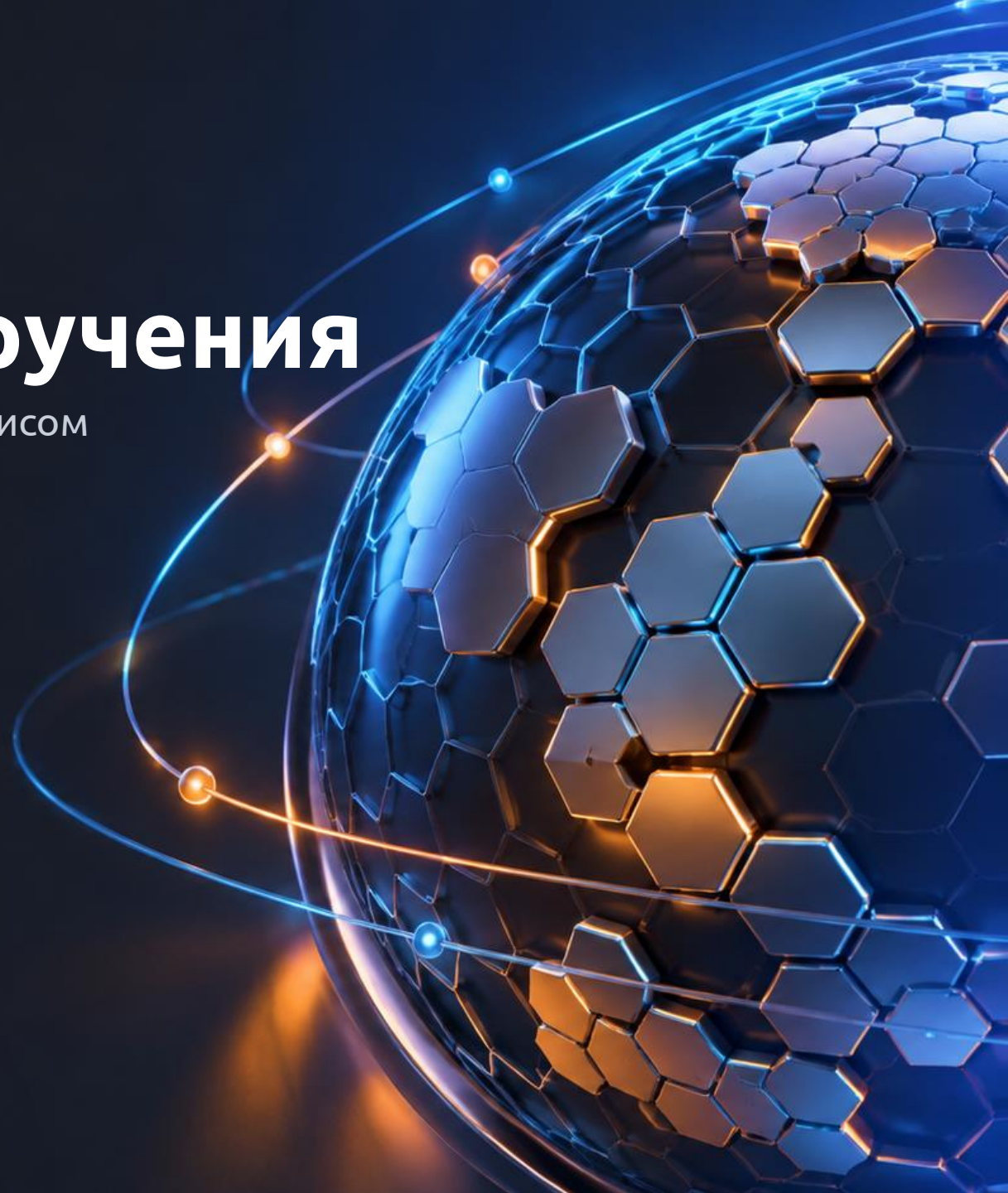


Ampire 360°

Комплексные киберучения

От технического реагирования к управлению кризисом

Кузнецов Андрей



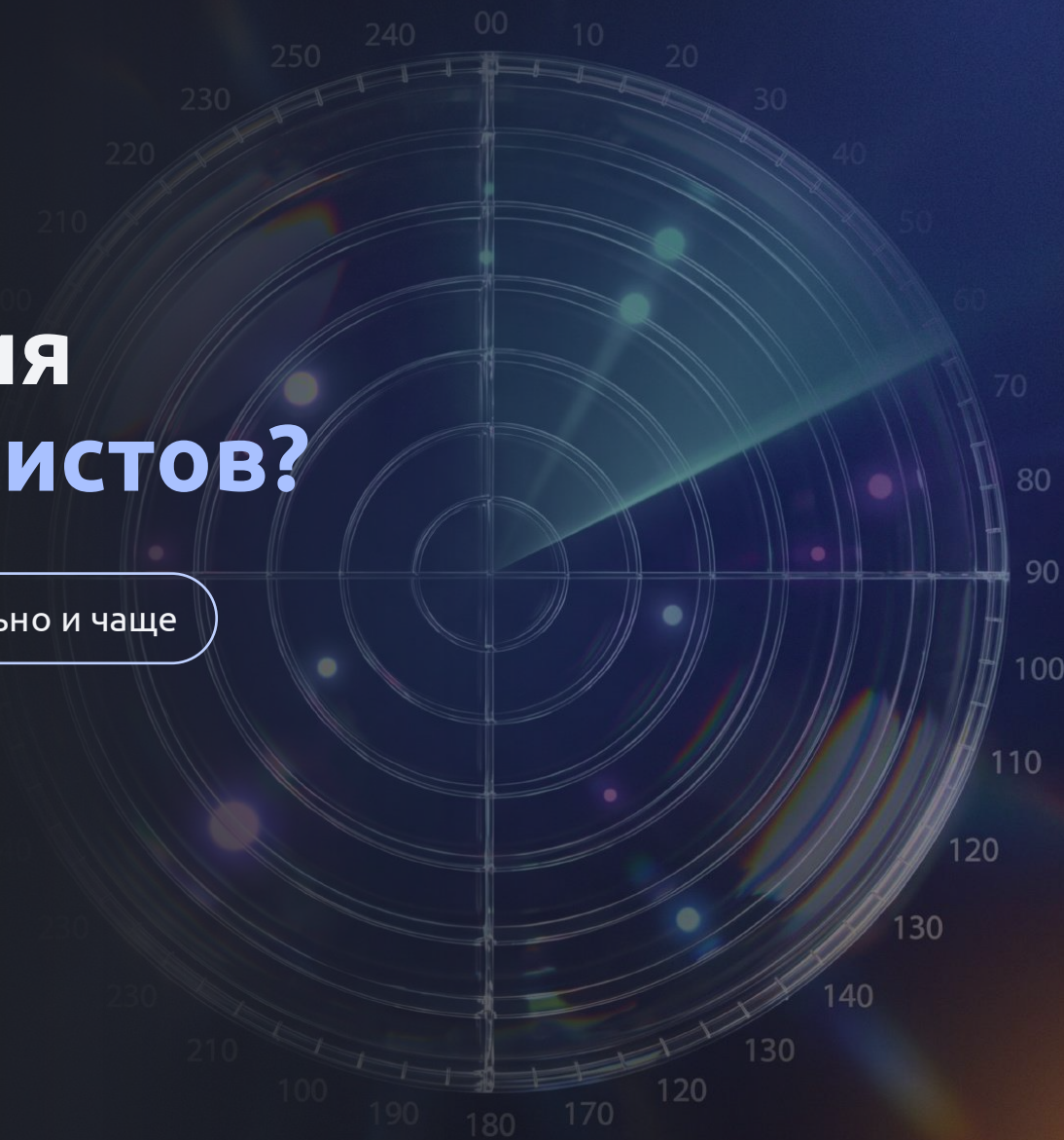
Как часто вы проводите тренировки и киберучения для технических специалистов?

Ни разу

Реже раза в год

1-2 раза в год

Ежеквартально и чаще



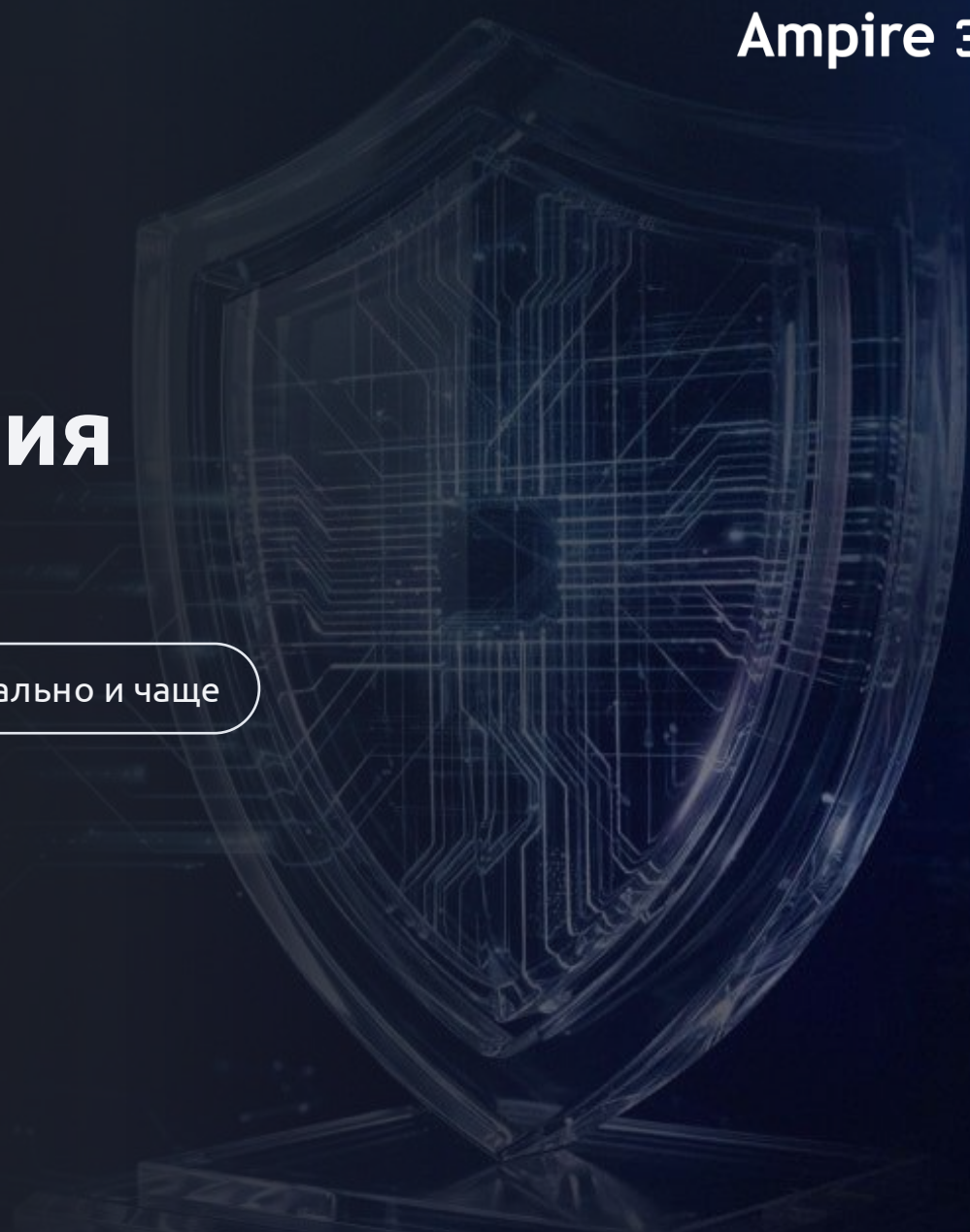
Как часто вы проводите тренировки и киберучения для руководителей?

Ни разу

Реже раза в год

1–2 раза в год

Ежеквартально и чаще

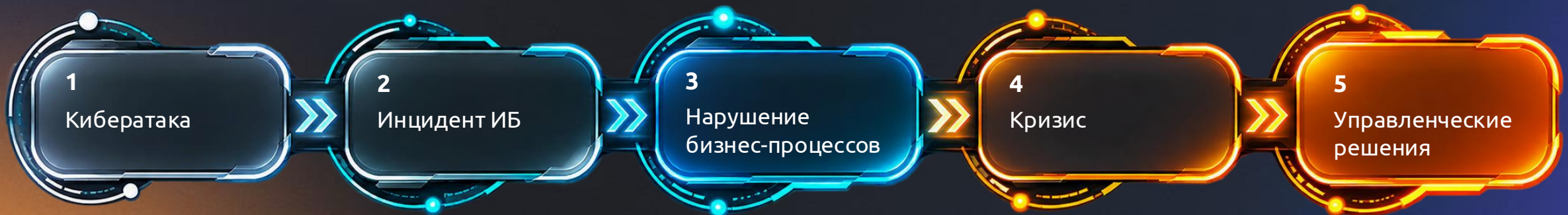


Кибератаку отражает SOC. Киберкризис — вся компания

Ampire 360°

*Ваша команда SOC умеет отражать атаки.
А ваша компания умеет переживать киберкризисы?*

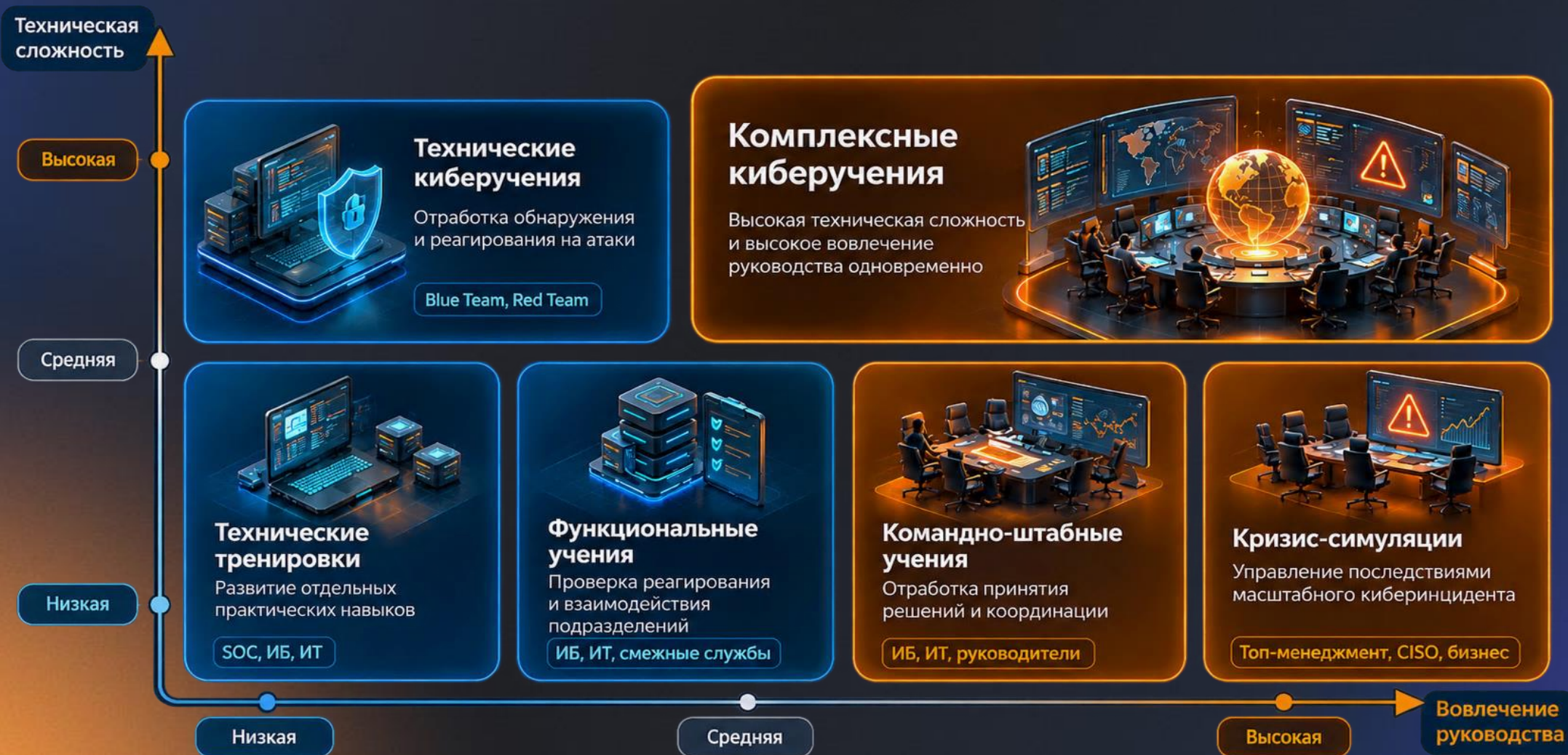
Киберустойчивость — способность всей организации противостоять последствиям кибератак, а не только навык SOC



Киберучения бывают разными

...и решают разные задачи

Ampire 360°



Почему технических киберучений недостаточно?

Можно выиграть техническую кибербитву, но проиграть реальный кризис

ВИДИМАЯ ЧАСТЬ АЙСБЕРГА

Что хорошо проверяют

- Обнаружение и расследование атак
- Работу средств защиты
- Навыки технического реагирования
- Взаимодействие внутри технических команд
- Восстановление инфраструктуры



ПОДВОДНАЯ ЧАСТЬ

Что остается за пределами

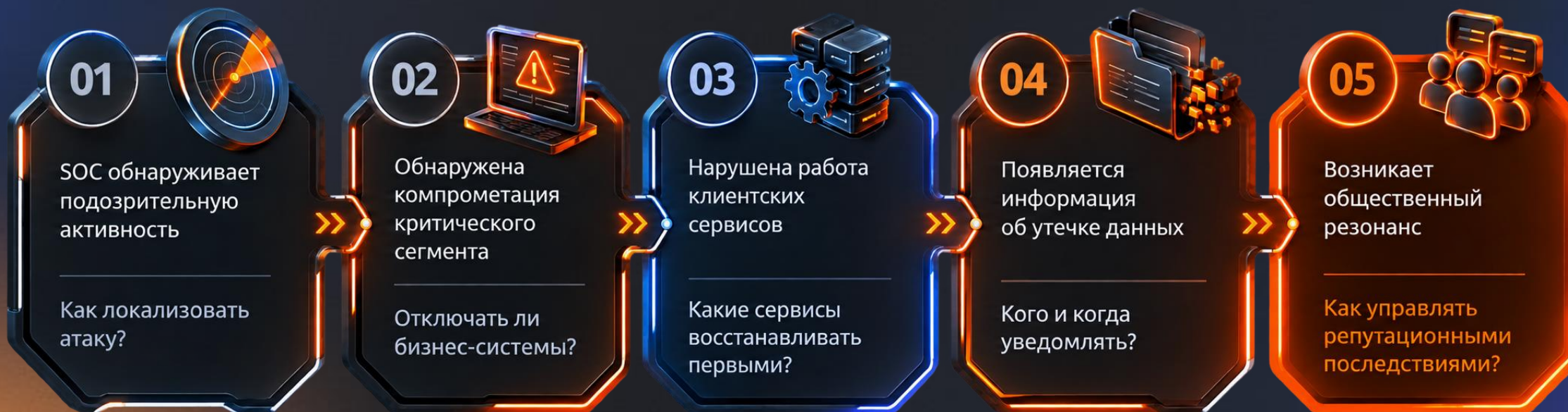
- Принятие управленческих решений
- Межфункциональное взаимодействие
- Управление бизнес-последствиями
- Коммуникации с клиентами и регуляторами
- Работа в условиях неопределенности
- Распределение ответственности между подразделениями



От технического инцидента до кризиса всего несколько решений

На каждом следующем этапе растет цена ошибки и расширяется круг тех, кто принимает решения

Сценарий: атакующие проникли в инфраструктуру банка и начали распространять шифровальщик



Решает SOC

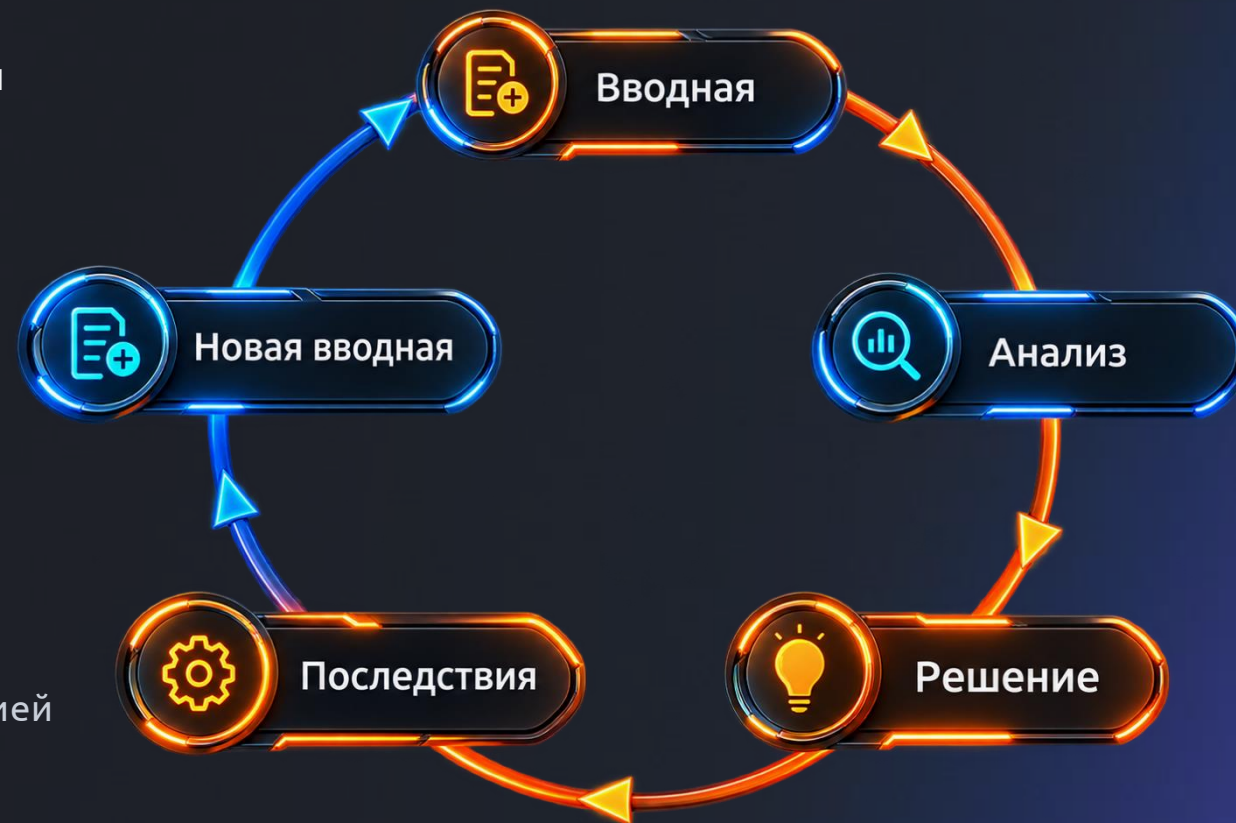
Решает кризисный штаб

Штабные киберучения: тренируем решения, а не инструменты

Моделирование киберинцидента, в котором участники анализируют ситуацию, принимают решения и координируют действия – **без обязательных технических операций** в реальной инфраструктуре

Основные элементы

- Реалистичный сценарий кибератаки
- Последовательное развитие кризисной ситуации
- Вводные с ограниченной и противоречивой информацией
- Решения в условиях ограниченного времени
- Моделирование последствий принятых решений
- Разбор действий и выявление организационных проблем



Зачем штабные учения техническим специалистам?

Технический специалист должен понимать последствия своих решений для бизнеса

КАКИЕ КОМПЕТЕНЦИИ РАЗВИВАЮТ

Оценка бизнес-последствий

Влияние технических решений на бизнес

Коммуникация с руководством

Объяснять сложные угрозы простым языком

Приоритизация действий

Выбор между техническими и бизнес-приоритетами

Принятие решений

Работа в условиях неопределенности

Межфункциональное взаимодействие

Координация SOC, ИТ, ИБ и бизнеса

Эскалация инцидентов

Когда и кого нужно подключать

ПРИМЕР

SOC предлагает изолировать сегмент сети, чтобы остановить атаку. Но это остановит платежную систему

SOC

Остановить распространение атаки

Бизнес

Сохранить доступность критического сервиса

Кто принимает решение и что нужно знать руководству?

Зачем штабные учения топ-менеджменту?

*В условиях киберкризиса руководитель не обязан знать, как работает шифровальщик
Но он обязан понимать, какие решения необходимо принять*

**Сколько времени
потребуется вашему
СЕО, чтобы решить
остановить ключевой
бизнес-процесс из-за
кибератаки?**

Управление кризисом

- Приоритеты организации
- Решения при неполной информации
- Управление ресурсами



Организация взаимодействия

- Формирование кризисного штаба
- Распределение ответственности
- Координация подразделений



Управление последствиями

- Непрерывность бизнеса
- Взаимодействие с регуляторами
- Репутационные риски
- Коммуникации с клиентами и партнерами



Проверка готовности

- Эффективны ли процедуры?
- Понятны ли зоны ответственности?
- Хватает ли информации для решений?



Комплексные киберучения: объединяем техническое реагирование и управление кризисом



Как это работает

- Blue Team обнаруживает и расследует инцидент
- Итоги реагирования меняют ход сценария
- Кризисный штаб получает данные от технических команд
- Решения руководства влияют на действия Blue Team
- Организаторы моделируют бизнес-последствия

Что измерять? От технических метрик к организационной готовности



Техническая готовность Technical Readiness

- Время обнаружения атаки
- Время локализации
- Качество расследования
- Эффективность восстановления
- Успешность противодействия



Организационная готовность Operational Readiness

- Время эскалации инцидента
- Скорость взаимодействия подразделений
- Соблюдение процедур
- Корректность распределения ответственности
- Эффективность коммуникаций



Управленческая готовность Crisis Readiness

- Время принятия решений
- Качество приоритизации
- Обоснованность решений
- Управление бизнес-последствиями
- Управление кризисным штабом

Скорость vs качество

Быстрое решение об отключении инфраструктуры может оказаться неоправданным

Что получает организация по итогам учений

- Оценку готовности технических команд
- Проблемы управленческих решений
- Недостатки процессов реагирования
- План корректирующих мер с ответственными и сроками
- Оценку межфункционального взаимодействия

Киберустойчивость нельзя построить только на технических навыках

01

Технические киберучения необходимы, но недостаточны

Формируют навыки обнаружения, расследования и реагирования, но не проверяют всю систему управления кризисом

02

Штабные киберучения нужны не только руководителям

Развивают взаимодействие технических команд и бизнеса, помогают принимать согласованные решения

03

Будущее за комплексными киберучениями

Единый сценарий связывает технические действия, организационные процессы и управленческие решения

ТЕХНОЛОГИИ

+

ПРОЦЕССЫ

+

ЛЮДИ

=

КИБЕРУСТОЙЧИВОСТЬ

Киберустойчивость – это не способность SOC остановить атаку. Это способность **всей организации** сохранить управляемость, продолжить критические операции и восстановиться после киберинцидента.

ВОПРОС, КОТОРЫЙ СТОИТ ЗАДАТЬ СЕБЕ

«Мы годами учим специалистов правильно реагировать на кибератаки. Но как часто мы учим руководство правильно реагировать на действия **собственных специалистов?**»



Кузнецов Андрей

Telegram: @OT_security
+7 926 666 71 78

