SOC
FORUM
2023

Полуоткрытый контур

Денис Гойденко

МОСКВА 2023

SOC
FORUM
2023

Денис Гойденко

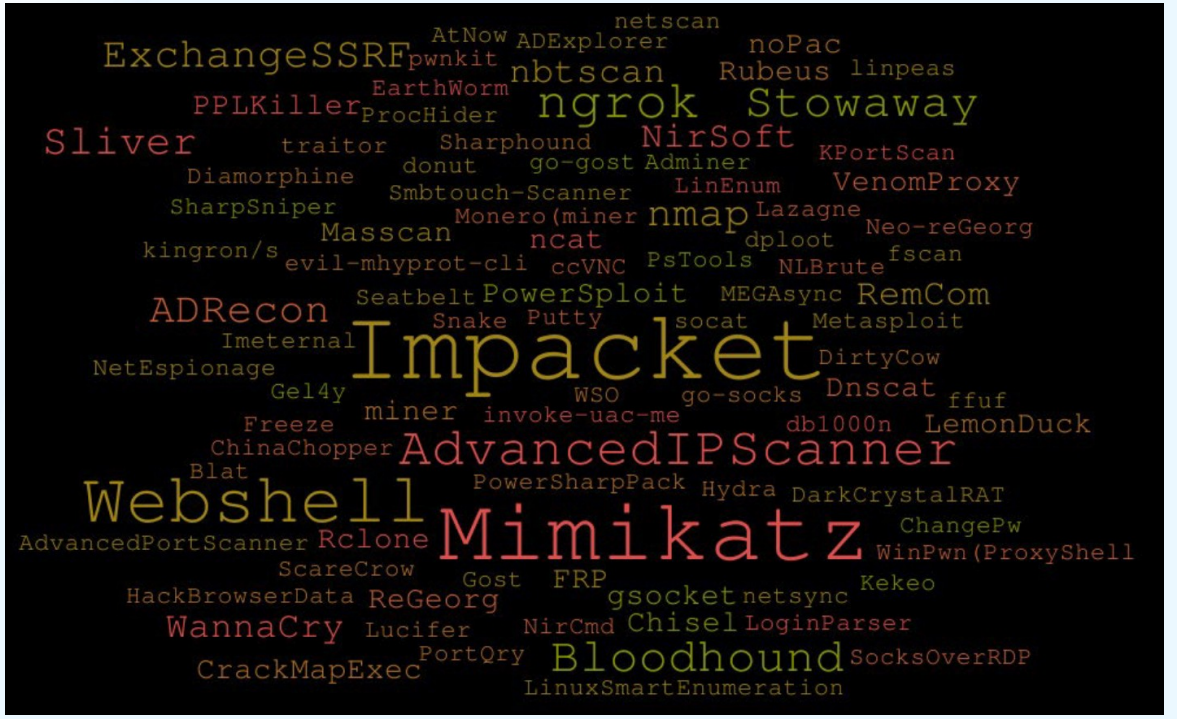
Руководитель отдела реагирования на угрозы ИБ
экспертного центра безопасности Positive Technologies
(PT ESC)

Positive Technologies

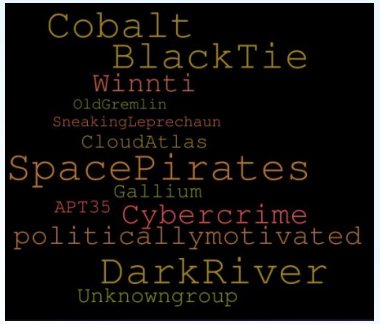
60%

За девять месяцев 2023 года — на 60% больше инцидентов, чем за весь 2022 год*

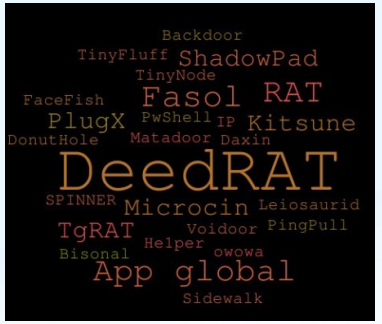
Утилиты



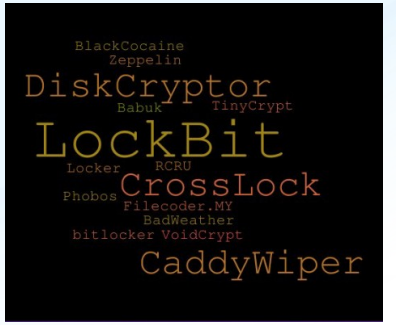
APT-группировки



APT-утилиты



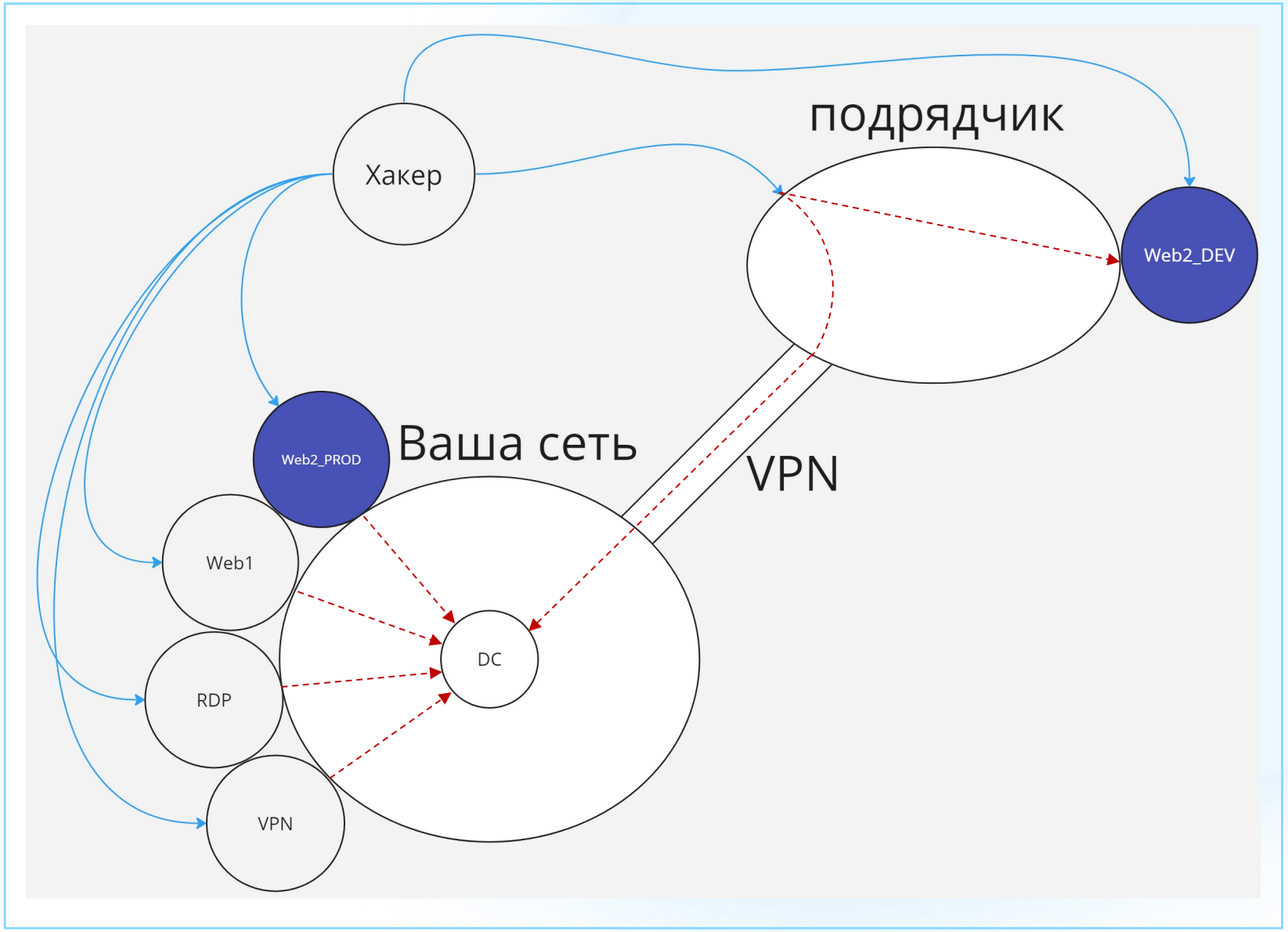
Шифровальщики



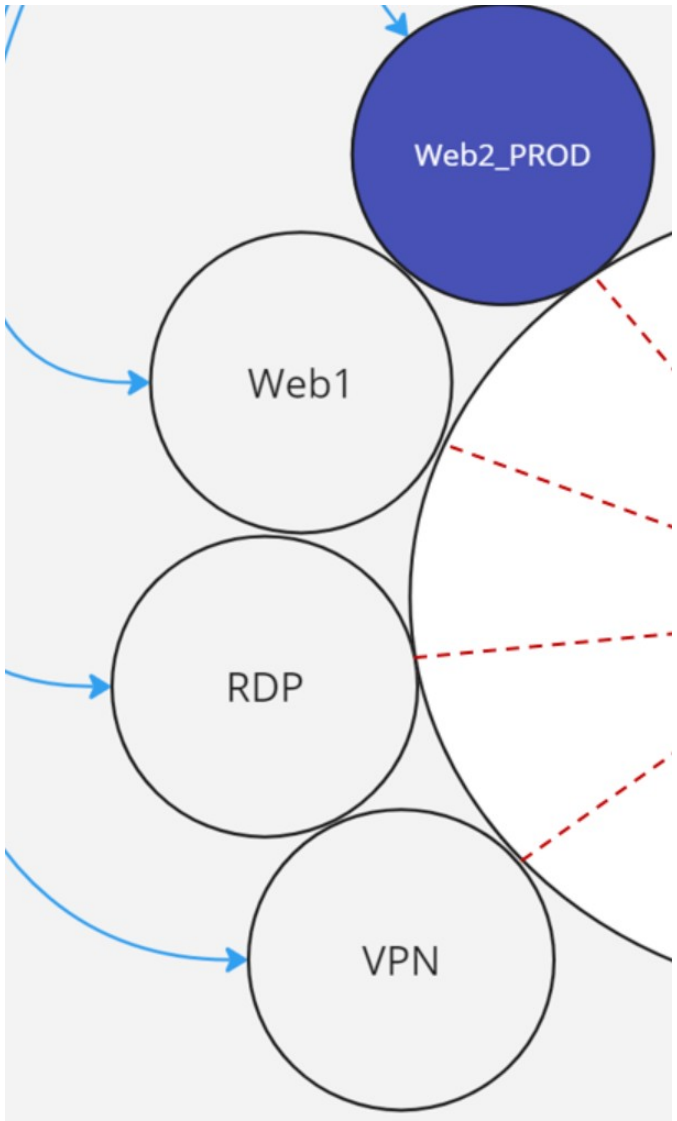
*На основе экспертизы и расследований Positive Technologies

1. Ошибки снаружи
2. Ошибки внутри
3. Ошибки на узле и общее

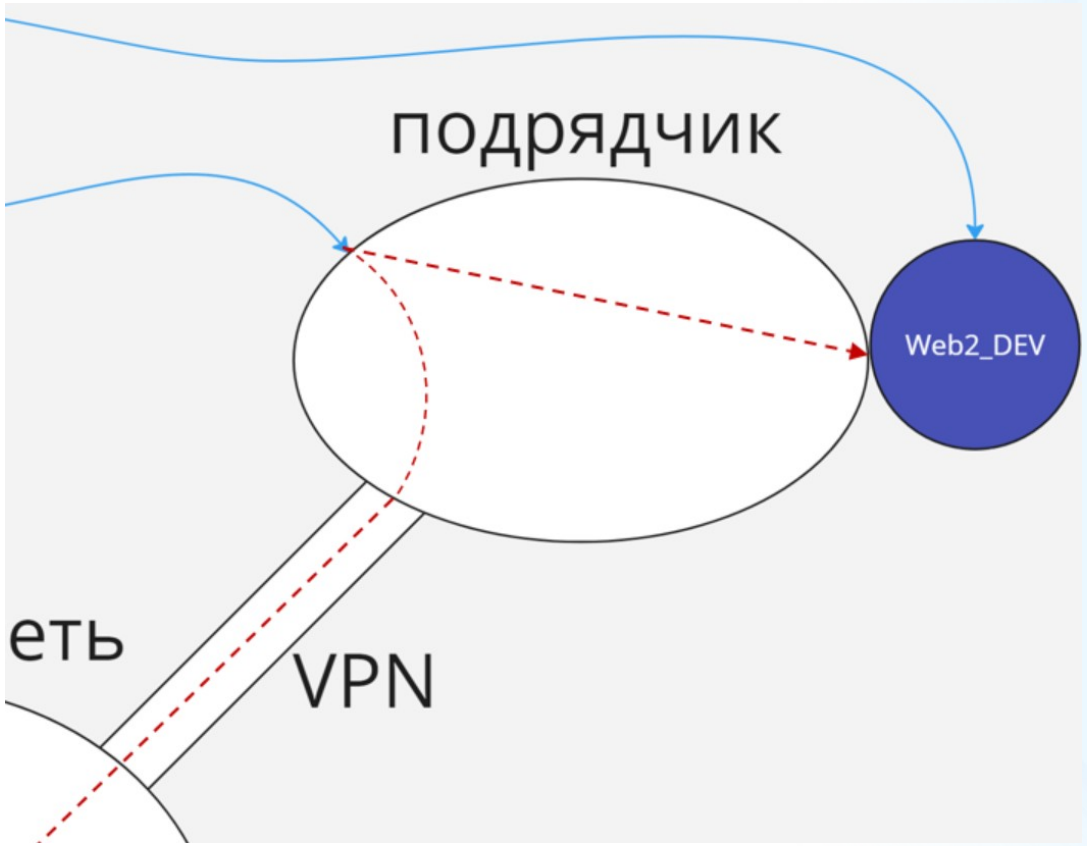
Ошибки снаружи



Ошибки снаружи

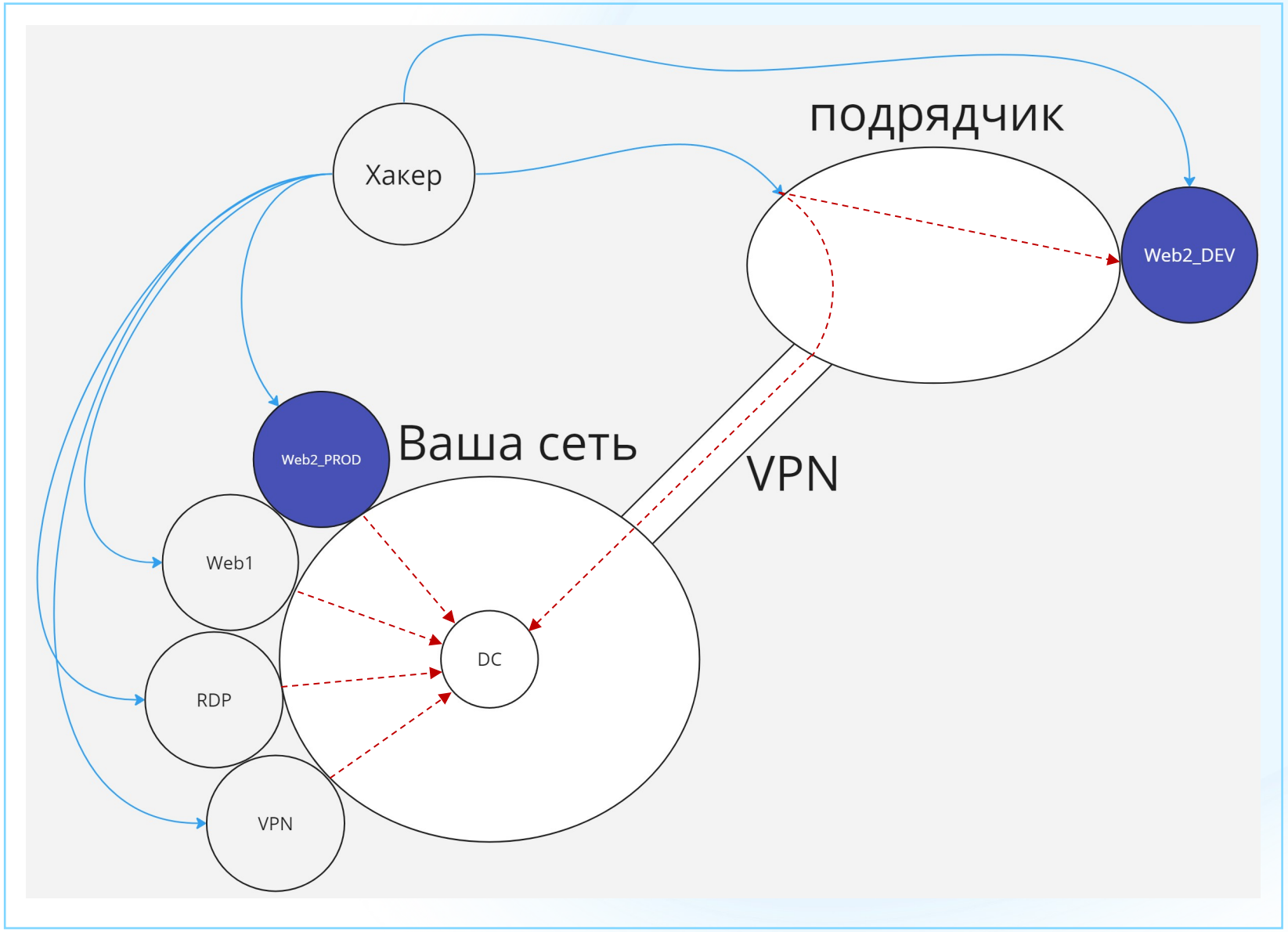


- Web — непропатченные веб-сервисы:
  - «1С-Битрикс: Управление сайтом»
  - OWA
  - Citrix
- RDP:
  - Трансляции рабочих мест
  - Трансляции RDP без VPN
- VPN:
  - Отсутствие второго фактора
  - Отсутствие журналирования
- Уязвимые ОС: Windows 2003



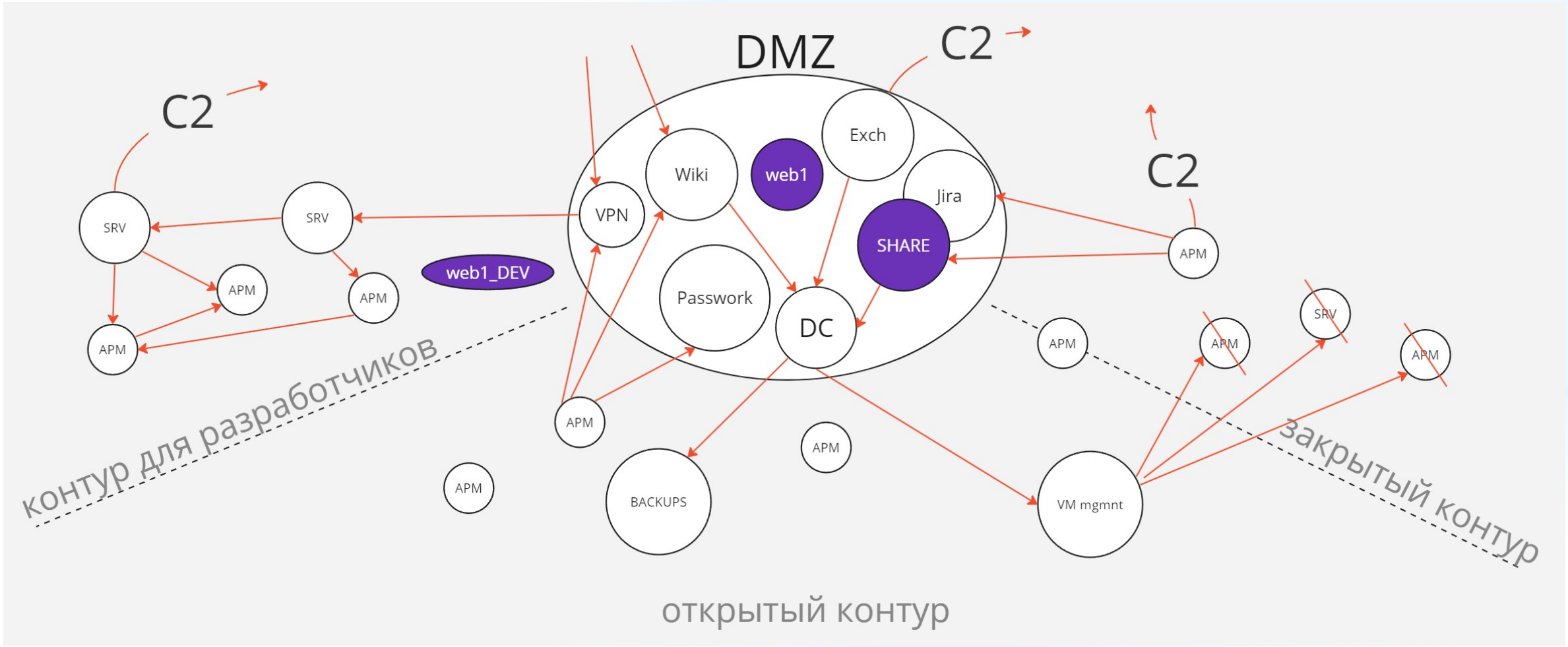
- Тестовые серверы для разработчиков
  - Отсутствует мониторинг
  - Не меняется секрет для генерации токенов
  - Не меняются пароли
  - Не удаляются учетные записи
- VPN
  - Неконтролируемая связь с полным доступом к сети
  - Общие сервисные узлы
- Фишинг

Ошибки снаружи: результаты пролома подрядчика

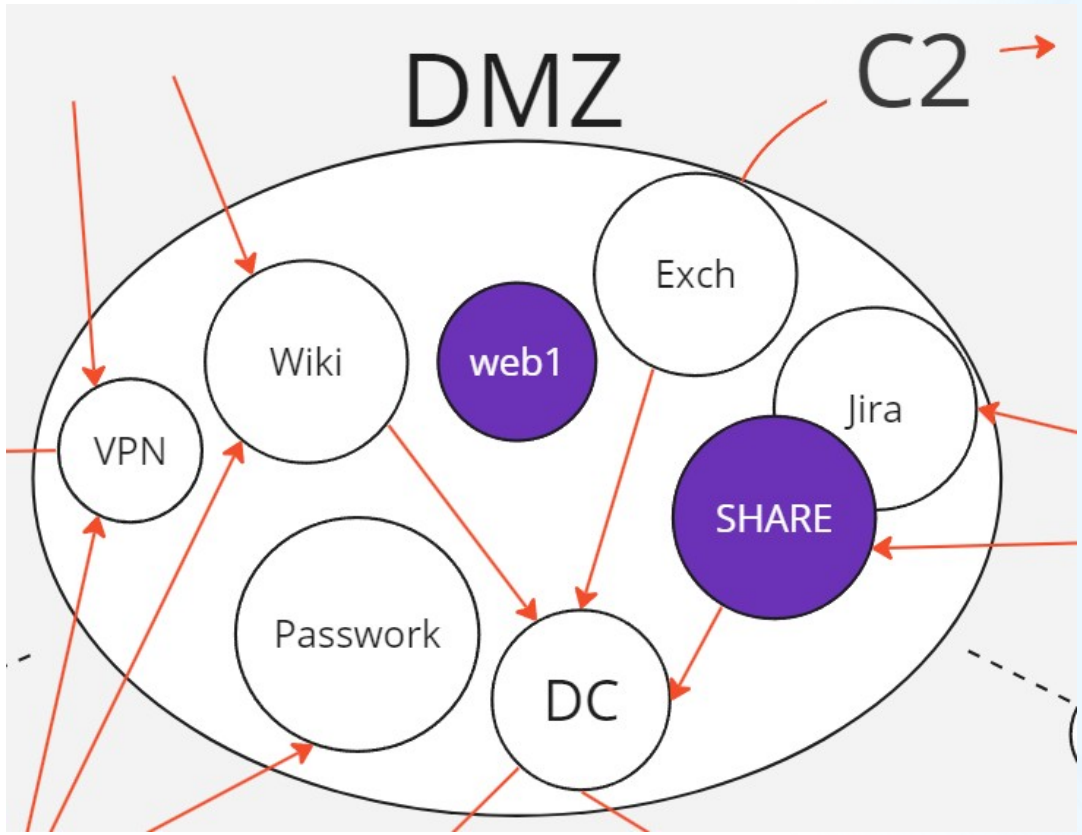


Ошибки снаружи

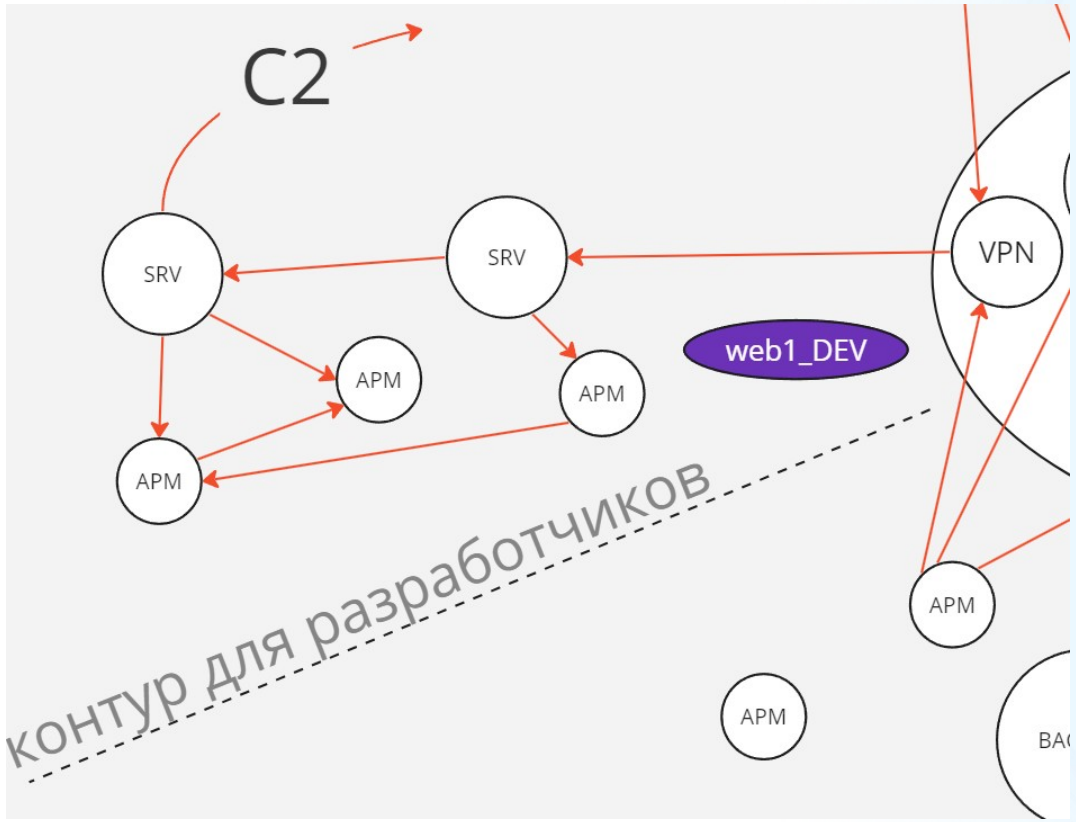
Ошибки снаружи



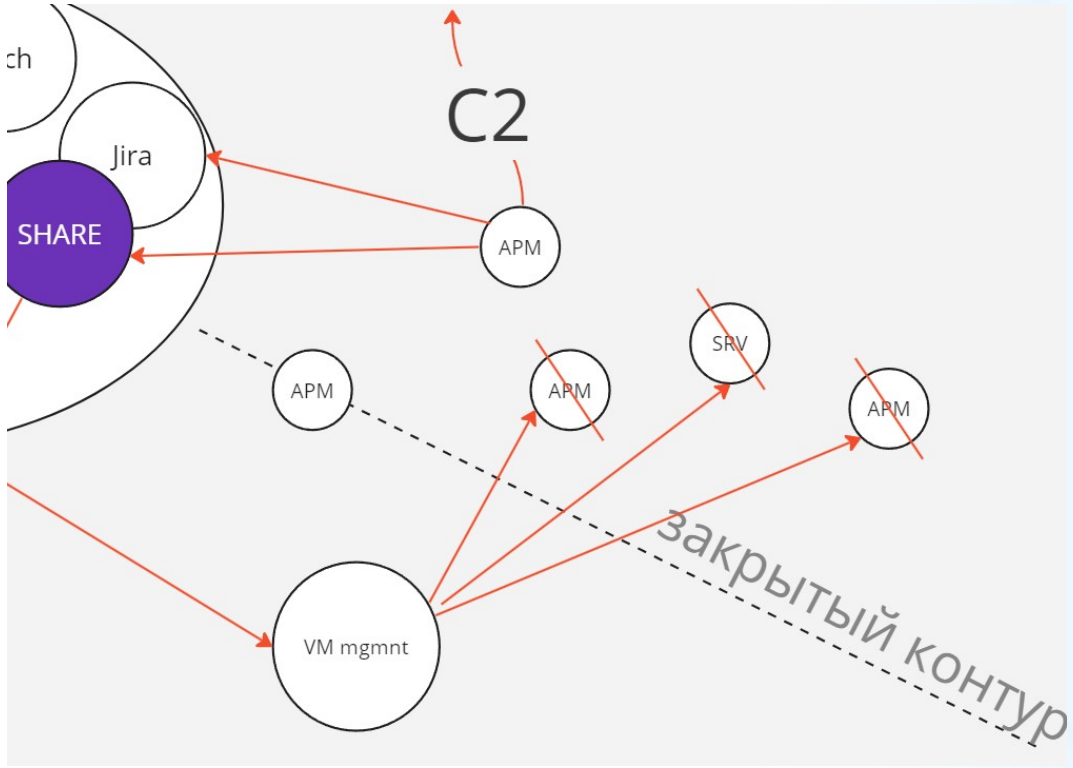
Ошибки внутри



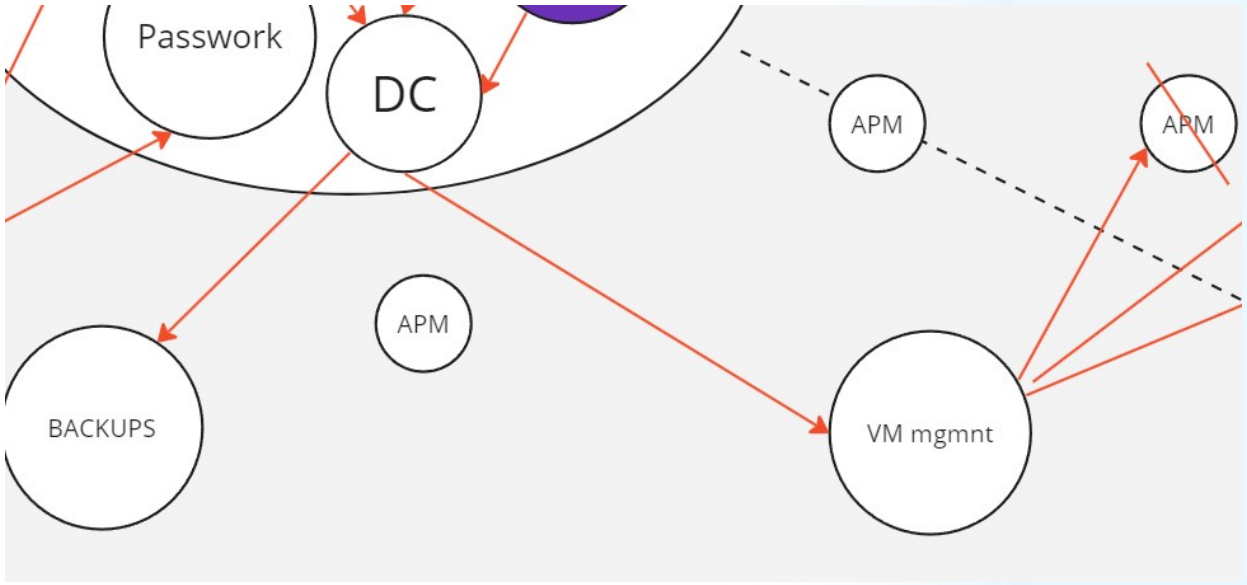
- Отсутствие контроля конфигураций (Exch)
- Хранение паролей на вики
- Хранение полной информации обо всех бизнес-процессах на вики
- Передача учетных записей в открытом виде через почту
- Использование общих ресурсов для разных контуров
- Отсутствие сегментации



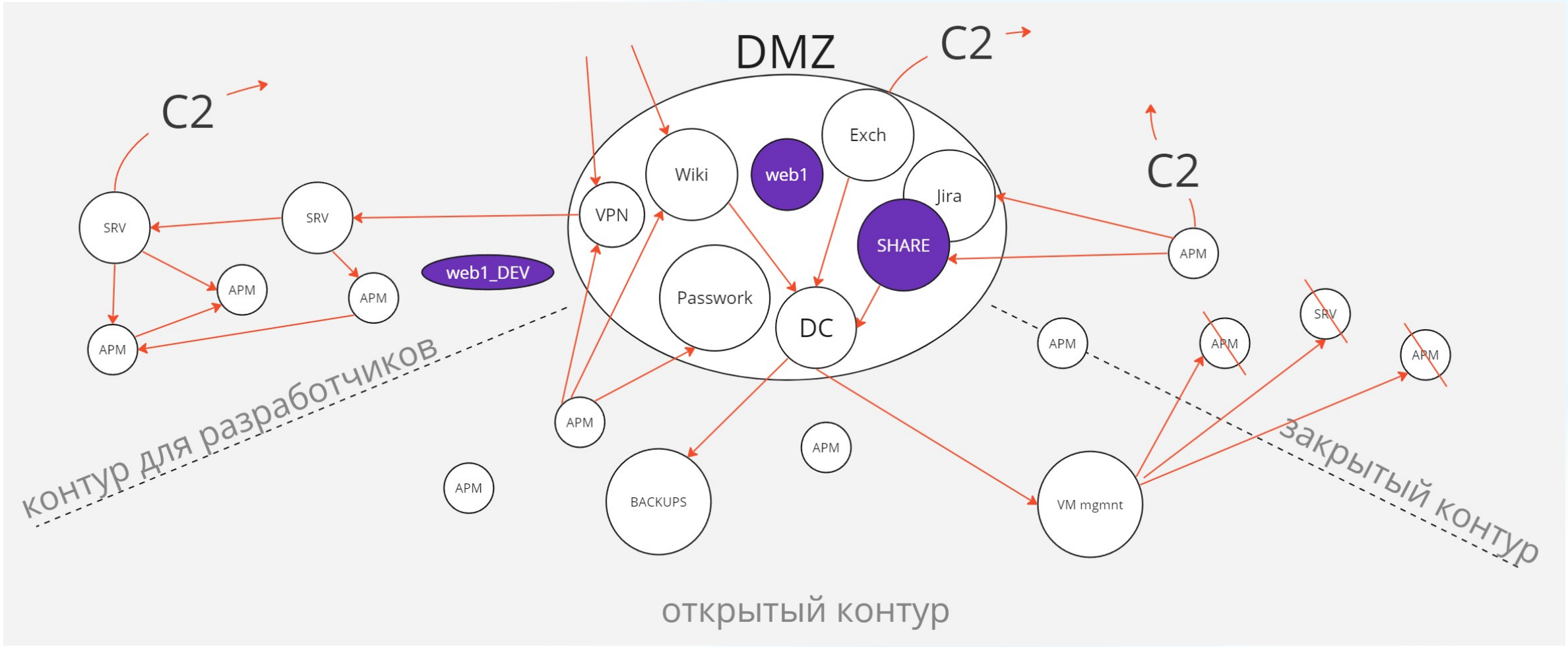
- Отсутствие сегментации
- Полный доступ на узлах
- Полный доступ к соседним подрядчикам из сети-песочницы
- Тестовые ресурсы
- Неконтролируемый доступ в интернет
- Отсутствие журналирования VPN
- Администрирование при помощи RAT
- Применение утилит двойного назначения



- Наличие более чем двух сетевых карт на АРМ
- Использование общих ресурсов с открытым контуром
- Отсутствие сегментации
- Полный доступ на узлах
- Полный доступ к соседним подрядчикам из сети-песочницы
- Тестовые ресурсы
- Неконтролируемый доступ в интернет
- Отсутствие журналирования VPN



- Отсутствие контура управления (VM)
- Хранение бэкапов в одной сети с бэкапируемыми узлами
- Управление закрытой инфраструктурой из менее защищенных контуров
- Отсутствие контроля трафика



Ошибки внутри

Ошибки на узле и общее

Аутентификация и учетные записи

SOC FORUM 2023

1	123456
2	12345
3	123456789
4	Password
5	Iloveyou
6	princess
7	1234567
8	12345678
9	Abc123
10	Nicole
11	Daniel
12	babygirl

- Отсутствие двухфакторной аутентификации
- Слабая парольная политика
- Отсутствие разделения на привилегированные и администраторские учетные записи

Конфигурации и управление ПО

SOC FORUM 2023

- Недостаточное понимание ПО, установленного на компьютерах
- Отсутствие контроля целостности конфигураций
- Попытки переустановить зараженные узлы без понимания хакерских атак
- Отсутствие патчей

Инфраструктура и сетевая безопасность

SOC FORUM 2023

- Присоединение непроверенной инфраструктуры
- Неудаление тестовой инфраструктуры и копий сервисов
- Переустановка скомпрометированных серверов без расследования
- Отсутствие сетевой сегментации
- Незащищенная публикация сервисов и узлов в интернете
- Отсутствие контроля за трафиком

Хранение учетных данных и конфиденциальность

SOC FORUM 2023

- Хранение паролей на облачных дисках
- Отсутствие ПИН-кодов в мессенджерах
- Хранение паролей на вики
- Хранение паролей в текстовых файлах, на «шарах»

Учетные записи и администрирование

SOC FORUM 2023

- Передача данных по почте без шифрования
- Использование доменного администратора и системных учетных записей
- Пользователи с правами администраторов как исключение
- Администрирование инфраструктуры вредоносным программным обеспечением

Бэкапы и восстановление

SOC FORUM 2023

Бэкапы есть. Но их тоже зашифровали

Люди

SOC FORUM 2023

- Самоуверенность администраторов
- «Не пошифровали же»
- Забывание об инциденте после расследования

Дружба

SOC
FORUM
2023

Подразделения IT
и ИБ — в контрах

SOC FORUM 2023

+7 495 744 01 44
(московский офис)
pt@ptsecurity.com

107061, Москва,
Преображенская пл., д. 8