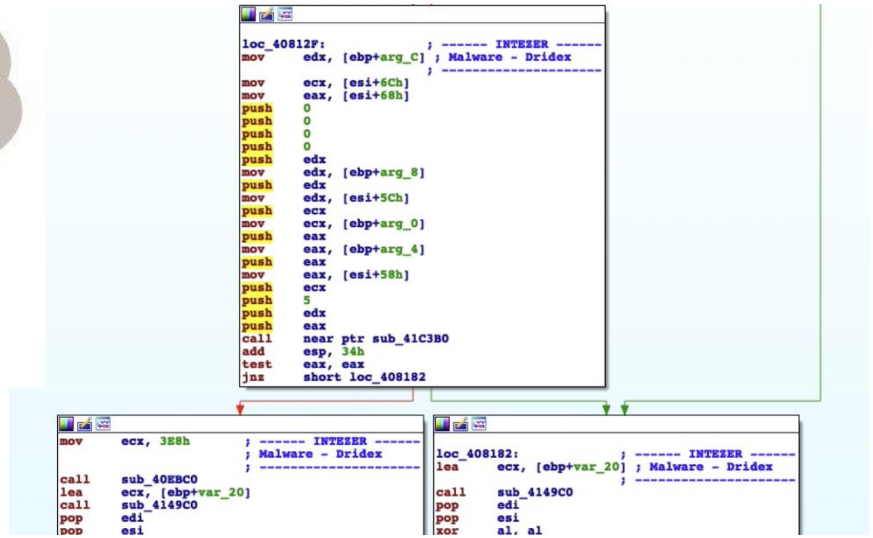
Мобильные приложения

ДБО

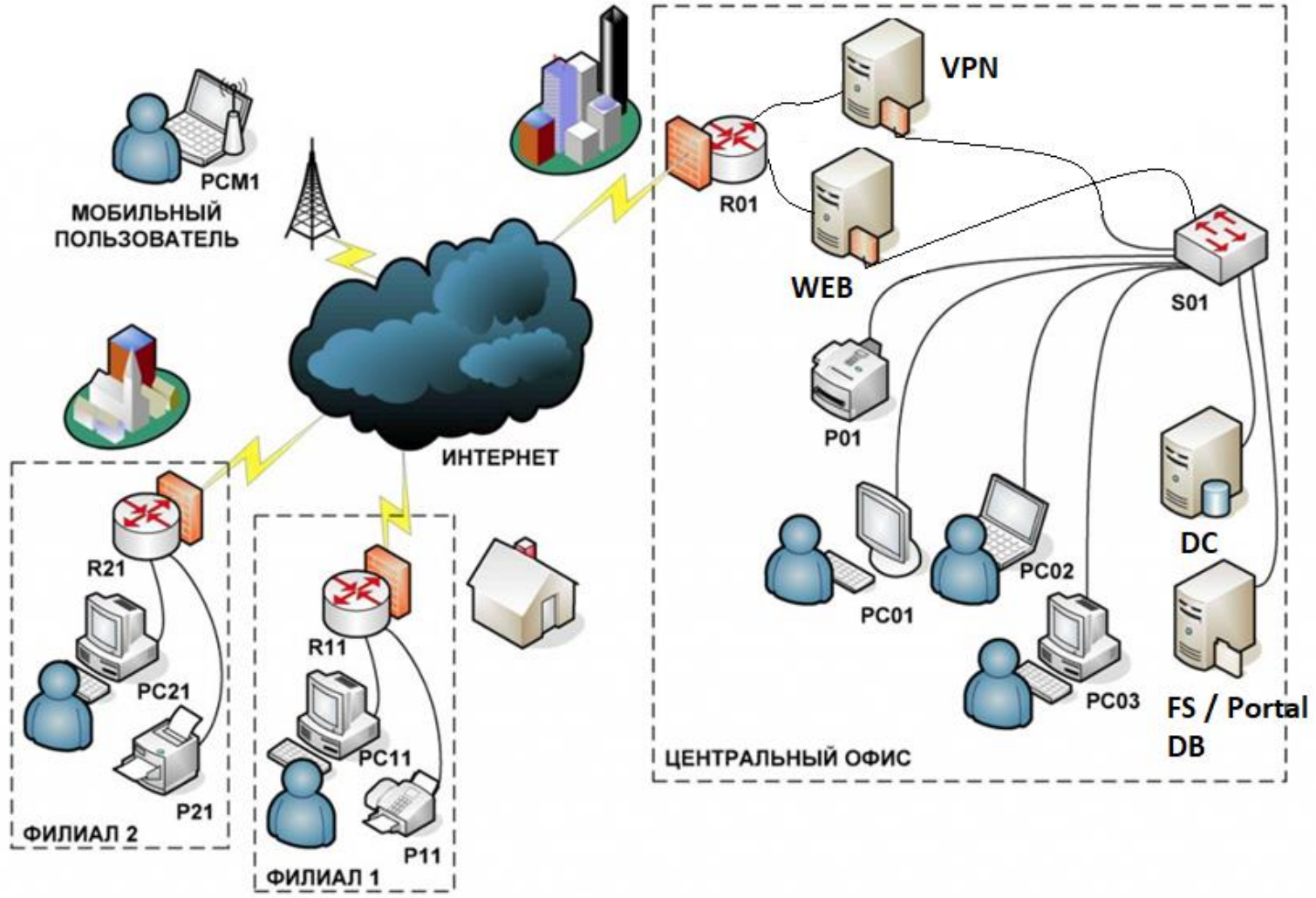
Pentest



Reverse Engineering



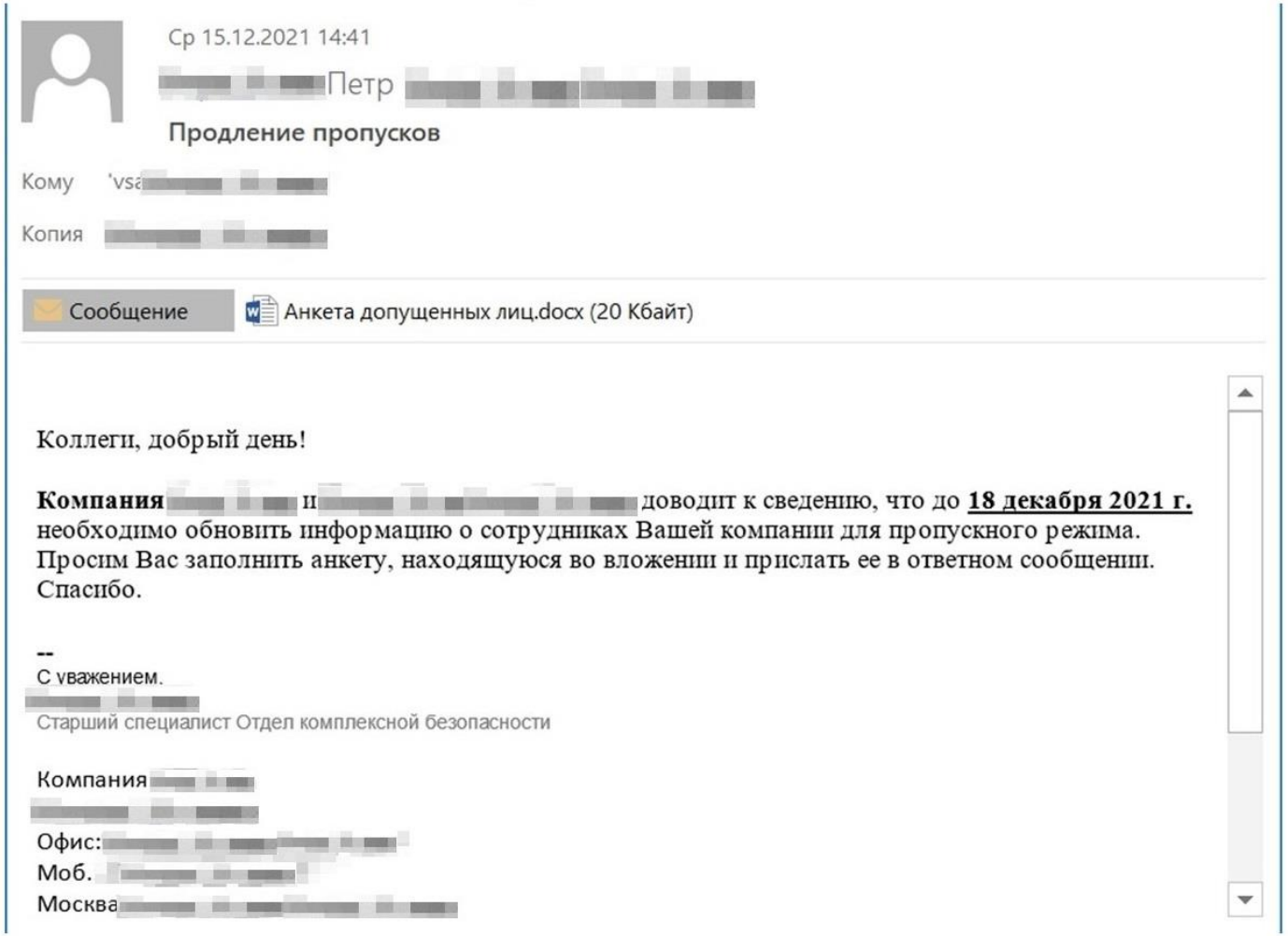
Как выглядит организация



Этапы проведения атаки

- Разведка (OSINT)
- Первичный доступ (Initial Access)
- Закрепление в сети (Persistence)
- Перемещение внутри периметра (Lateral movement)
- Повышение привилегий (Privilege Escalation)
- Реализация целей

Социальная инженерия



Ср 15.12.2021 14:41

[redacted]Петр [redacted]

Продление пропусков

Кому 'vs[redacted]

Копия [redacted]

Сообщение | Анкета допущенных лиц.docx (20 Кбайт)

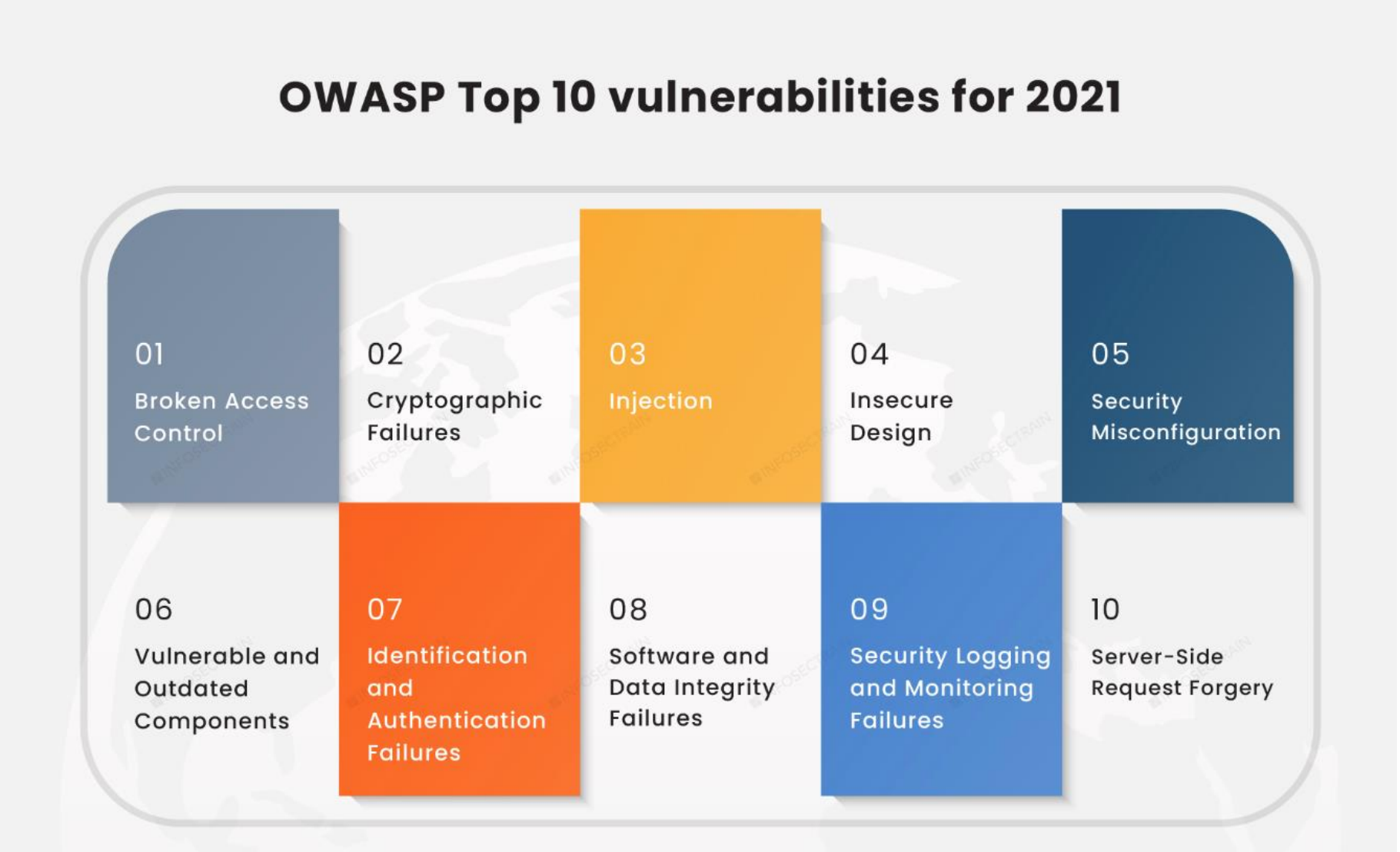
Коллеги, добрый день!

Компания [redacted] и [redacted] доводит к сведению, что до **18 декабря 2021 г.** необходимо обновить информацию о сотрудниках Вашей компании для пропускного режима. Просим Вас заполнить анкету, находящуюся во вложении и прислать ее в ответном сообщении. Спасибо.

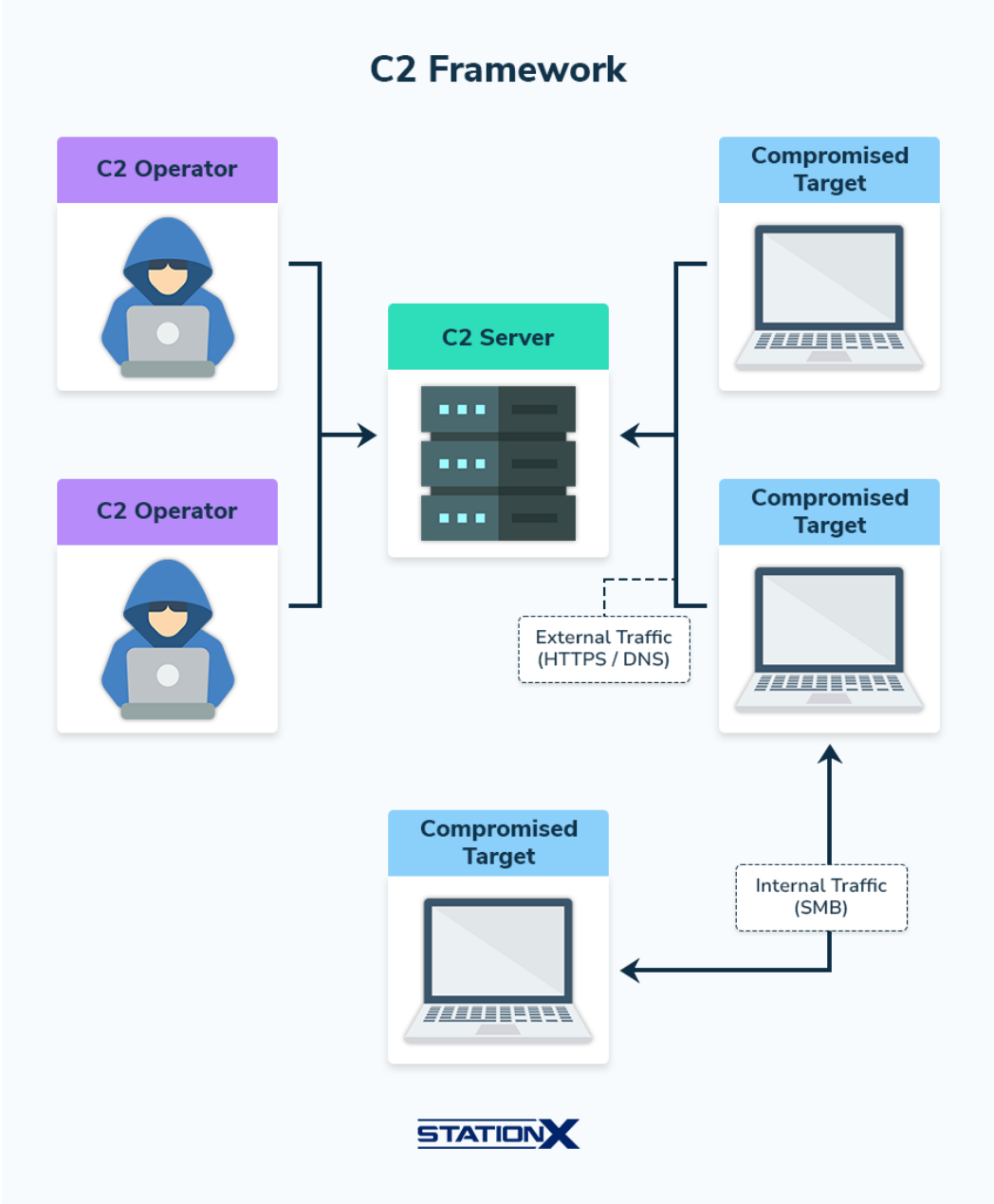
--
С уважением.
[redacted]
Старший специалист Отдел комплексной безопасности

Компания [redacted]
[redacted]
Офис: [redacted]
Моб. [redacted]
Москва [redacted]

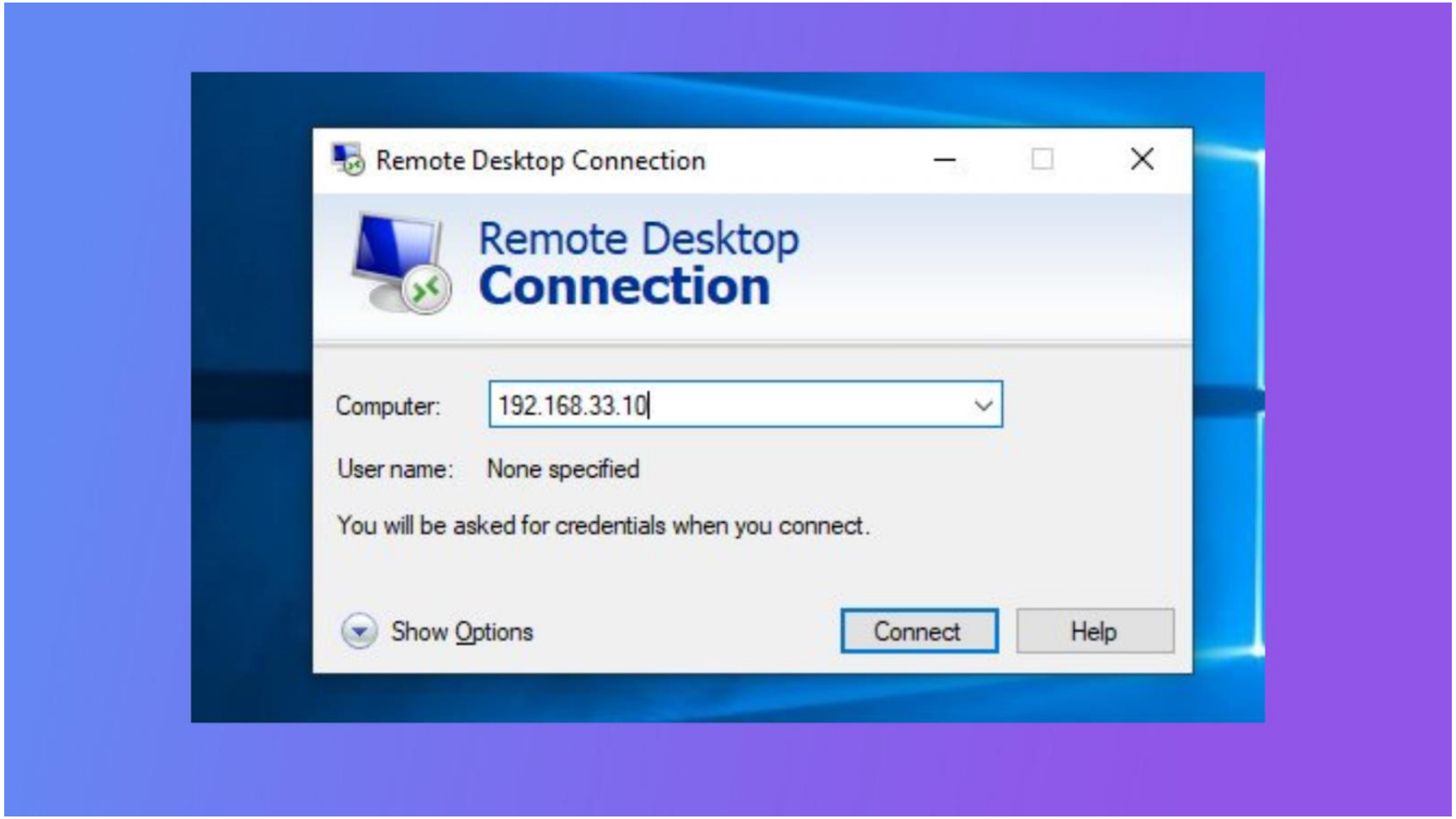
Уязвимости на периметре



Закрепление

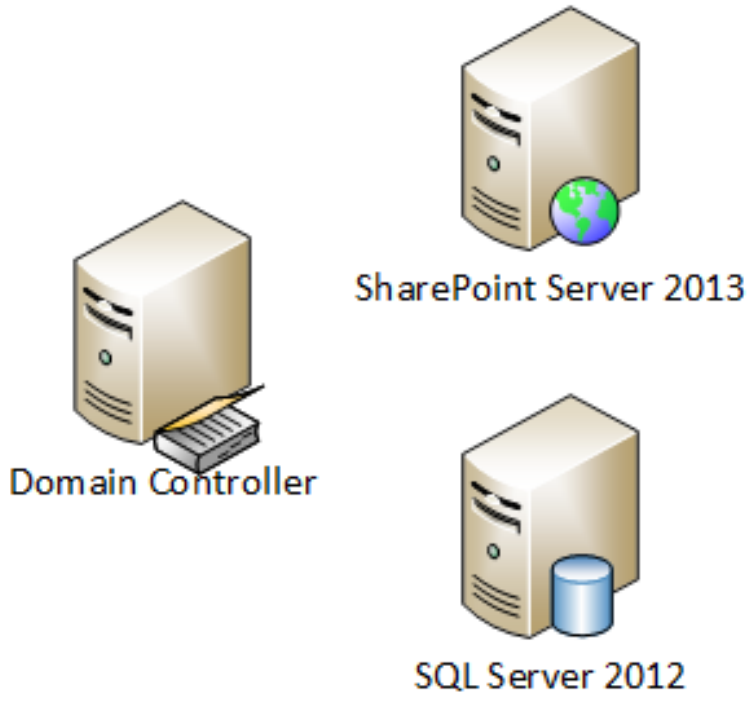


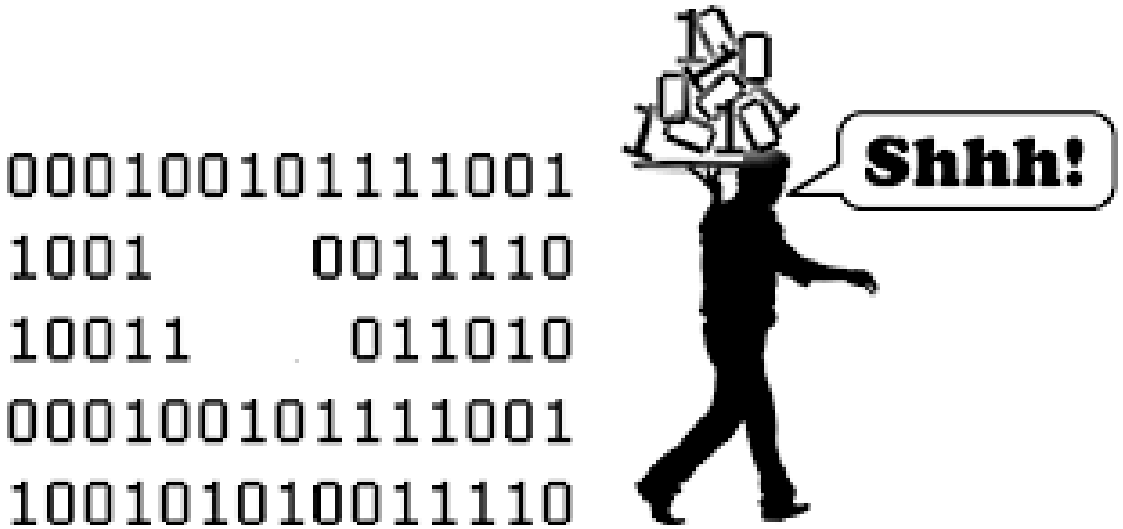
Перемещение внутри периметра



Повышение привилегий

Реализация целей





Особенности работы белого хакера

- Постоянное обучение (статьи, новые уязвимости, новые технологии, и т.д.)
- Интересные и разноплановые задачи
- Работа в сильной команде, обмен опытом
- Возможность участия в конференциях, командировки, выступления
- Прохождение сертификаций и обучений (OSEP, OSCP, OSWE и т.д.)
- Обмен опытом с командой защитников (SOC), помощь в развитии продуктов защиты

* Всё вышесказанное применимо к моей команде в Positive Technologies

Сообщество

Где работать?

Профильные компании:

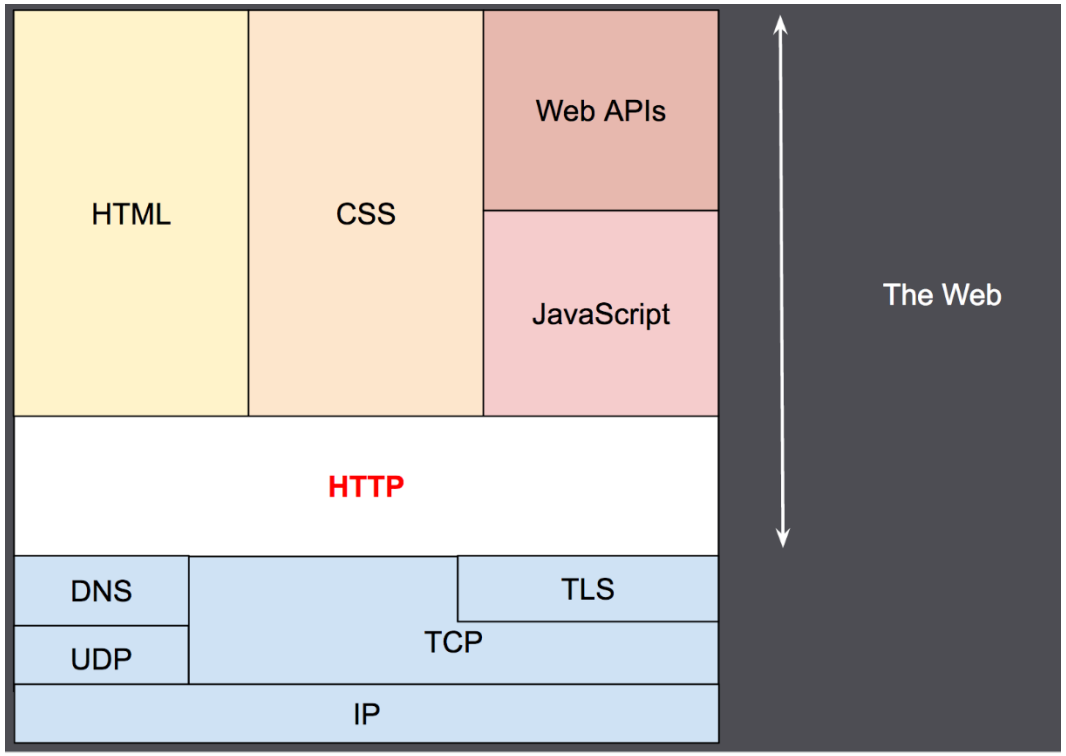
- Positive Technologies
- BI.ZONE
- Лаборатория Касперского
- Ростелеком-Солар
- и другие

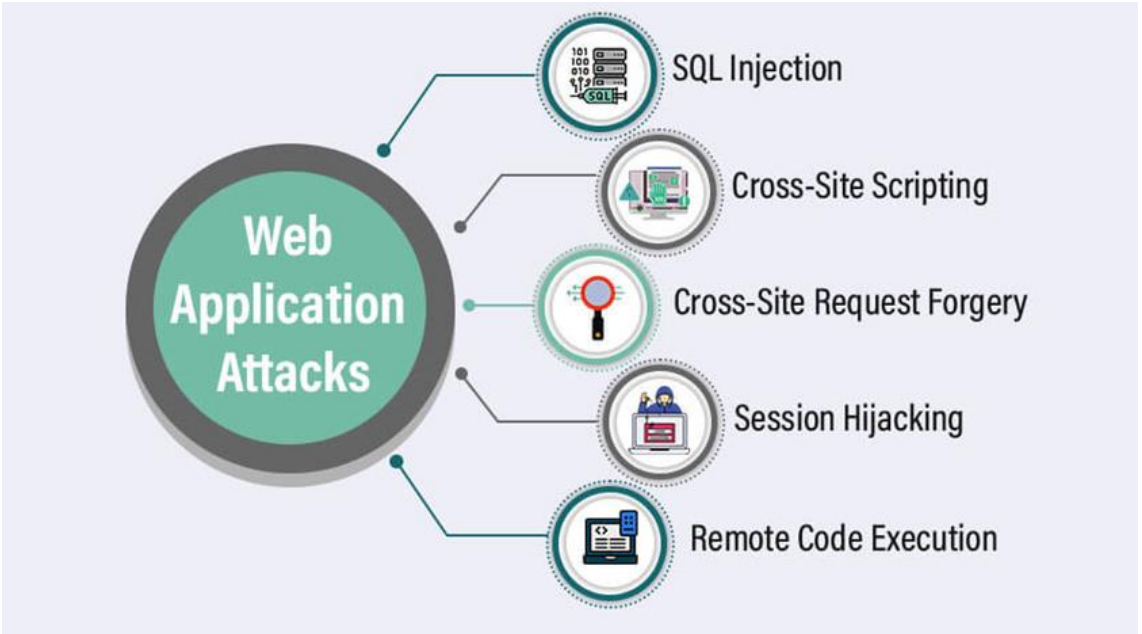
Bug Bounty:

- Standoff Bug Bounty
- BI. ZONE Bug Bounty

Навыки

Изучаем технологию –> Изучаем аспекты её безопасности

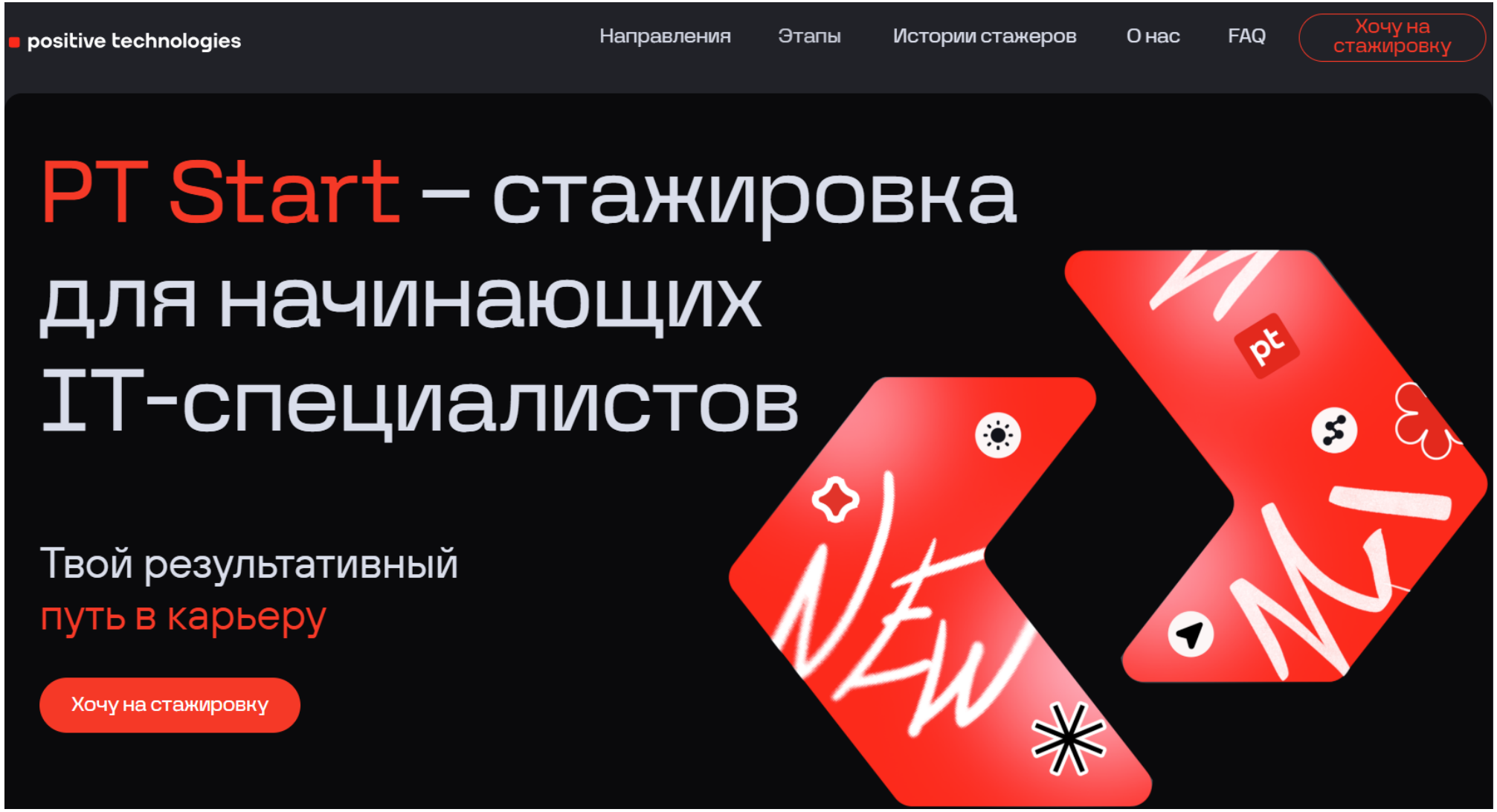




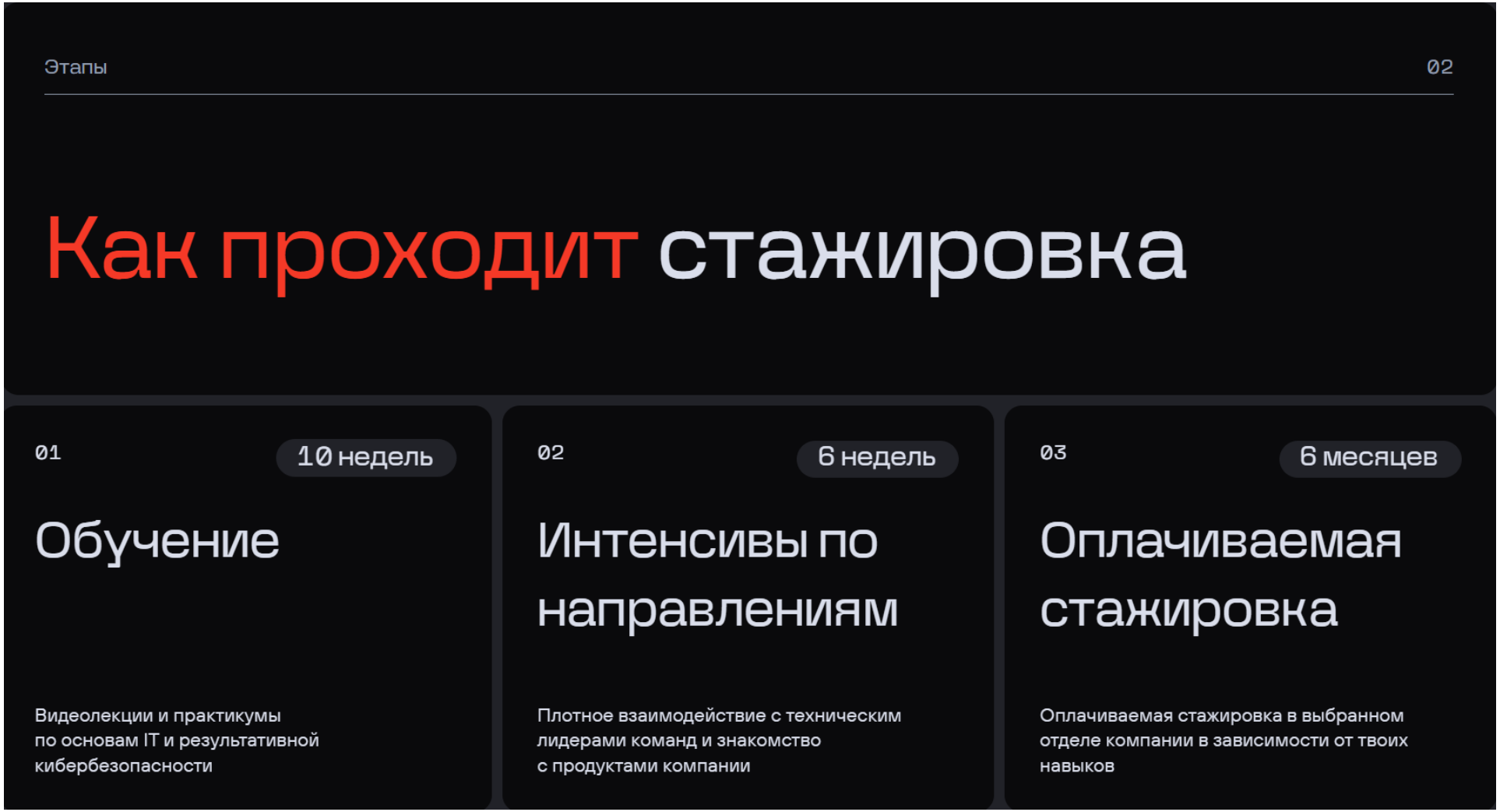
Навыки

- English (как минимум чтение статей)
- Системное администрирование (Windows, Linux)
- Программирование (python, bash, powershell)
- Компьютерные сети, протоколы (TCP, UDP, IP, HTTP)
- Знание уязвимостей (OWASP TOP 10, https://portswigger.net/web-security и т.д.)
- Понимание инфраструктуры компании (Active Directory, Kerberos)
- Тренировки (CTF, лабораторные, стажировки)

Стажировка: PT Start



Стажировка: PT Start

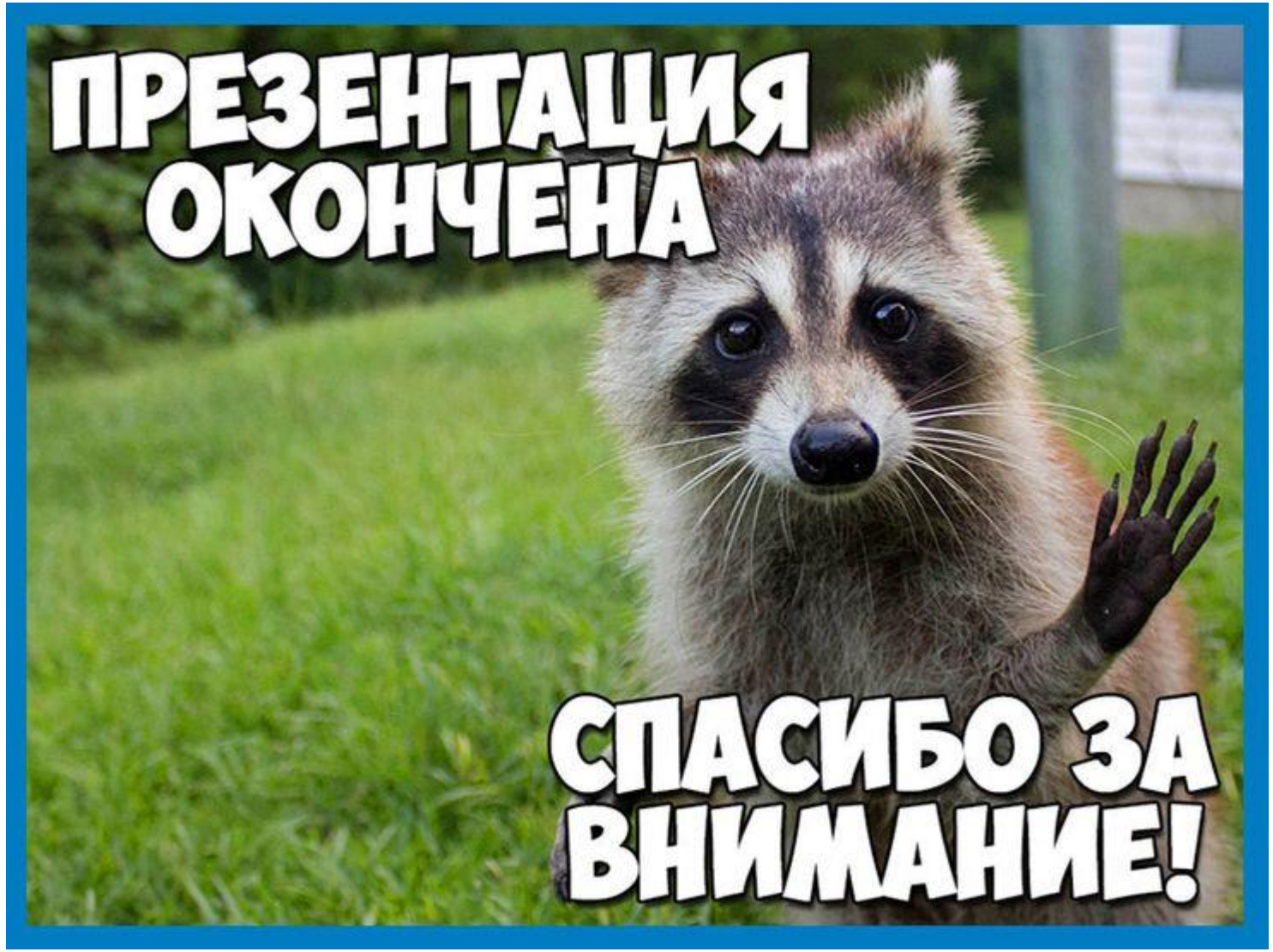


Полезные ресурсы: задания

- https://2019.hackerdom.ru/ - задачки
- https://ctftime.org/ - информация о CTF
- https://sql.training.hackerdom.ru/ - простой SQL injection квест для новичков
- https://exploit.education/ - интересные задания
- https://www.root-me.org/?lang=ru – интересные задания
- Площадок для обучения очень много, можно читать подборки сними, например: https://habr.com/ru/articles/538766/

Полезные ресурсы: углубленные

- https://ardent101.github.io/ - атаки на Active Directory и не только на русском
- https://portswigger.net/web-security - обучение и лабораторные по вебу
- Hack the box – лабораторные
- t.me/OffensiveTwitter, t.me/RedTeambro – продвинутые телеграмм каналы по пентесту
- Журнал Хакер


ПРЕЗЕНТАЦИЯ
ОКОНЧЕНА
СПАСИБО ЗА
ВНИМАНИЕ!