SOC FORUM 2023

Purple Team: адаптация к меняющемуся ландшафту проблем кибербезопасности

Спикер

SOC FORUM 2023

Алексей Гришин

CPO CICADA8, основатель VOLGA CTF, бывший тренер World Skills, и в целом полезный.

14 лет

организации CTF

12 лет

работы в ИБ

9 лет

преподавания ИБ по профильным направлениям

CICADA8

О чем сегодня поговорим?

SOC FORUM 2023

- Эволюция в обучении ИБ
- Проблемы кадрового рынка ИБ
- Почему CTFы дают увеличивают интерес к ИБ, но не решают проблему
- Ниша образовательного рынка занята киберполигонами
- Неохваченный потребительский сектор
- Закрытие потребности услугами Red/Purple Team

Эволюция в обучении информационной безопасности

SOC FORUM 2023

1990-е

Первые продукты CISCO для создания отдельных сетей и выделения отдельных ветвей безопасности

1993

Первая конференция Defcon с соревнованием по кибербезопасности Capture the Flag (CTF)

2001

Securing Cisco IOS Networks
Первые вендорские курсы «основы обеспечения безопасности в сетях»

2008

RUCTF: Зарождение в РФ образовательной методики в соревн-овательном формате

2020

Киберполигон Минцифры

Общее образование в сфере ИБ

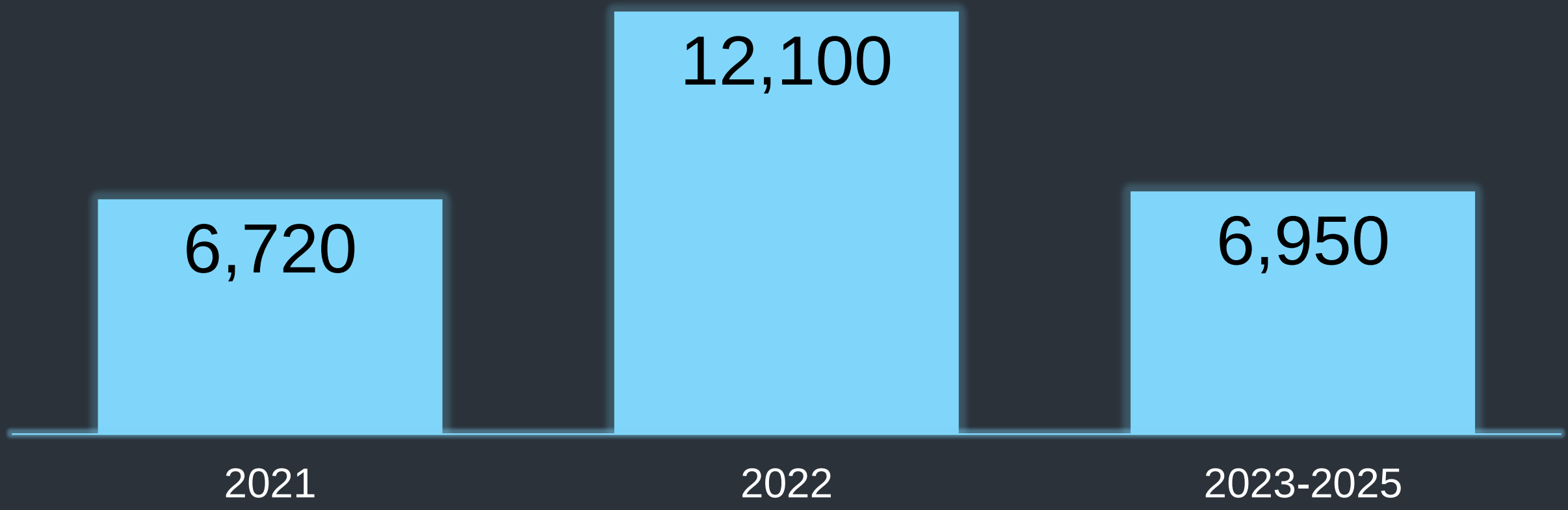
Эксперт, как швейцарский нож, осведомлен во всех направлениях ИБ

- Forensics
- Cryptography
- AppSec
- DevSecOps
- Pentest
- Complains

CICADA8

Потребность в специалистах по защите информации

SOC FORUM 2023



Данные ФСТЭК России

CTF как тренд вовлечения в ИБ

SOC FORUM 2023

Геймификация практических заданий по ИБ с ранжированием сложности

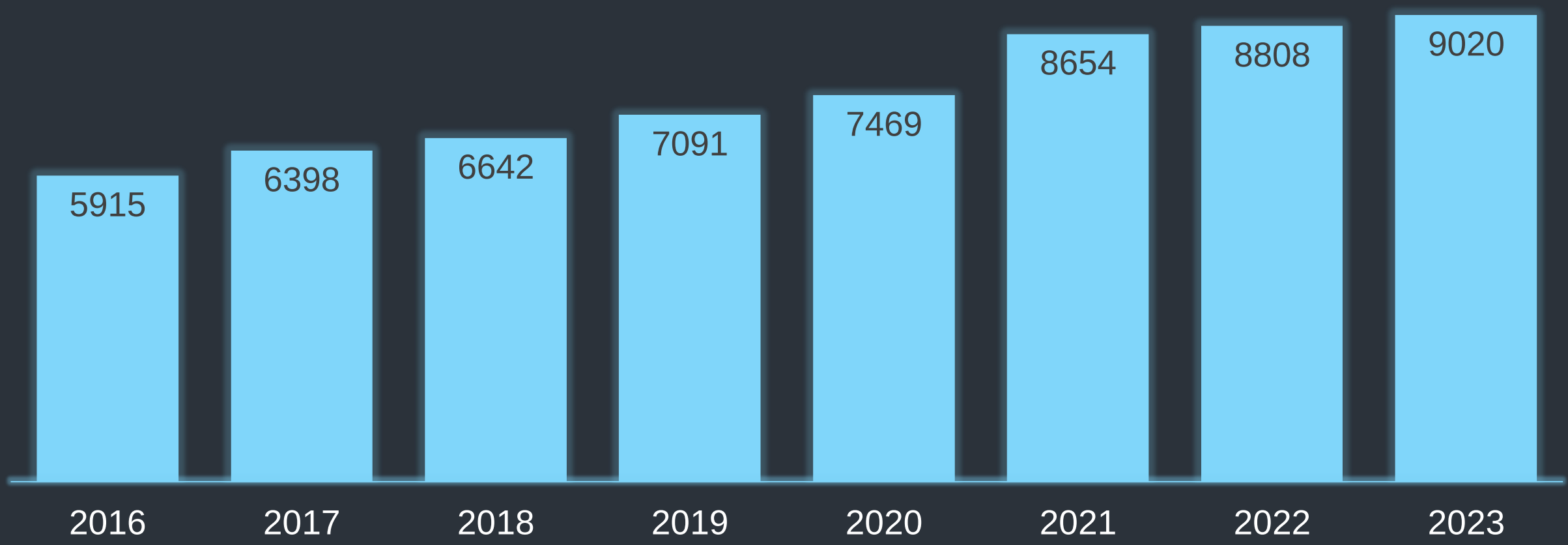
Охват всех возрастных групп: от учащихся стершей школы до молодых специалистов

Насыщенный график соревнований с доступом в online-режиме

CIDADA

Динамика роста объема контрольных цифр приема по специальностям и направлениям подготовки «Информационная безопасность»

SOC FORUM 2023



CIDADA[8]

Данные ФСТЭК России

Проблема не решена

SOC FORUM 2023

- Задание в вакууме (один сервис – одна бага)
- Отсутствие документирования работ (полное)
- Низкая командная работа
- Задача обучения в приоритете
- Максимум offensive, минимум defensive
- Развивает только hard skills

> …площадок, где ты можешь сперва тыкнуть кавычку, потом перед тобой появляется код, ты его как-то пытаешься исправить и дальше на стороне бэкенда обучающего портала прогоняются тесты, пока у тебя не пройдет тест, который закрывает эти кавычки.
>
> *Ольга Свиридова,*
> *руководитель триаж-команды Standoff 365*

Современное решение проблемы

CIDADA8

Национальный киберполигон

SOC FORUM 2023

Мультифункциональный программно-аппаратный комплекс для тренировки и проверки киберзащитных навыков и реакции персонала, а также для разработки и тестирования киберзащитных систем и стратегий.

- Контролируемая среда, где специалисты могут безопасно проводить учебные и тестовые мероприятия информационной безопасности
- Наличие тренингов, симуляций атак и учебных программ для специалистов в области кибербезопасности
- Отчет по завершению киберучений с рекомендациями по траектории развития

ИСКУССТВЕННАЯ СРЕДА

CIDADA8

А в чём разница?

SOC FORUM 2023

CTF

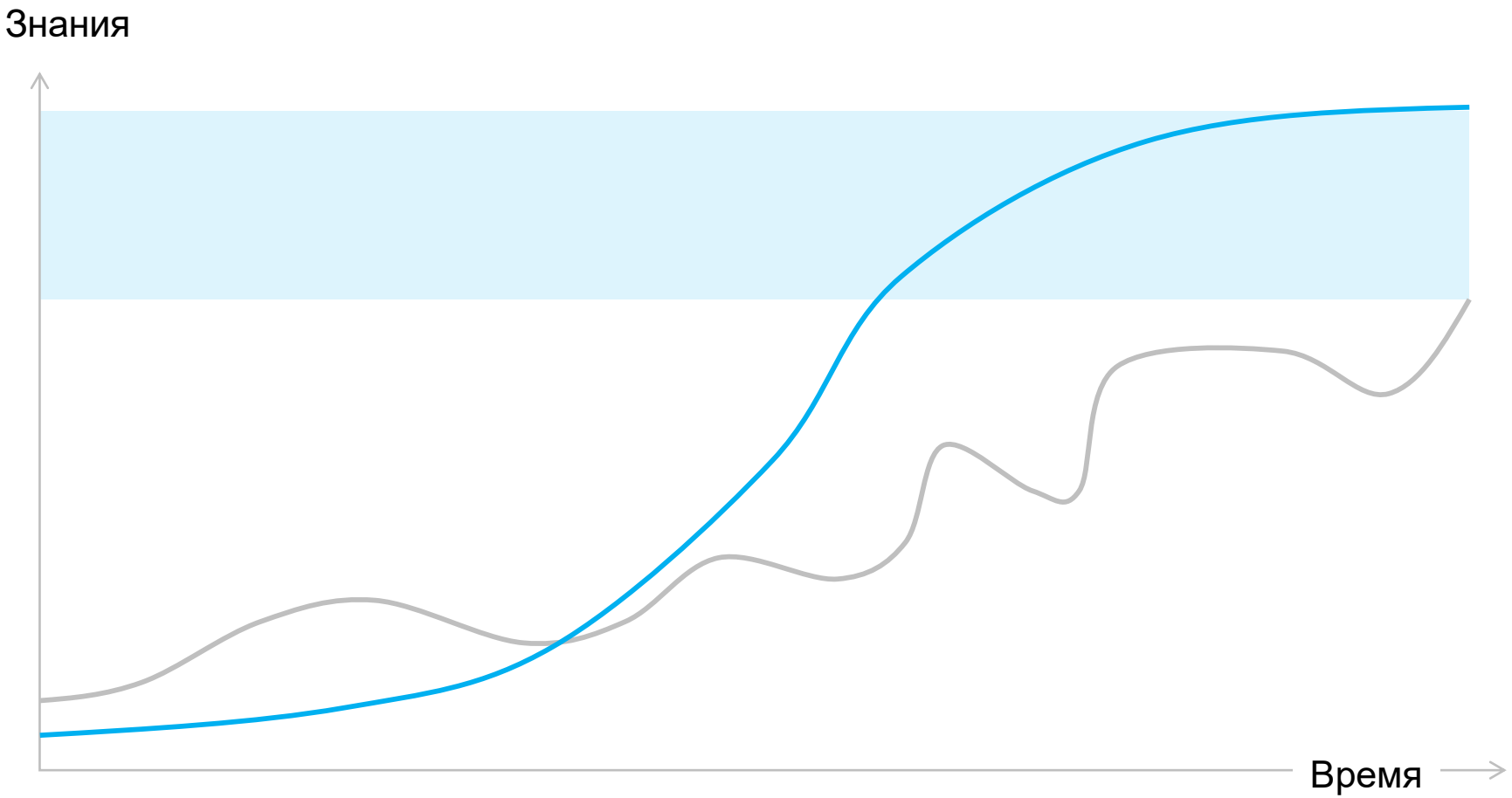
- Олимпиадные условия
- Личные достижения
- Акцент на offensive умениях участников

Киберполигон

- Конкурентные условия
- Успех только при командной работе
- Основной упор на мониторинг

Различие подходов

SOC FORUM 2023



CTF

Киберполигон

УЧИТЕЛЬ КОМПЕНСИРУЕТ ФАЗУ РЕГРЕССА

CIDADA8

Неохваченных потребительский сектор

CICADA8

Секторы

SOC FORUM 2023

13,6 тыс.
Крупный бизнес

18,7 тыс.
Средний бизнес

215 тыс.
Малый бизнес

63%
СМБ имеют корпоративный сайт

Данные ФНС, Интерфакс и Аналитического центра НАФИ

Обучение через RED Team

SOC FORUM 2023

Оценка методик обнаружения и процессов реагирования на инциденты

Практическая оценка уровня защищённости ключевых бизнес-рисков и недопустимых событий

Формирование и актуализация модели угроз

Оценка эффективности работы ИБ подразделений

CIDADA8

Обучение через PURPLE Team

SOC FORUM 2023

Оценка методик обнаружения и процессов реагирования на каждом MITRE-кейсе

Поэтапная реализация всех кейсов MITRE в соответствии с моделью злоумышленника

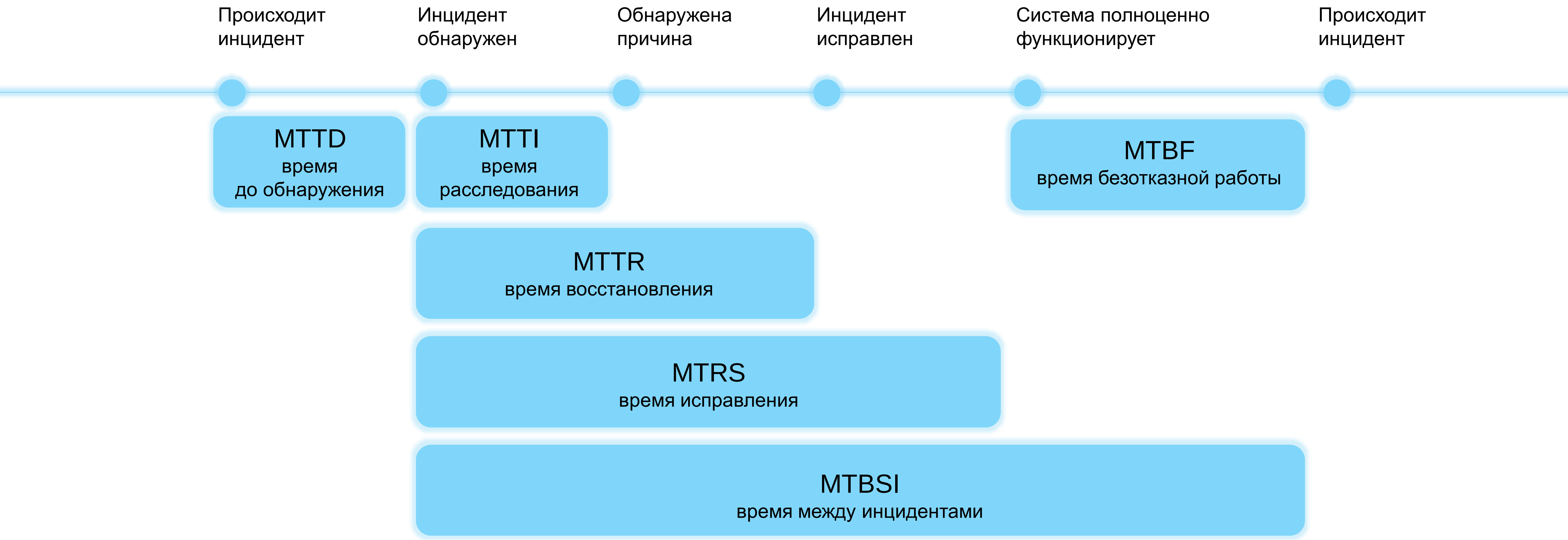
Совместная работа по повышению по эффективности инструментов мониторинга и обнаружения

Рекомендации по разработке и/или внедрению дополнительных уровней контроля

CIDADA8

Временная шкала инцидента

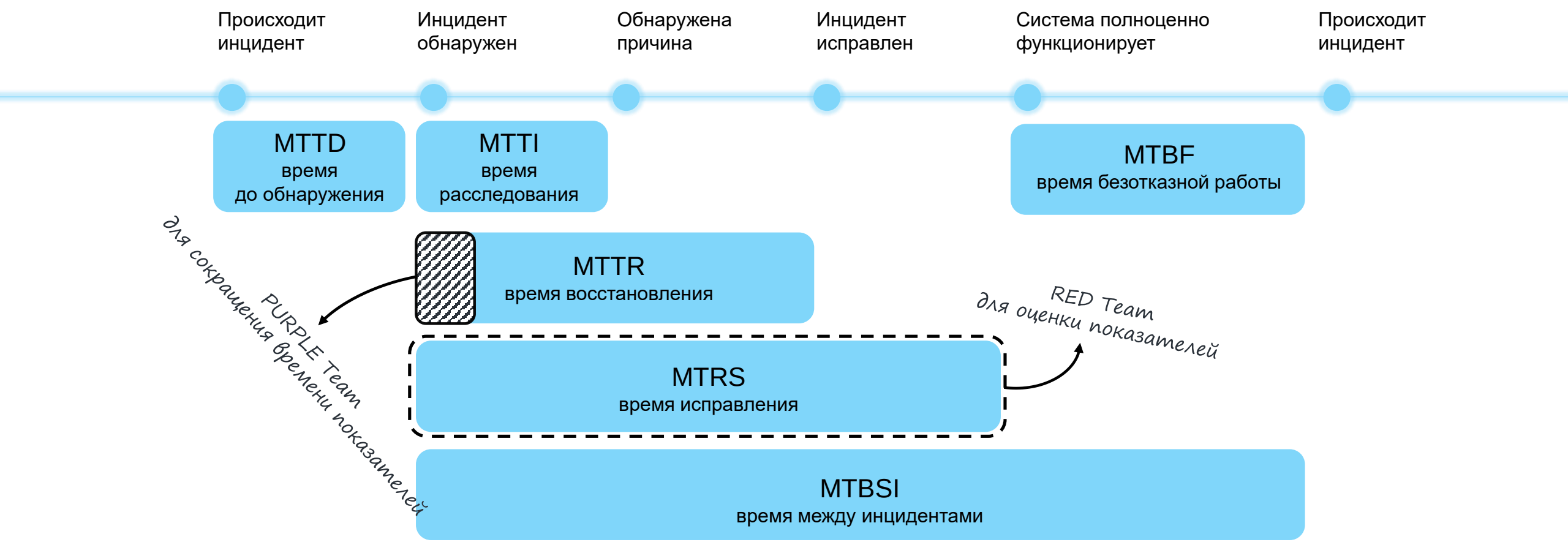
SOC FORUM 2023



CICADA8

Временная шкала инцидента

SOC FORUM 2023



Основные различия RED TEAM, PURPLE TEAM

SOC FORUM 2023

RED TEAM
ЭТО ПУПСЕНЬ!

PURPLE TEAM
А ЭТО ВУПСЕНЬ!

Цель	Проверка практической кибербезопасности	Улучшение практической кибербезопасности
Методы	Имитация кибератаки и оценка действий службы кибербезопасности	Отработка различных векторов атаки и улучшение уровня защиты
Обучающая роль	Экзаменатор	Ментор/учитель

CIDADA8

SOC FORUM 2023

ЗАДАЙ ВОПРОС ЭКСПЕРТАМ

Futurecrew@mts.ru