Влияние анализа защищенности на расследование инцидентов

КОД ИБ: ИТОГИ 2025

BELYAEV

Директор по КБ: Беляев Дмитрий Александрович

ОБО МНЕ

Беляев Дмитрий Александрович

•Более 10 лет в ИБ;

• Имею 2 образования (ИБ и Юриспруденция);

•Имею более 130 сертификатов/дипломов и благодарностей по тематике ИБ;

•Победитель в рейтинге ТОП-100 Лидеров ИТ;

•В прошлом руководил 5-ю стартапами (в т.ч и по ИБ) и командой из более 100 человек;

• Имею за плечами более 60 выступлений на публику суммарной численностью >5000 человек (TADVISER, ТБ Форум, Территория Безопасности, CISO Форум, CNews, ITsec, Security Summit и т.д).

ПОЧЕМУ АНАЛИЗ ЗАЩИЩЕННОСТИ ВАЖЕН

- **Идентификация уязвимостей:** Сканирование и аудит кода выявляют слабые места, которые используют злоумышленники.

- **Построение корреляций в SIEM-системах:** Они позволяют связывать действия злоумышленников на разных этапах, что упрощает расследование и подтверждение фактов атак.

- **Оптимизация затрат:** Предупреждение инцидентов через анализ защищенности обходится дешевле, чем ликвидация их последствий.

СТАТИСТИКА 2024 ГОДА

Cnews:
96% компаний в России можно взломать с помощью старых уязвимостей, которые уже описаны в Сети

Solar:
43% продвинутых кибератак на российский бизнес связаны с уязвимостями в корпоративных веб-приложениях

Securitylab:

Активность при эксплуатации уязвимостей веб-приложений 43% инцидентов в 2024 году

Проблемы

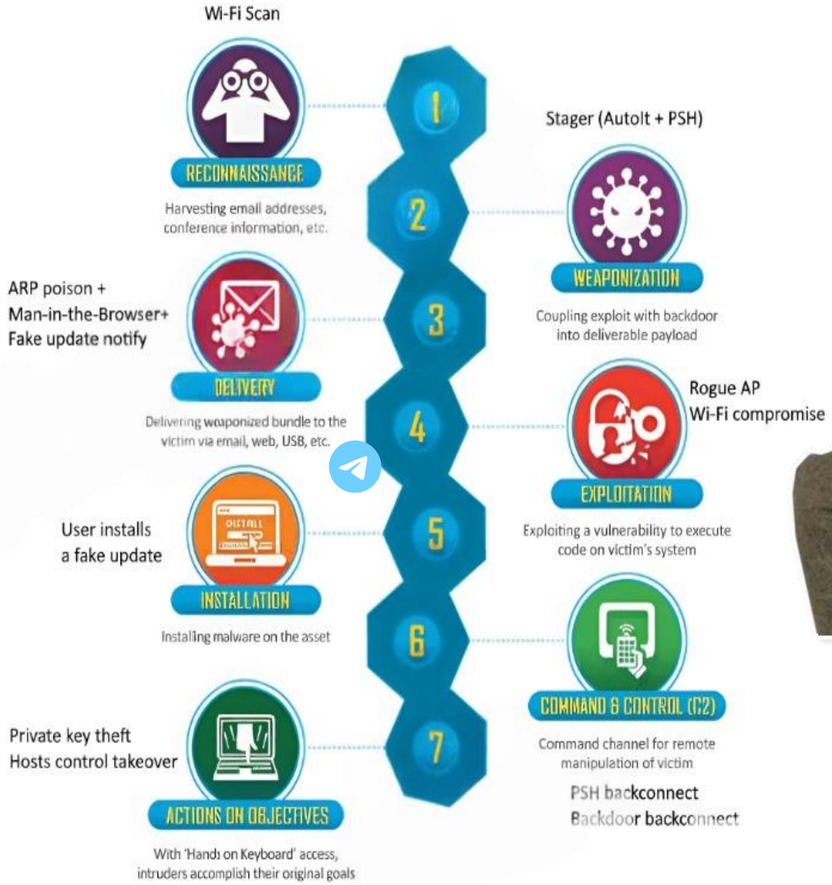
- Дефицит кадров;
- Отсутствие ШЕ;
- Отсутствие бюджета;
- Не высокая квалификация;
- Отсутствие регулярных киберучений;
- Отсутствие стратегии;
- Слабый регуляторный контроль.

Решение

Почему анализ защищенности важен и как это влияет на расследования?

Cyber Kill Chain

1. Сбор информации о цели
2. Вооружение
3. Доставка ВПО
4. Эксплуатация уязвимостей
5. Установка ВПО
6. Установка канала связи с C2
7. Достижение целей атаки

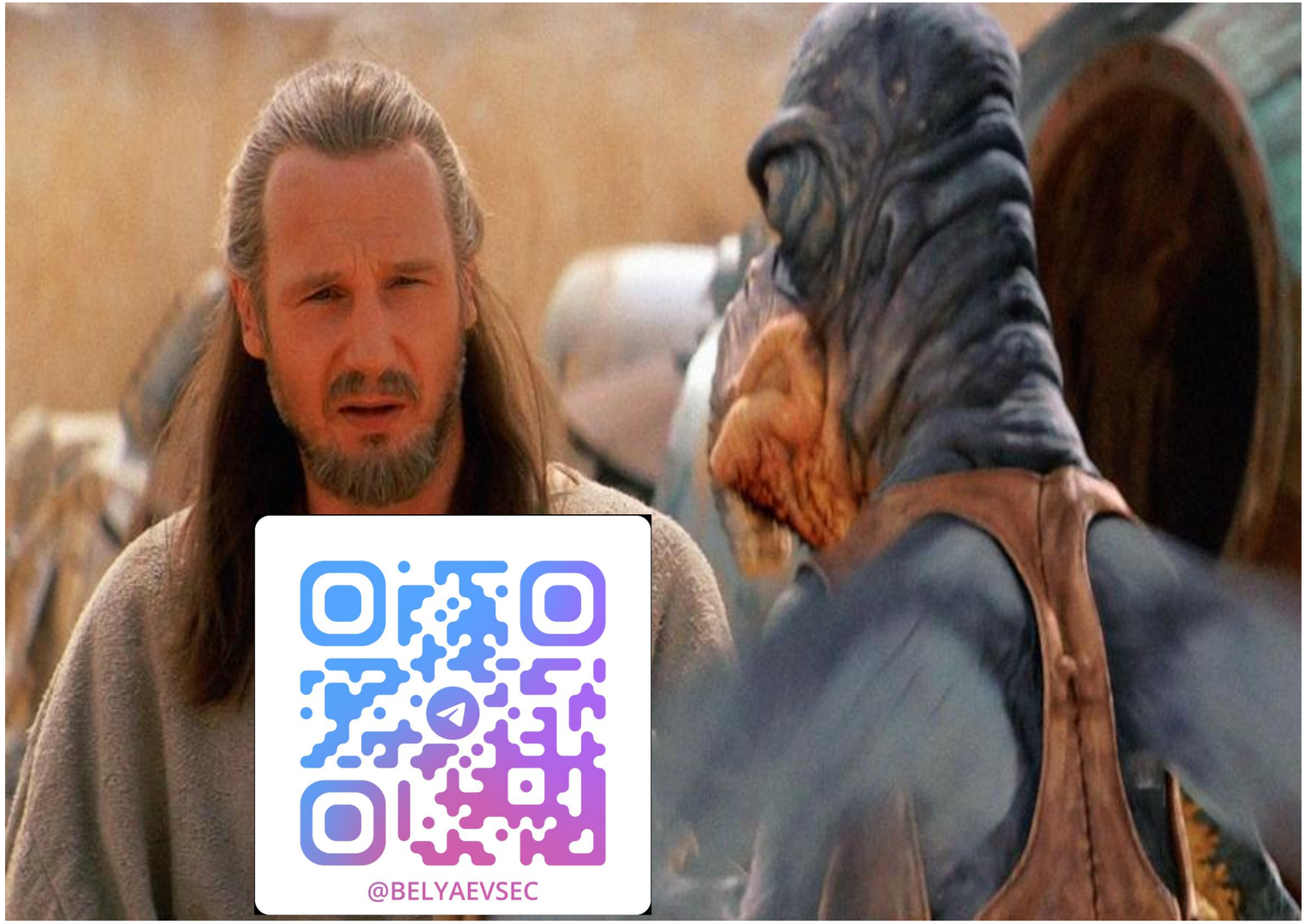


РОСТ СПРОСА НА ПРОЕКТЫ ПО РАССЛЕДОВАНИЮ ИНЦИДЕНТОВ

- 2023 - 176%;
- Первые три квартала 2024 года +24%.*

* https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/

Подпишитесь на канал



Спасибо за внимание!

Вопросы?