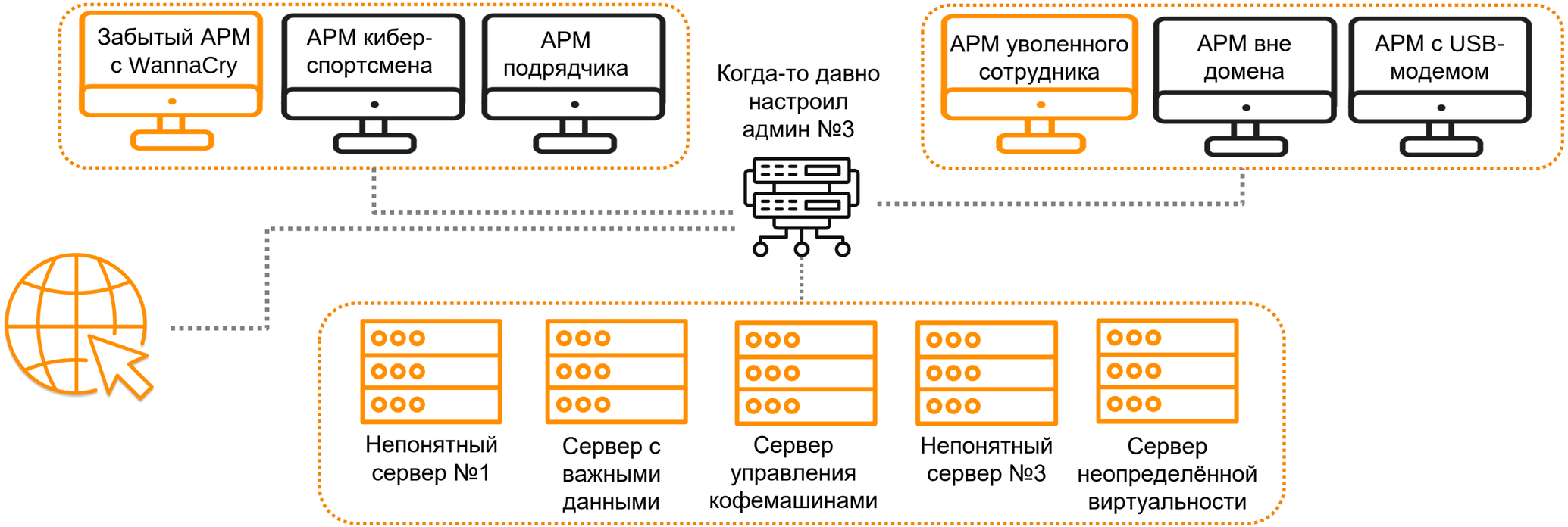
Расследование инцидента до инцидента

Денис Строченко,
руководитель направления мониторинга,
«Перспективный мониторинг»

Теперь о наболевшем



Неуязвимых структур не бывает

NVIDIA

Кража исходного кода продуктов и сертификатов

IObit

Заражение клиентов вредоносным ПО

NORDEX

Отключение удалённого доступа к управляемым ветряным турбинам

ION MARKETS

Перебои в работе клиентского сервиса

THALES

Кража данных клиентов

KSC
شرکت فولاد خوزستان

Остановка производства, пожар в цехе

MARQUARD & BAHLS

Перебои со снабжением топливом заправочных станций

WWU MÜNSTER

Приостановка деятельности образовательного учреждения

okta

Компрометация клиентов

TU/e Technische Universiteit Eindhoven University of Technology
Where innovation starts

Кража и публикация конфиденциальных данных

CDSL

Приостановка клиринговых и расчётных услуг

Universität Zürich[UZH]

Отключение веб-ресурса образовательного учреждения

Millennium bcp

Приостановка обслуживания клиентов

medibank

Кража денежных клиентов

Несанкционированное изменение температурного режима хранения продукции

महेश बैंक
ESTD. 1978

Кража денежных средств из банкоматов

Утечки данных

Время публикации данных	Жертва утечки	Направление деятельности
09.09.2023 13:41		Провайдер цифровых услуг и сервисов
07.09.2023 17:41		Коммерческий банк
19.08.2023 19:13		Страховая компания
18.08.2023 0:58		Хостинг
12.08.2023 12:55		Образовательное учреждение высшего образования
07.08.2023 12:32		Государственное учреждение Москвы
05.08.2023 17:21		Вендор ПО
05.08.2023 1:33		Сервис электронных и аудиокниг
03.08.2023 14:45		Частное медицинское учреждение
02.08.2023 10:25		Магазин косметики и парфюмерии
29.07.2023 10:25		Медицинская лаборатория
28.07.2023 21:13		Туроператор
08.07.2023 20:19		Образовательное учреждение дополнительного образования
06.07.2023 17:20		Книжный интернет-магазин
05.07.2023 16:51		Международный детский центр
04.07.2023 23:35		Ремонт электроники и бытовой техники
03.07.2023 19:46		Интернет-магазин велосипедов
27.06.2023 20:25		Теннисный клуб
27.06.2023 20:15		Медицинский центр
26.06.2023 17:43		Магазин медицинского оборудования
14.06.2023 3:36		Магазин спортивного питания
11.06.2023 17:05		Коммерческий банк
10.06.2023 15:02		Некоммерческая организация
10.06.2023 4:41		Книжный магазин
09.06.2023 14:09		Платформа оптимизации финансовых операций клиентов банк
09.06.2023 13:50		Производитель одежды
08.06.2023 9:57		Книжный магазин
08.06.2023 16:25		Универсальный оператор связи
08.06.2023 19:40		Интернет-аптека
08.06.2023 9:55		Магазин одежды
08.06.2023 9:53		Магазин стройматериалов
08.06.2023 9:00		Книжный магазин
08.06.2023 9:00		Магазин товаров для дома
06.06.2023 11:31		Оператор розничной сети
06.06.2023 10:32		Гипермаркет товаров для дома
02.06.2023 13:08		Государственная образовательная платформа

Разбираем процесс

Состояние системы до инцидента → ! → Развитие ещё не обнаруженного инцидента → Обнаружение и реагирование → Привлечение команды расследования → Расследование (магия) → Ликвидация последствий

Активные действия злоумышленника

Следы деятельности злоумышленника, которые можно обнаружить

Команда ИБ в штатном режиме

Команда ИБ может что-то подозревать

Команда ИБ в режиме «мистер Вульф»

Команда ИБ делает выводы

О чём вас спросят?

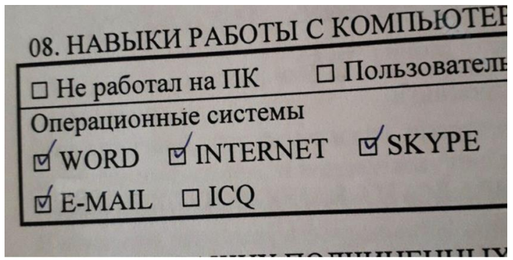
Приглашённая команда ИБ в режиме «мистер Вульф»

Уяснение поставленной задачи

Оценка обстановки

1. Инфраструктура

2. Люди



3. Процессы

4. Ресурсы

Zero Trust

1 Необходимо знать каждое устройство в своей сети

- Идентификационные данные (IP-адрес, MAC-адрес, VLAN, порты подключения и т.д.)
- Какие данные циркулируют и насколько они ценные
- Функциональное назначение
- Кто работает с этим узлом, кто его администрирует
- Состав ПО, версии, конфигурации

2 Необходимо знать каждого пользователя системы

- Стандартизированная персонификация учётных записей
- Явное разделение учётных записей по ролям
- Стойкая парольная политика
- Использование сервисных учётных записей для сервисов
- Ревизия пользователей

3 Необходимо знать все значимые для организации данные

- Циркулирующие данные явно распределены по критичности
- Определено, какие пользователи работают с важными данными
- Определено, на каких узлах циркулируют важные данные
- Определены политики резервного копирования важных данных
- Определено, какие данные находятся в общем доступе

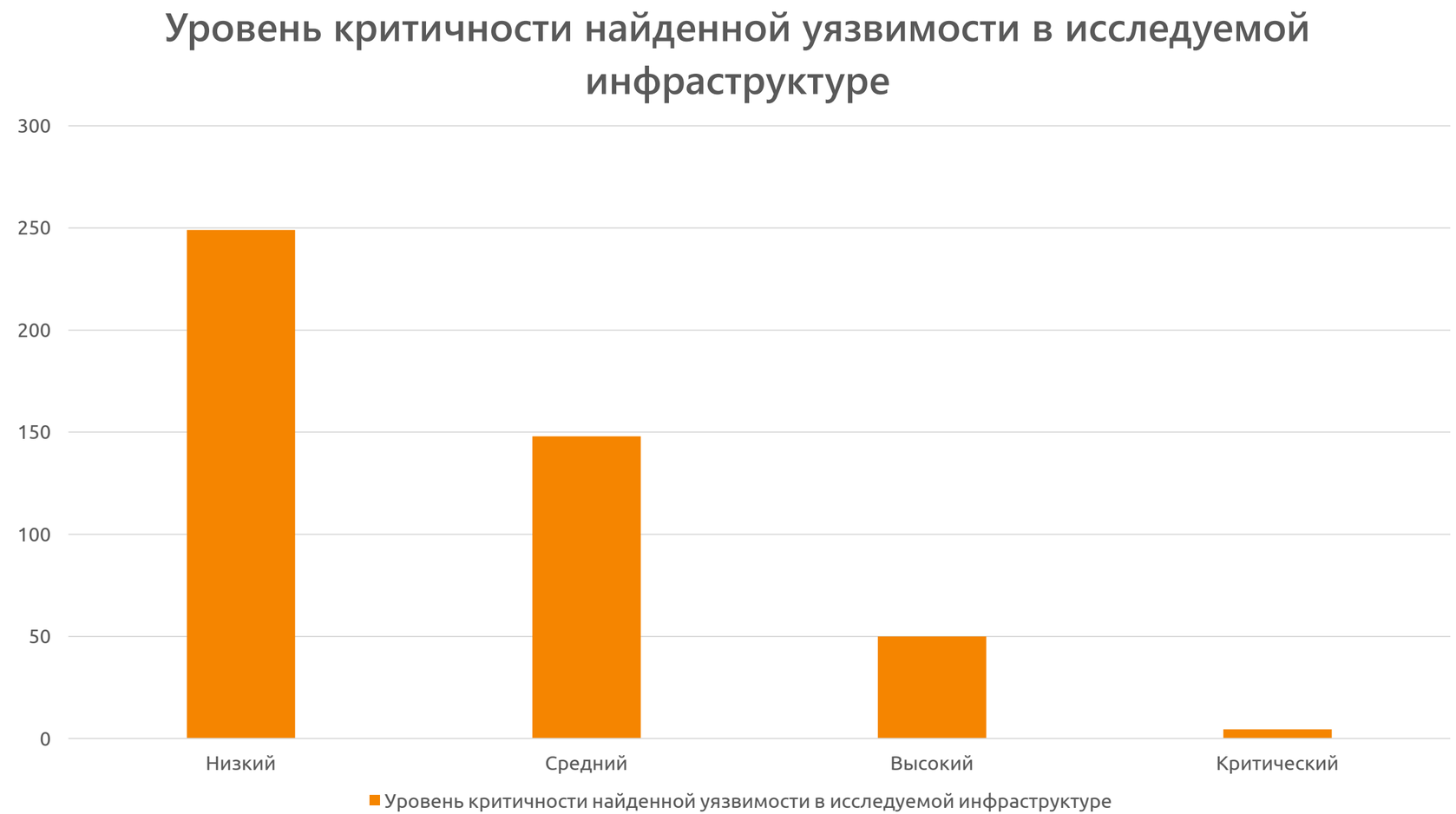
Немного о политиках аудита

Простое бинго

Как оценить (не)готовность организации к проведению расследования инцидента ИБ

Есть отчёты о ранее проведённых пентестах или bug bounty Пентесты или bug bounty не проводились	**Применяются оптимальные политики аудита** Политика аудита next->next->ok	**Имеется контроль за актуальностью версий применяемых ОС и ПО** Подобный контроль отсутствует	**Применяются только персонифицированные учётные записи** Сотрудники используют общие учётные данные
СЗИ применяются, они актуальны и с актуальными обновлениями СЗИ не применяются или неактуальны	**Имеется система централизованного сбора событий ИБ** Централизованный сбор событий ИБ отсутствует	**Имеется схема циркуляции чувствительных данных** Не знаем, как, кем и где именно обрабатываются чувствительные данные	**СЗИ покрывают не менее 99,9% инфраструктуры** Область покрытия инфраструктуры СЗИ недостаточна
Существует полная и актуальная схема сети и инвентаризация Данные отсутствуют или не отражают текущую действительность	**Проводится обучение персонала по вопросам ИБ** Работа с персоналом не проводится	**Имеется стойкая парольная политика** Парольная политика нестойкая или фактически не применяется	**СЗИ управляются квалифицированным персоналом** СЗИ управляются людьми, далёкими от сферы ИБ

А что по пентестам?



Выжимка по докладу

Что поможет в расследовании инцидента ИБ и что можно обеспечить заранее

1. Результаты пентестов и программ bug bounty
2. Применение СЗИ и поддержание их в актуальном состоянии (версии, экспертные данные, конфигурации, область покрытия)
3. Применение элементов концепции Zero Trust
4. Инвентаризация активов (устройства, узлы, пользователи, системы, данные)
5. Определение критичных областей инфраструктуры
6. Контроль актуальности версий применяемых ОС и ПО
7. Централизованное управление журналами
8. Оптимальная политика аудита

Дополнительные
источники информации

- Definitive Guide to Cyber Threat Intelligence
- Positive Research / 2023
- Gartner, McMillan (2013) from Tactics, Techniques and Procedures (TTPs) to Augment Cyber Threat Intelligence (CTI): A Comprehensive Study

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

Денис Строченко

Руководитель направления мониторинга

+7 (495) 737-61-97

Denis.Strochenko@amonitoring.ru

t.me/pm_public

amonitoring.ru