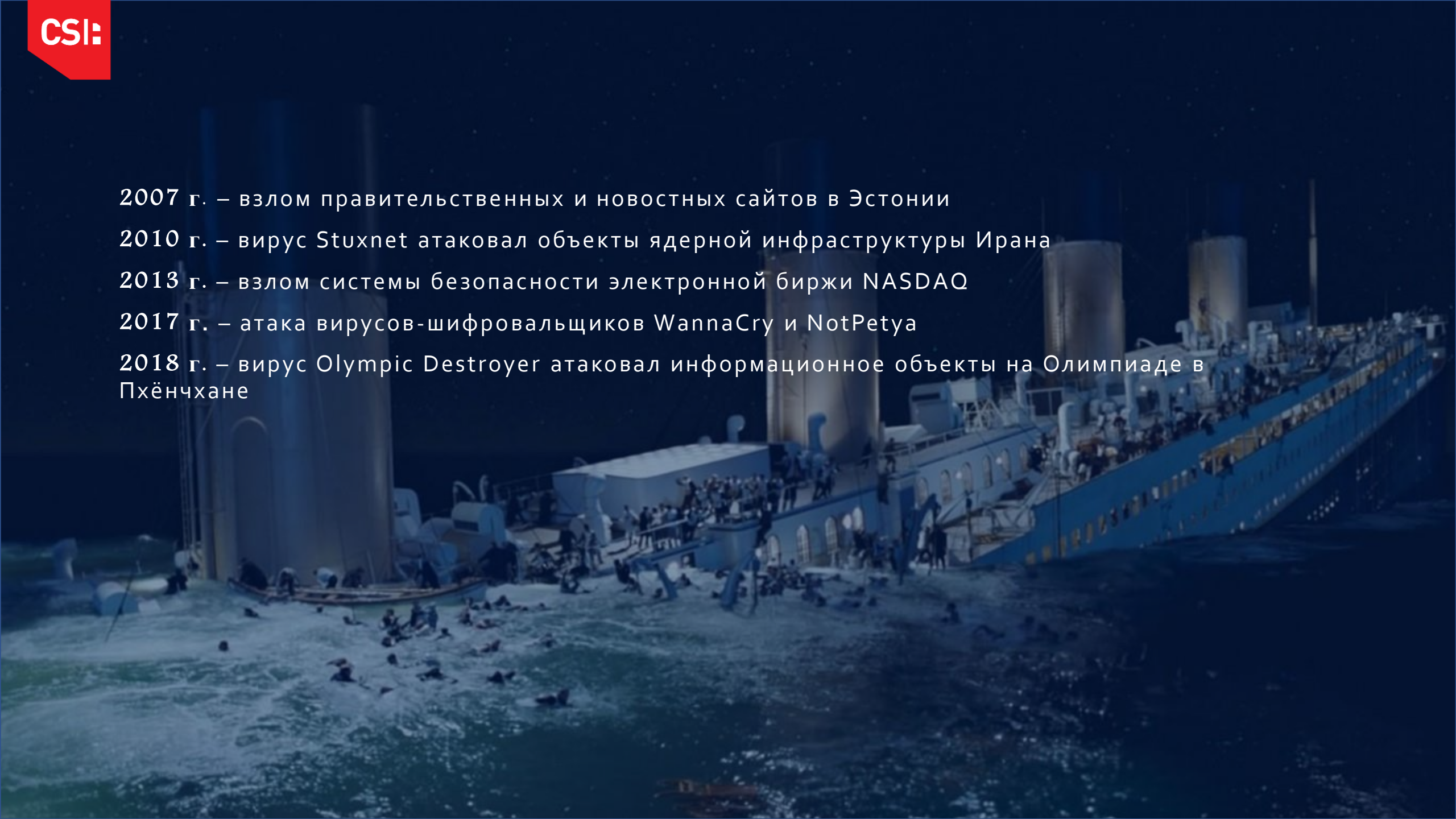
CyberSec Checkup:

Оценка состояния информационной безопасности в компаниях для повышения уровня защищенности

Олег Безик
Специалист по компьютерной криминалистике и ИБ
CSI Group



2007 г. – взлом правительственных и новостных сайтов в Эстонии

2010 г. – вирус Stuxnet атаковал объекты ядерной инфраструктуры Ирана

2013 г. – взлом системы безопасности электронной биржи NASDAQ

2017 г. – атака вирусов-шифровальщиков WannaCry и NotPetya

2018 г. – вирус Olympic Destroyer атаковал информационное объекты на Олимпиаде в Пхёнчхане

Атака вируса-шифровальщика «WANNACRY»

По данным Лаборатории Касперского

МАСШТАБ

- Около 150 стран
- Более 200 000 зараженных устройств
- Пострадавшие организации представляли различные индустрии и структуры, среди них Renault, Nissan, Honda, МВД России

Атака вируса-шифровальщика «WANNACRY»

ФАКТЫ ОБ АТАКЕ ВИРУСА

- Вирус использовал эксплоит «EternalBlue»
- «EternalBlue» использовал известную **на тот момент** уязвимость в ОС Windows: CVE-2017-0147
- **За два месяца** до атаки в бюллетене «MS17-010» корпорация Microsoft выпустила патч, закрывающий уязвимость

Почему такие атаки становятся возможными?

1. Незакрытые общеизвестные уязвимости
2. Небезопасные конфигурации оборудования
3. Отсутствие внутренних процессов обеспечения безопасности
4. Человеческий фактор

CyberSec Checkup

НЕЗАВИСИМЫЙ ВЗГЛЯД НА ОБЕСПЕЧЕНИЕ КИБЕР-БЕЗОПАСНОСТИ ВНУТРИ КОМПАНИИ

Что мы делаем

- Оценка процессов обеспечения безопасности и уровня их зрелости
- Выявление уязвимостей в программном обеспечении внутри сети и на ее периметре
- Анализ конфигураций сетевого оборудования
- Анализ конфигураций средств защиты
- Детальное исследование отдельных аспектов обеспечения безопасности
- Разработка детальных рекомендаций по повышению уровня защищенности компании и устранению выявленных уязвимостей

CyberSec Checkup

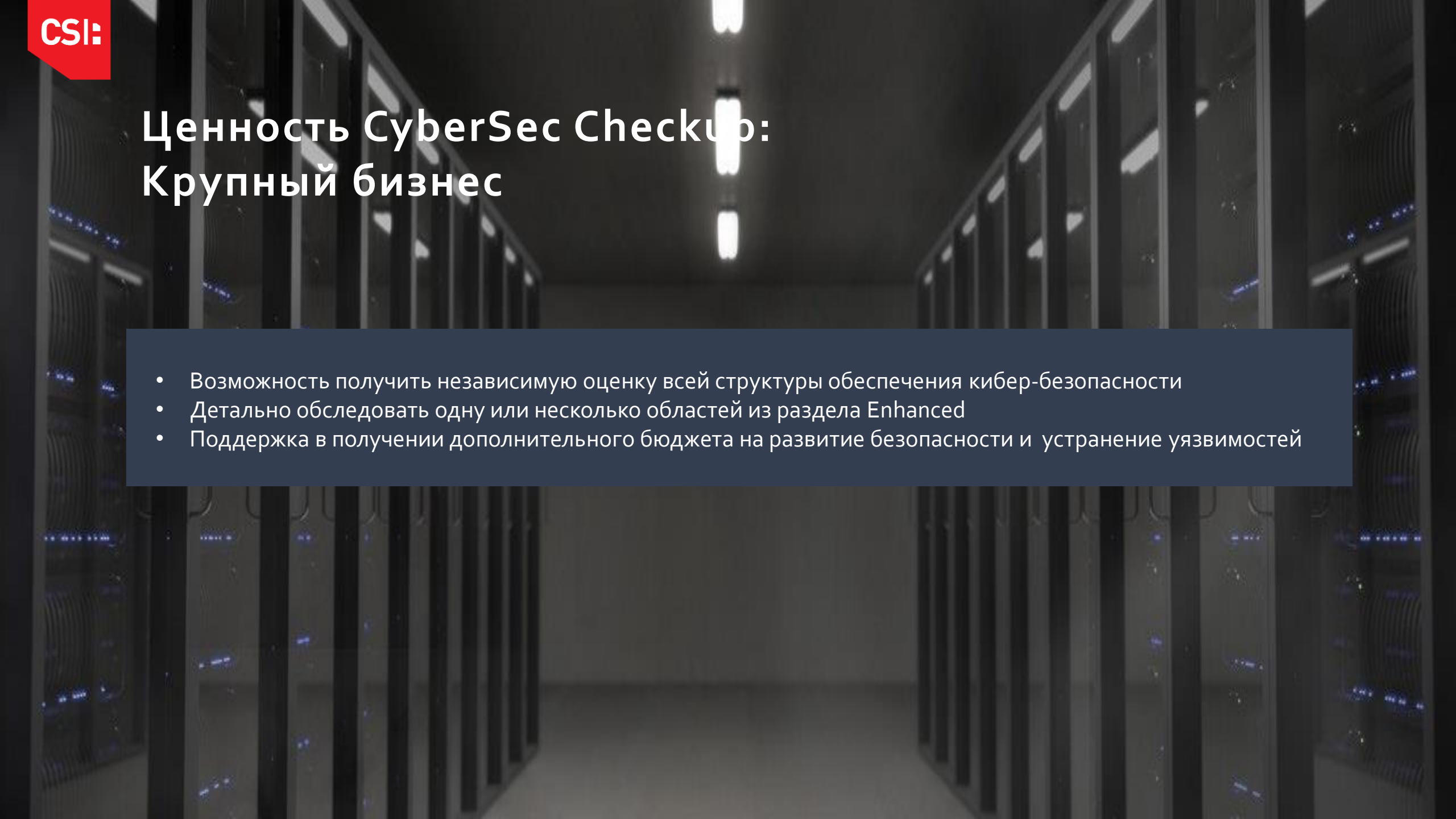
Basic

- CSC 20, ISO 27001 и т.д.
- Сканирование сетевых узлов с целью поиска уязвимостей
- Сканирование периметра
- Анализ настроек средств обеспечения безопасности
- Разработка рекомендаций

Enhanced

BASIC + одна или несколько опций

- Лицензионная сверка
- Аудит беспроводных сетей
- Аудит безопасности баз данных
- Анализ конфигурации сетевых устройств
- Анализ документации по безопасности
- Аудит безопасности облачных сервисов
- Аудит безопасности web-приложений
- Аудит безопасности мобильных приложений
- и другие области по запросу клиента



Ценность CyberSec Checkup: Крупный бизнес

- Возможность получить независимую оценку всей структуры обеспечения кибер-безопасности
- Детально обследовать одну или несколько областей из раздела Enhanced
- Поддержка в получении дополнительного бюджета на развитие безопасности и устранение уязвимостей

Ценность CyberSec Checkup: SMB

- Возможно первый аудит безопасности в истории компании, выполненный специалистами
- Существенное изменение состояния ИБ в короткий промежуток времени
- Минимизация затрат на оценку уровня защищенности
- Систематизация процессов обеспечения безопасности

Пример из практики

КЛИЕНТ

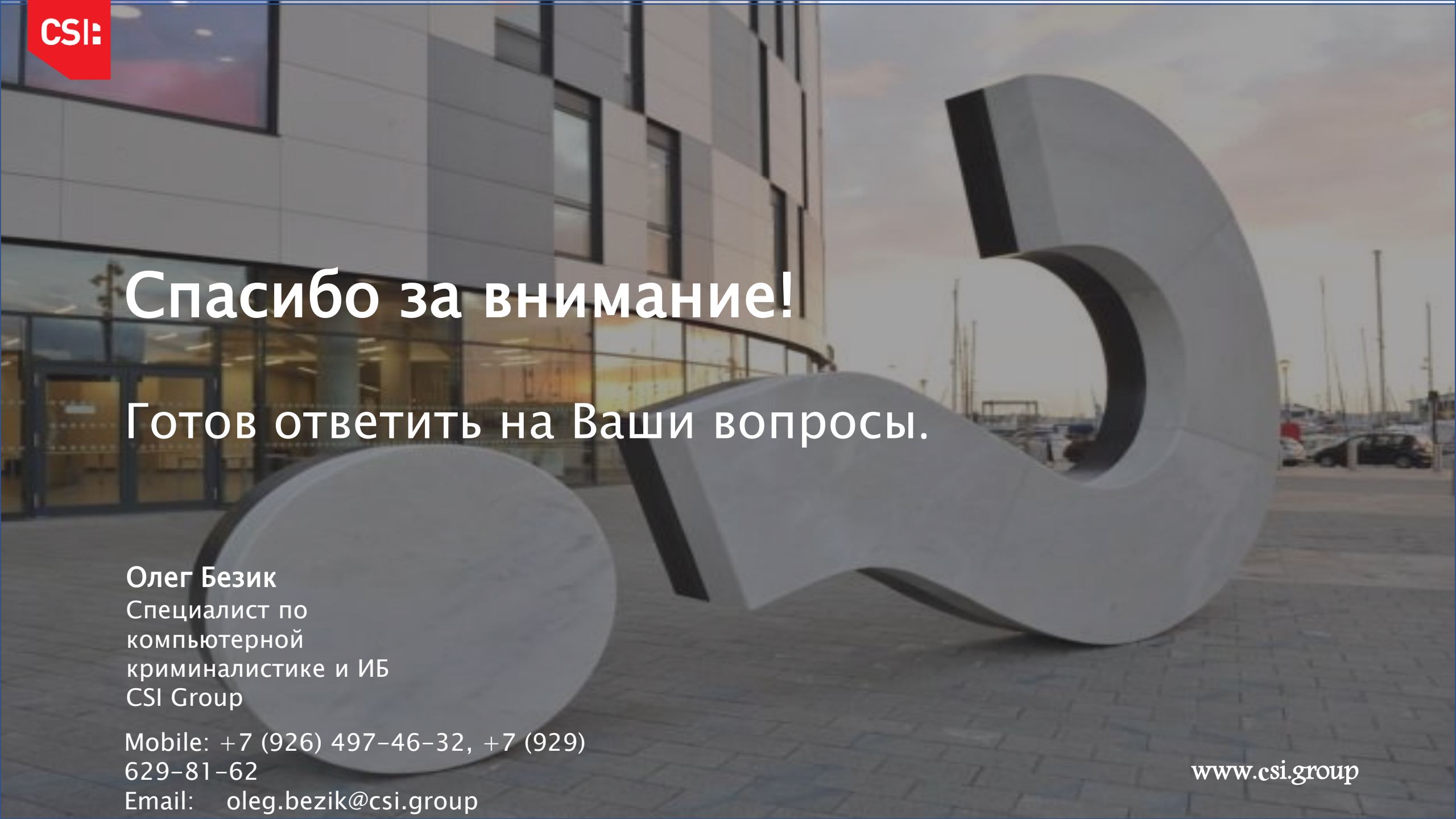
- Крупный российский ритейлер
- Представительство практически в каждом регионе страны
- Более 2000 устройств

ЧТО МЫ СДЕЛАЛИ?

- ✓ Опросили сотрудников IT
- ✓ Просканировали более 200 устройств в двух локациях
- ✓ Изучили конфигурации более 20 сетевых устройств
- ✓ Изучили более 10 доменных политик

ЧЕМ МЫ ПОМОГЛИ?

- Обнаружить серьезные уязвимости в системном и прикладном ПО
- Обнаружить несоответствие требованиям безопасности доменных политик
- Обнаружить «торчащие» наружу GUI-интерфейсы для управления виртуальными серверами
- Обнаружить вирус-майнер, блуждающий по корпоративной сети



Спасибо за внимание!

Готов ответить на Ваши вопросы.

Олег Безик
Специалист по
компьютерной
криминалистике и ИБ
CSI Group

Mobile: +7 (926) 497-46-32, +7 (929)
629-81-62
Email: oleg.bezik@csi.group

www.csi.group