USSC SOC

Доктор УЦСБ SOC –
ваш личный эксперт
по киберздоровью

В РЕЖИМЕ 24/7

О КОМПАНИИ УЦСБ

> 18
лет на рынке

> 900
профессионалов в штате

> 4000
завершенных проектов

Топ-100 крупнейших отечественных ИТ-компаний[1]

Топ-15 крупнейших компаний России в сфере защиты информации[2]

Компетенции

- Информационная безопасность
- Информационные технологии
- Инженерно-технические средства охраны
- Интеллектуальные инженерные системы
- Анализ защищенности
- Центры обработки данных
- Сервисный центр

[1] Рейтинг CNews100: Крупнейшие ИТ-компании России 2024
[2] Рейтинг CNews Security: Крупнейшие компании России в сфере защиты информации 2024

ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ О ТРЕНДАХ В ИТ И ИБ

IT IS CONF

19-20.06

г. Екатеринбург

РЕГИСТРИРУЙСЯ

Треки конференции:

- ИБ не для галочки: «ответственное потребление» бюджетов
- Архитектура цифровой устойчивости
- Application Security: как безопасность приложений меняет правила игры
- Технологии построения цифрового доверия
- ИБ-экосистемы: утопия или рабочая модель
- Эфир по экосистемам

ЭВОЛЮЦИЯ СИЛЬНЫХ РЕШЕНИЙ

ПЛАН ВЕБИНАРА

USSC SOC

01 Скорая киберпомощь

02 Первые симптомы

03 Мониторинг киберздоровья

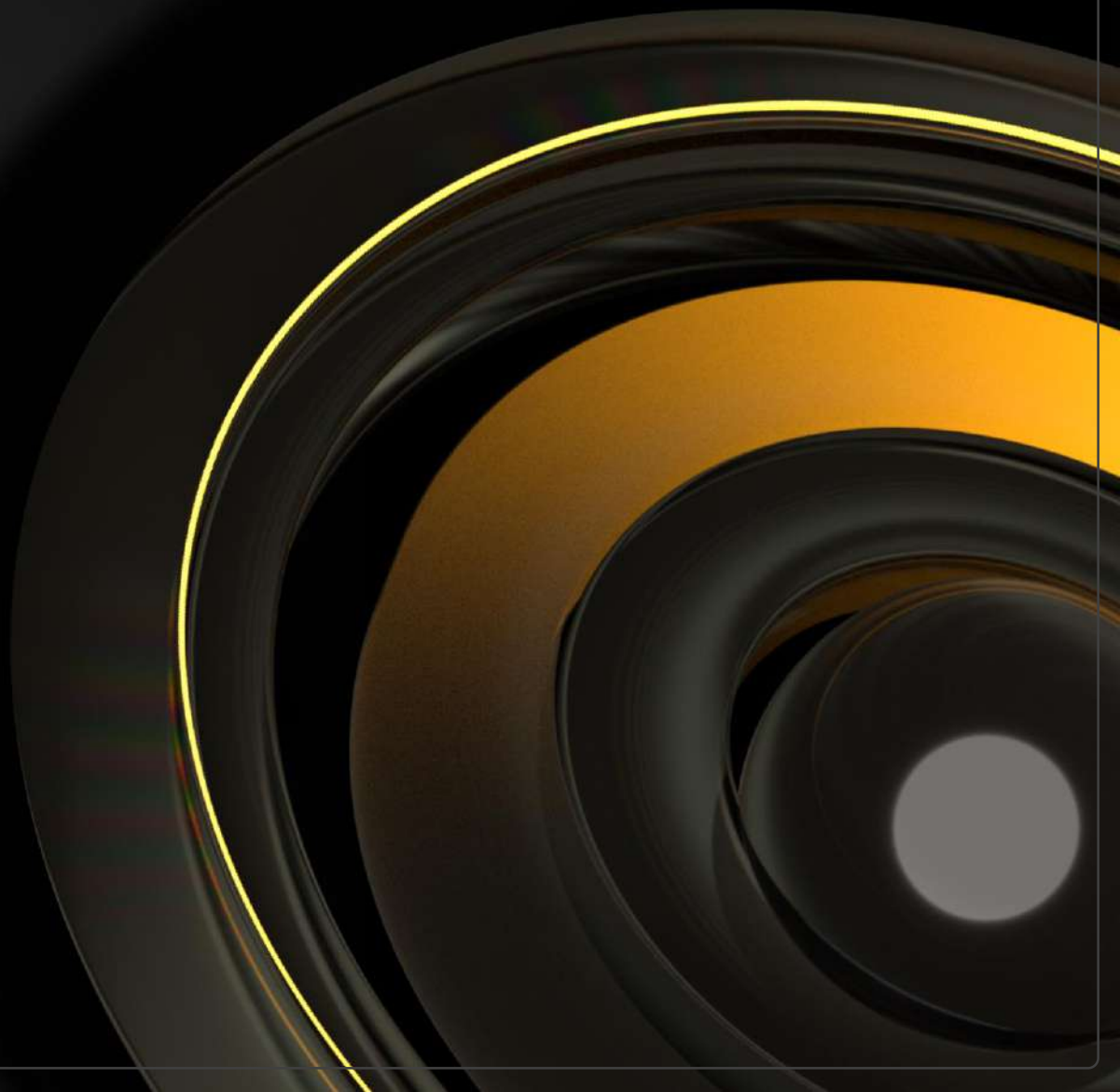
04 Ответы на вопросы участников

WHOAMI

- Директор коммерческого центра оперативного реагирование УЦСБ SOC
- Занимаюсь вопросами ИБ 15 лет
- Кандидат технических наук
- Председатель государственной экзаменационной комиссии - Кафедра безопасности информационных технологий
- Увлекаюсь охотой за компетентными аналитиками ИБ и инженерами

USSC SOC

КЕЙС №1: СКОРАЯ КИБЕРПОМОЩЬ



КЕЙС №1: СКОРАЯ КИБЕРПОМОЩЬ

Безопасность – не расходы,
а инвестиция в киберздоровье
организации

КЕЙС №1: СКОРАЯ КИБЕРПОМОЩЬ

КОГДА МОЖЕТ ПОНАДОБИТЬСЯ

- Заражение вредоносным ПО
- Инфраструктура зашифрована, просят выкуп
- Потерян контроль над инфраструктурой
- Утекла чувствительной информации
- Клиенты получили фишинговые рассылки от вашего имени
- Произошел дефейс сайта

КЕЙС №1: СКОРАЯ КИБЕРПОМОЩЬ

USSC SOC

ЧТО НУЖНО ДЕЛАТЬ ВАМ

Не восстанавливаться из бэкапов

Не торопиться с выплатами злоумышленникам

Незамедлительно обратиться к экспертам!

КЕЙС №1: СКОРАЯ КИБЕРПОМОЩЬ

USSC SOC

ПОРЯДОК ДЕЙСТВИЙ ОТ УЦСБ SOC

1. Оперативная встреча для сбора постановки задачи и выработки экстренных мер в течение **24 часов**
2. Сбор и анализ данных
3. Локализация инцидента
4. Восстановление бизнес-процессов
5. Подготовка отчета с исчерпывающим набором мер по недопущению повторного возникновения ИБ

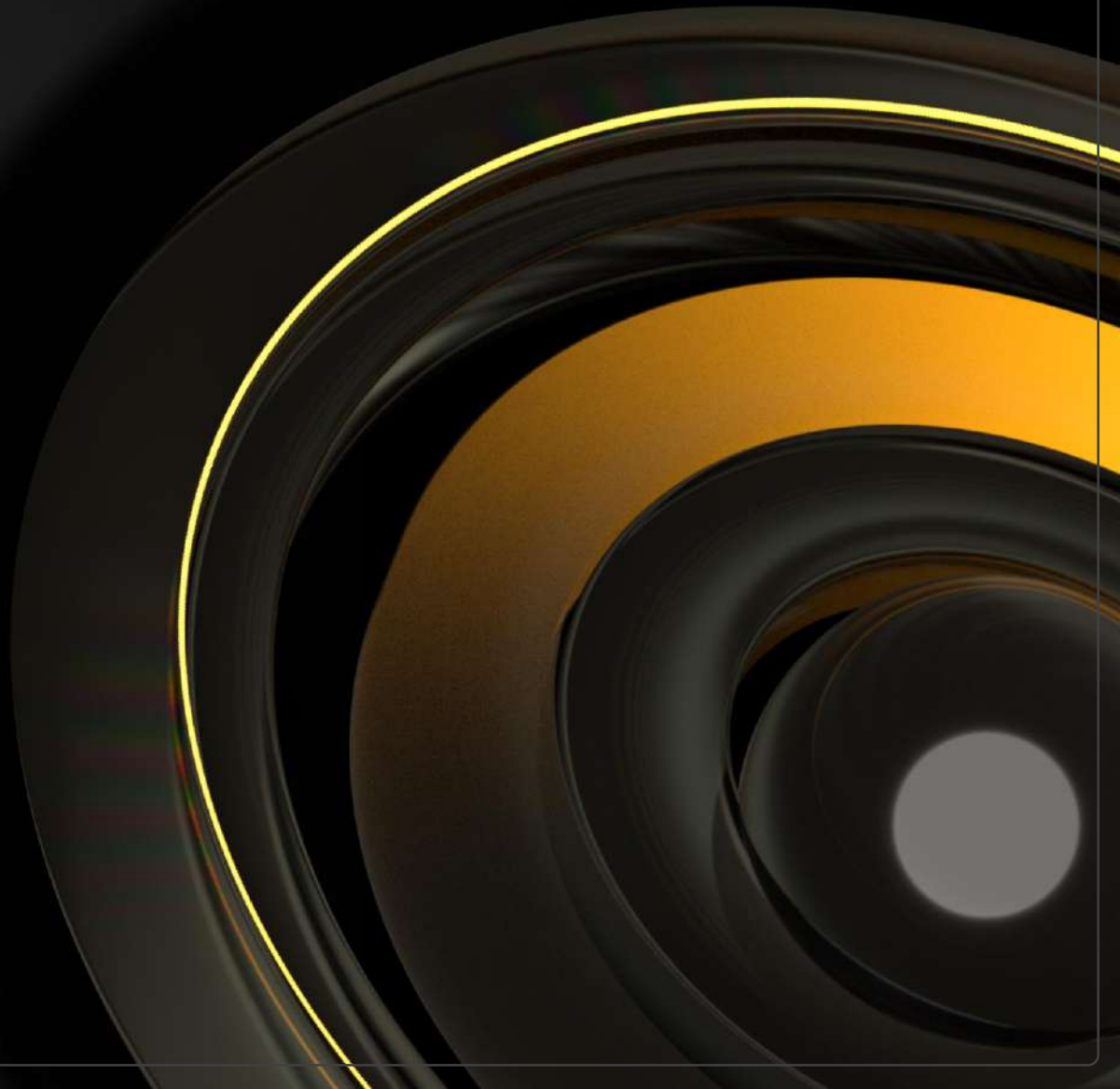
3 ФАКТОРА УСПЕШНОГО РАССЛЕДОВАНИЯ ИНЦИДЕНТА ИБ

Незамедлительное обращение к экспертом при обнаружении атаки

Быстрая реакция на обращение и оперативный сбор рабочей группы расследования

Обязательное выполнение всех рекомендаций от УЦСБ SOC

КЕЙС №2:
ПЕРВЫЕ СИМПТОМЫ



КЕЙС №2: ПЕРВЫЕ СИМПТОМЫ

Кибератаки — хроническая угроза современности

КЕЙС №2: ПЕРВЫЕ СИМПТОМЫ

01
Медленная работа, сбои или частые перезапуски приложений

02
Обнаружение неизвестного ПО, файлов или процессов в системе

03
Получение пользователями доступов к файлам или системам, которые они не используют

04
Внезапное увеличение сетевой активности, особенно в нерабочее время

05
Несанкционированные изменения прав доступа к файлам или их удаление

06
Незнакомые транзакции или изменения настроек учетной записи

07
Неожиданные изменения в системе или создание новых учетных записей

08
Подозрительные электронные письма с вложениями или ссылками

09
Внезапное увеличение загрузки процессора, активности диска или сети

КЕЙС №2: ПЕРВЫЕ СИМПТОМЫ

ЧТО НУЖНО ДЕЛАТЬ ВАМ

Не пытаться самому расследовать инцидент

Не пытаться перевести систему защиты в «боевой режим»

Незамедлительно обратиться к экспертам!

КЕЙС №2: ПЕРВЫЕ СИМПТОМЫ

ПОРЯДОК ДЕЙСТВИЙ ОТ УЦСБ SOC

1. Формирование гипотезы инцидента
2. Постановка задачи: план работ, область исследования, целевые артефакты, с кем работаем на стороне Заказчика
3. Сбор данных для анализа
4. Поиск артефакто в собранных данных, анализ
5. Подготовка к реагированию, при необходимости
6. Реагирование, при необходимости
7. Формирование подробного отчета с исчерпывающим набором мер по недопущению повторного возникновения инцидента ИБ

3 ФАКТОРА УСПЕШНОГО РАССЛЕДОВАНИЯ ИНЦИДЕНТА ИБ

Обращение к профессионалам – не пытайтесь самостоятельно справиться с инцидентом

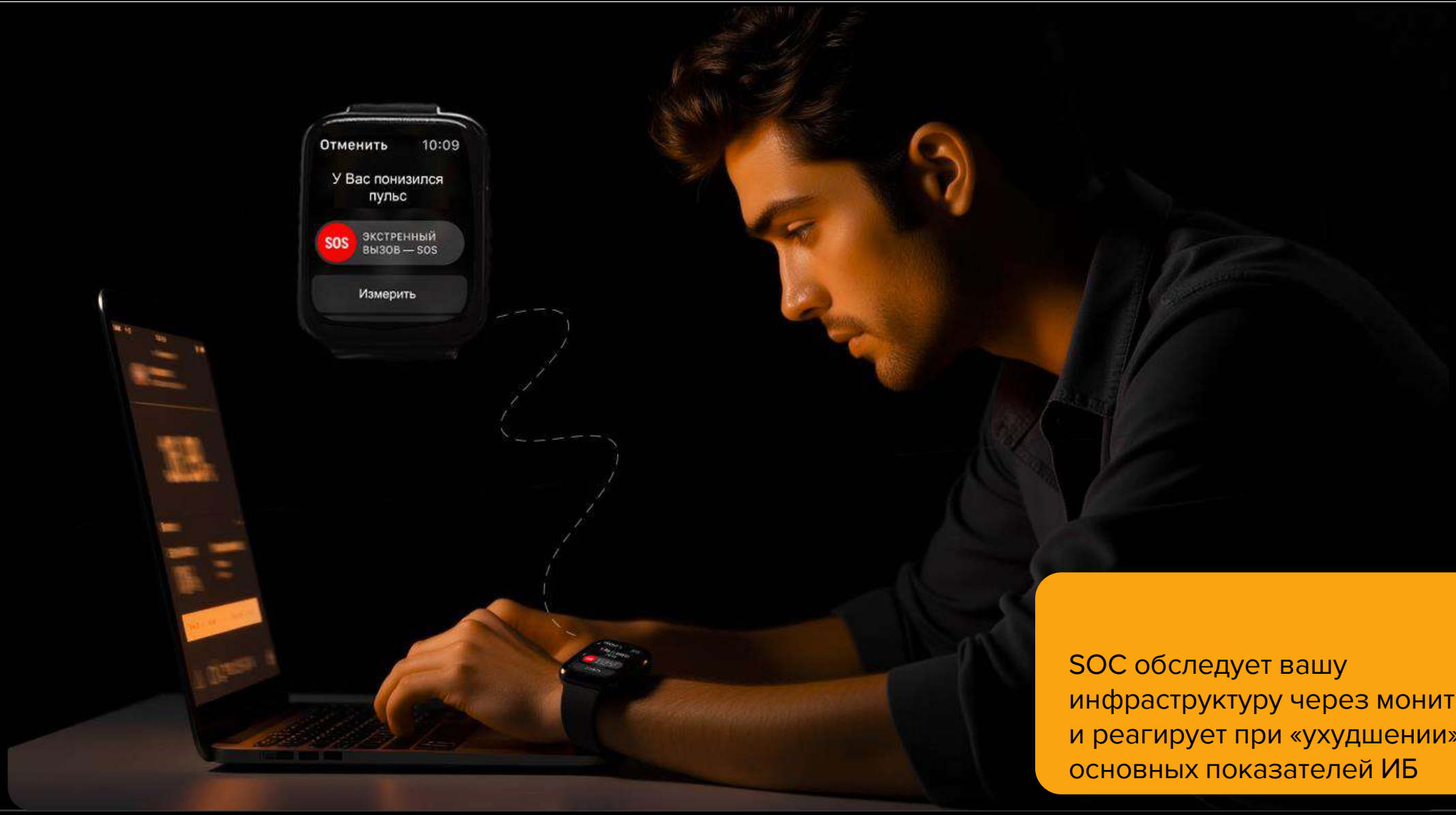
Быстрая реакция на обращение и оперативный сбор рабочей группы расследования

Обязательное выполнение всех рекомендаций от УЦСБ SOC

КЕЙС №3:
МОНИТОРИНГ КИБЕРЗДОРОВЬЯ

КЕЙС №3: МОНИТОРИНГ КИБЕРЗДОРОВЬЯ

USSC SOC



SOC обследует вашу инфраструктуру через мониторинг и реагирует при «ухудшении» основных показателей ИБ

КЕЙС №3: МОНИТОРИНГ КИБЕРЗДОРОВЬЯ

USSC SOC

ЧТО НУЖНО ДЕЛАТЬ ВАМ

Сформулировать перечень ценных бизнес-процессов и активов

Сформировать модель угроз/перечень недопустимых событий и т.п.

Определить состав ресурсов, которые подлежат мониторингу ИБ

Выбрать формат мониторинга информационной безопасности (inhouse, аутсорсинг, гибрид)

Обратиться к специалистам/самостоятельно строить мониторинг ИБ

КЕЙС №3: МОНИТОРИНГ КИБЕРЗДОРОВЬЯ

USSC SOC

ПОРЯДОК ДЕЙСТВИЙ ОТ УЦСБ SOC

1. Выясняем потребности или помогаем сформировать потребности в обеспечении ИБ
2. Формулируем задачи на выстраивание мониторинга ИБ
3. Готовим предложение на систему мониторинга ИБ
4. Формируем команду из наших экспертов
5. Разворачиваем необходимый инструментарий
6. Адаптируем наш опыт мониторинга под ваши бизнес-процессы и потребности
7. Закрепляем процессы и процедуры регламентом взаимодействия

ПОДДЕРЖКА ВАШЕГО КИБЕРЗДОРОВЬЯ С УЦСБ SOC

УЦСБ SOC — ЦЕНТР МОНИТОРИНГА КИБЕРЗДОРОВЬЯБЕЗОПАСНОСТИ

Мы сопровождаем весь процесс:
от выявления инцидента до его полной нейтрализации, устранения последствий и принятия мер по предотвращению его повторного возникновения.

БЫСТРЫЙ СТАРТ
Настроим мониторинг
в течение 14 дней

ГИБКИЙ ПОДХОД
Подстроим сервис
под ваши потребности

ШИРОКАЯ ЭКСПЕРТИЗА
Привлекаем экспертов
из различных сегментов ИБ

24/7
режим оказания услуг

< 15 минут
реакция на инцидент ИБ

> 5 лет
на рынке информационной безопасности

98%
продленных контрактов

ПОРЯДОК ОКАЗАНИЯ УСЛУГ

USSC SOC

1

ОБНАРУЖЕНИЕ И РЕГИСТРАЦИЯ ИНЦИДЕНТА

УЦСБ SOC

Предоставляет инструкции по настройке аудита, осуществляет централизованный сбор событий ИБ, регистрирует инцидент на основе событий ИБ

Наш Заказчик

Обеспечивает настройку источников событий

2

АНАЛИЗ ИНЦИДЕНТА

УЦСБ SOC

Проводит классификацию и анализ инцидента, отсеивает ложные срабатывания

3

РЕАГИРОВАНИЕ НА ИНЦИДЕНТ

УЦСБ SOC

Формирует оповещение об инциденте, предоставляет рекомендации по локализации (сдерживанию) инцидента, ликвидации последствий и предотвращению повторного возникновения инцидента

Наш Заказчик

Организует реализацию рекомендаций соответствующими службами

ПОРЯДОК ОКАЗАНИЯ УСЛУГ

USSC SOC

4 УСТРАНЕНИЕ ПОСЛЕДСТВИЙ ИНЦИДЕНТА

УЦСБ SOC
Реализует рекомендации по устранению последствий инцидента

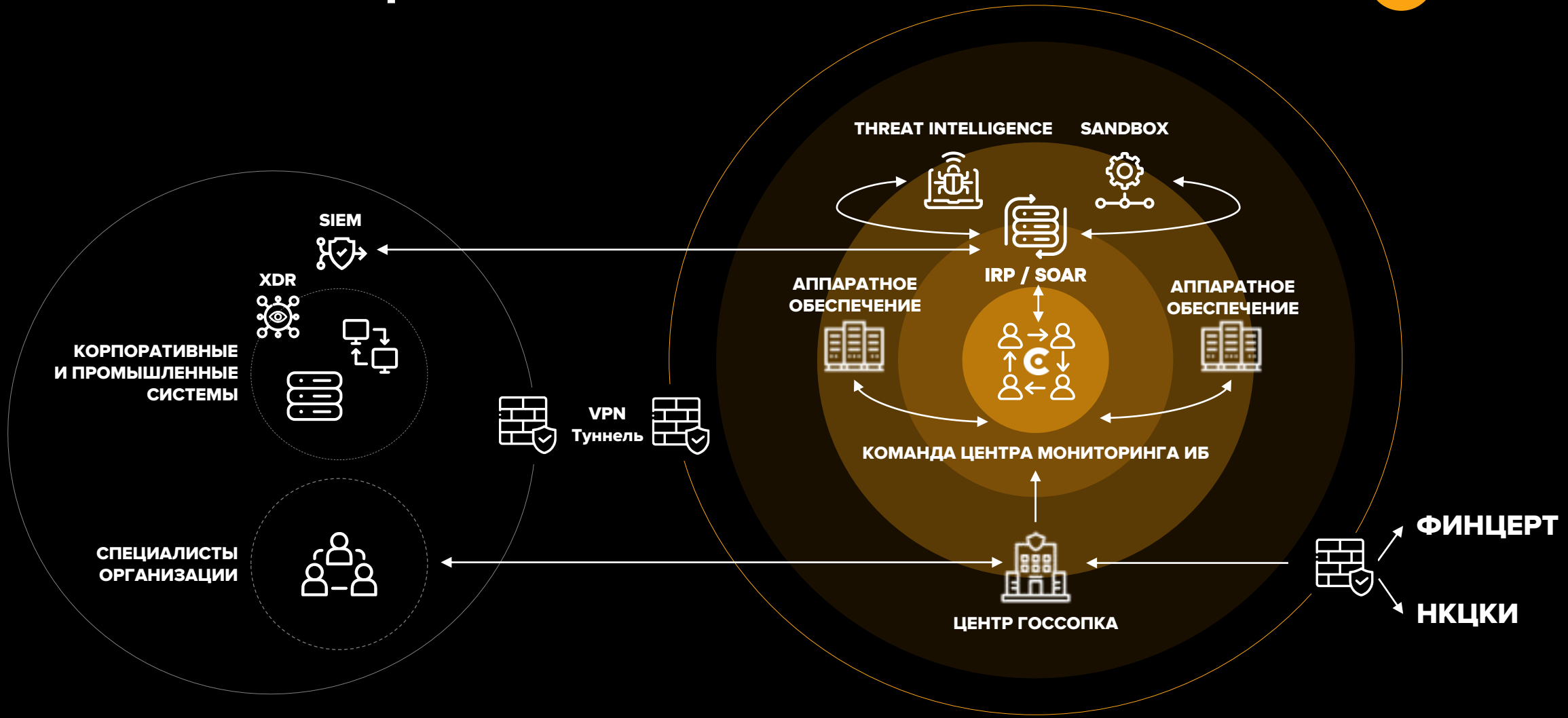
Наш Заказчик
Контролирует и осуществляет сопровождение реализации рекомендаций

5 АНАЛИЗ РЕЗУЛЬТАТОВ ДЕЯТЕЛЬНОСТИ ПО УПРАВЛЕНИЮ ИНЦИДЕНТАМИ

УЦСБ SOC
Представляет статистическую информацию по аналогичным инцидентам, транслирует Заказчику накопленный опыт, корректирует работу мониторинга ИБ (при необходимости)

Наш Заказчик
Планирует реализацию рекомендаций по предотвращению повторного возникновения инцидента

АРХИТЕКТУРА УЦСБ SOC

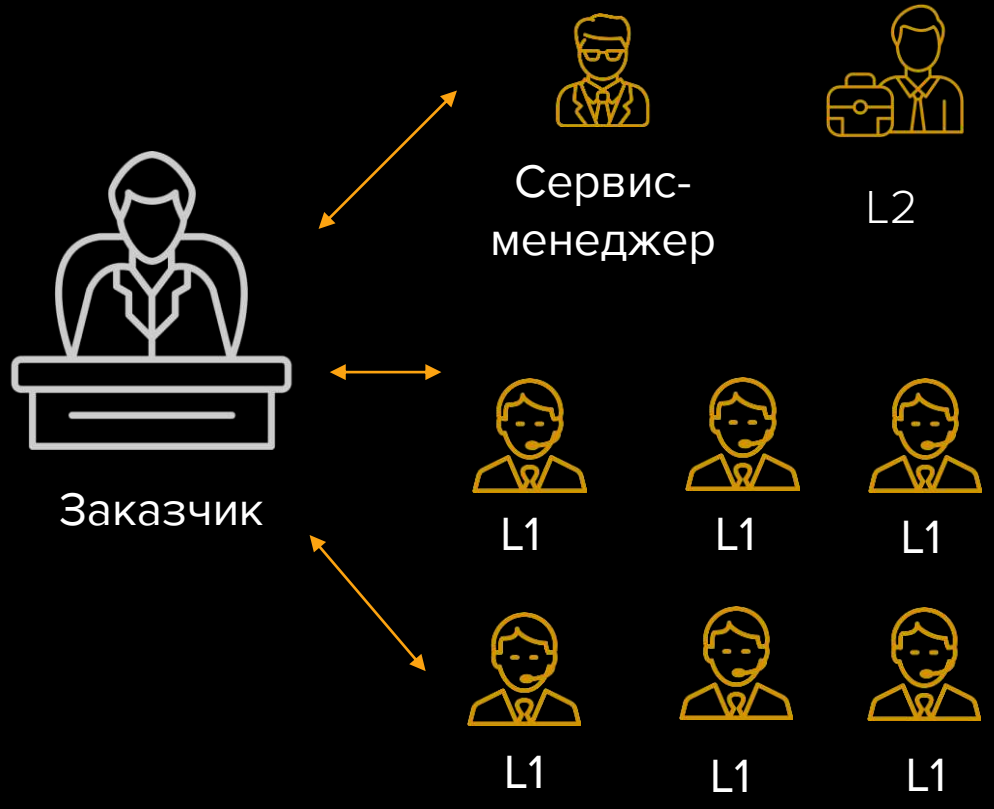


НАШИ ЗАКАЗЧИКИ

УЦСБ SOC

КОМАНДА УЦСБ SOC

ВЗАИМОДЕЙСТВИЕ С ЗАКАЗАЧИКОВ



ВНУТРИ УЦСБ SOC

РЕШАЕМ ПРОБЛЕМЫ БИЗНЕСА

До УЦСБ SOC

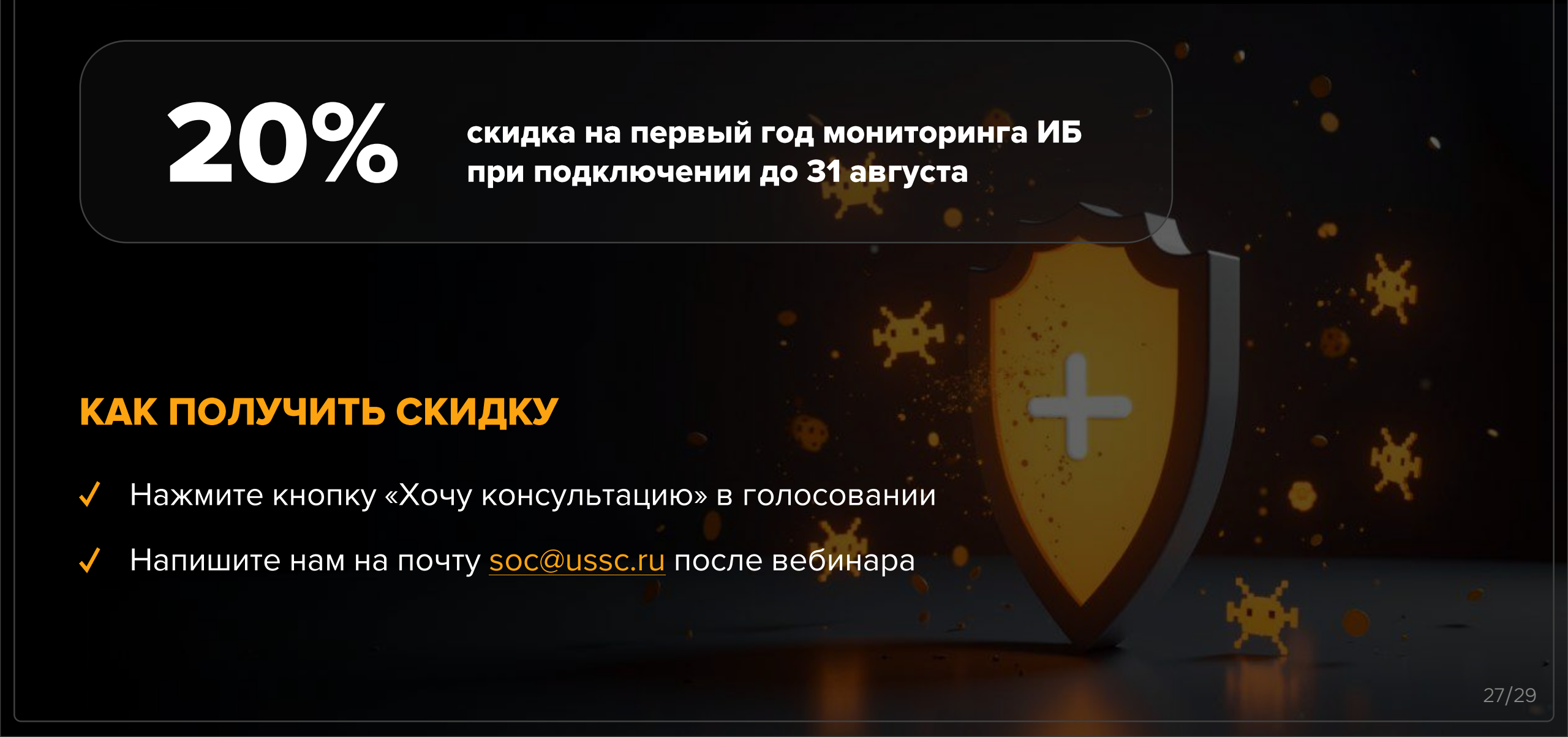
- «Кадровый голод» рынка специалистов по информационной безопасности
- Непрогнозируемые затраты на информационную безопасность
- Обеспечение безопасности данных
- Необходимость быстрой реакции на взломы и предотвращение распространения атаки

С УЦСБ SOC

- **Постоянный доступ к экспертам на аутсорсе**
  Наши эксперты с большим опытом в кибербезе возьмут на себя все рутинные задачи и высвободят время ваших специалистов для решения важных стратегических задач.
- **Прозрачность тарифов и понимание бюджета**
  Подключение к УЦСБ SOC позволит уйти от традиционной модели существенных капитальных затрат на закупку оборудования и ПО к понятным и прогнозируемым операционным платежам. Оплата может быть как годовой, так и другом порядке, который удобен вам.
- **Безопасный SOC**
  Наш центр мониторинга построен на базе собственного кластера гео-разнесенных ЦОД с резервированием каналов связи.
- **Бизнес не терпит убытки из-за взломов и простоя**
  Наши услуги предоставляются в соответствии с SLA, которые определены в договоре. Оперативная реакция и быстрая отработка рекомендаций экспертов SOC позволит вам избежать минимизировать ущерб, а расследование позволит избежать повторений в будущем.

СПЕЦПРЕДЛОЖЕНИЕ ДЛЯ УЧАСТНИКОВ ВЕБИНАРА

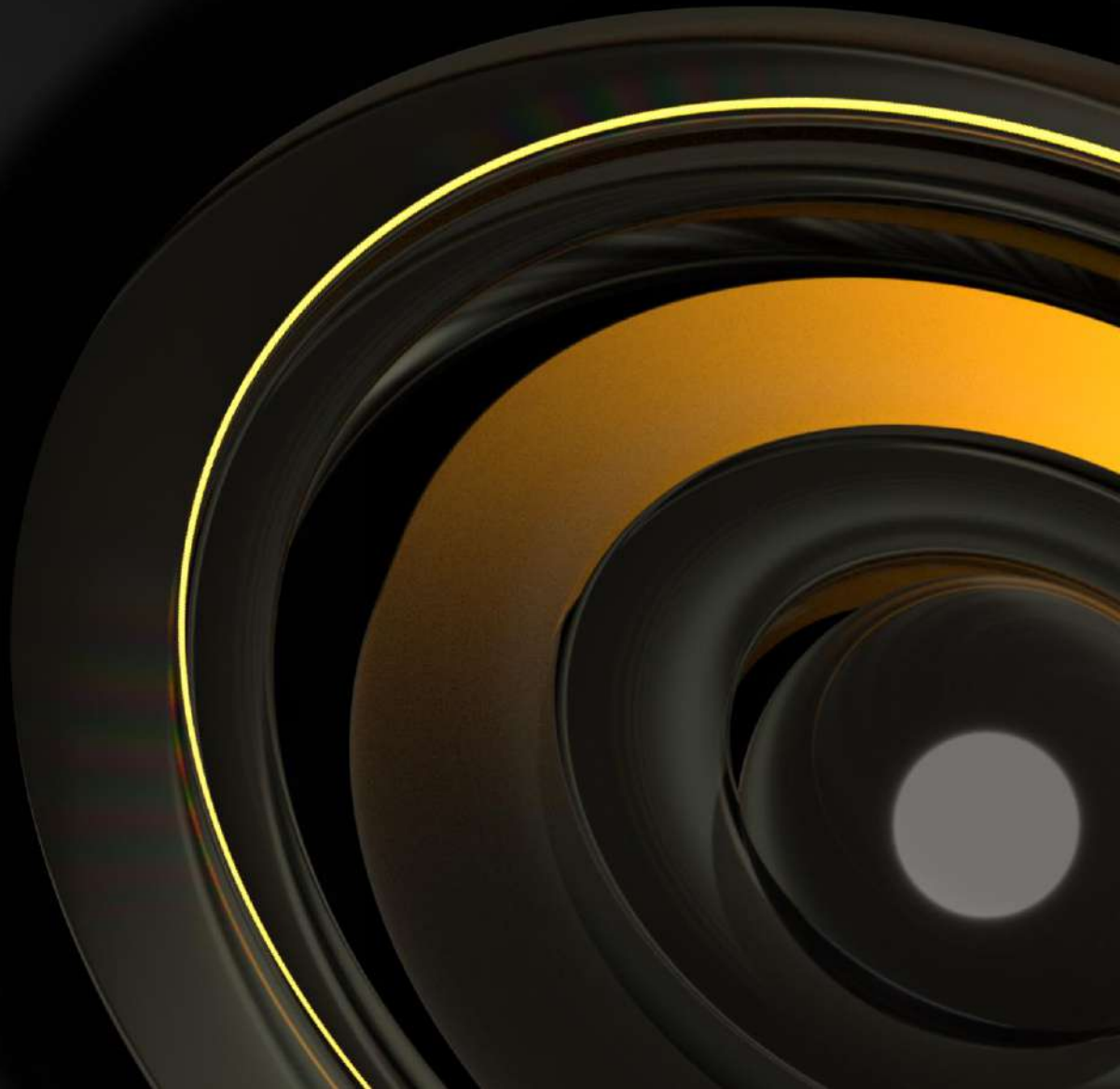
20% **скидка на первый год мониторинга ИБ при подключении до 31 августа**



КАК ПОЛУЧИТЬ СКИДКУ

- ✓ Нажмите кнопку «Хочу консультацию» в голосовании
- ✓ Напишите нам на почту soc@ussc.ru после вебинара

Вопросы?



Security Operations Center

Константин Мушовец

Директор УЦСБ SOC
+7 (913) 036-16-28

soc.ussc.ru