Быть лучше каждый день

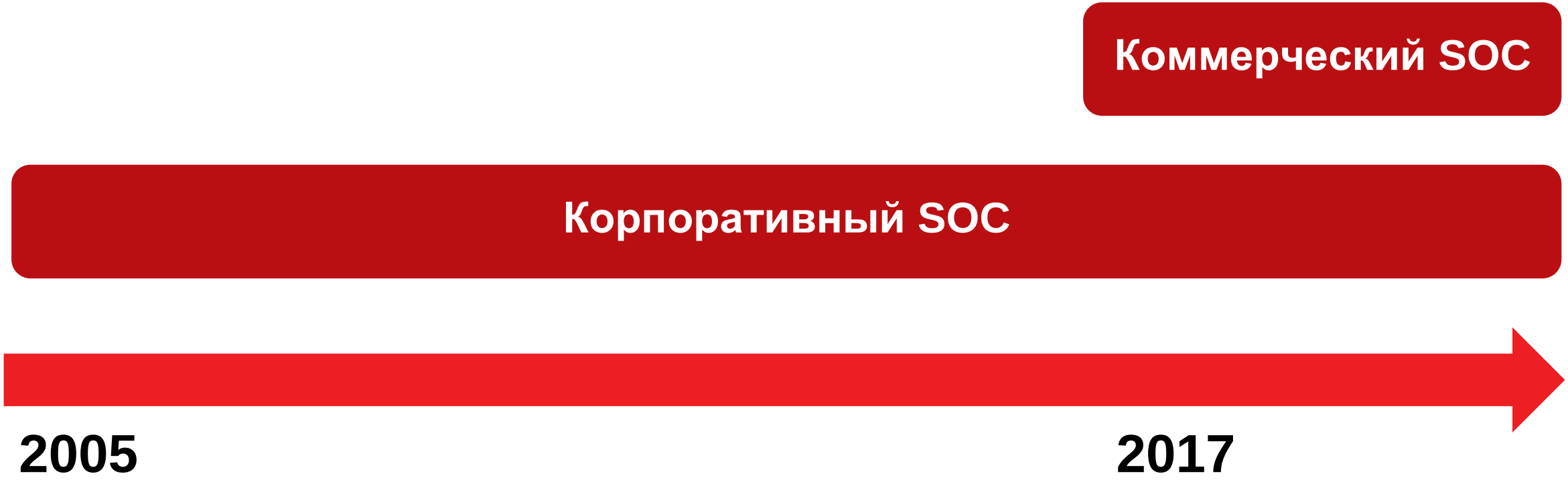
Критерии эффективности центров кибербезопасности

Андрей Дугин
Начальник отдела обеспечения информационной безопасности
Руководитель SOC

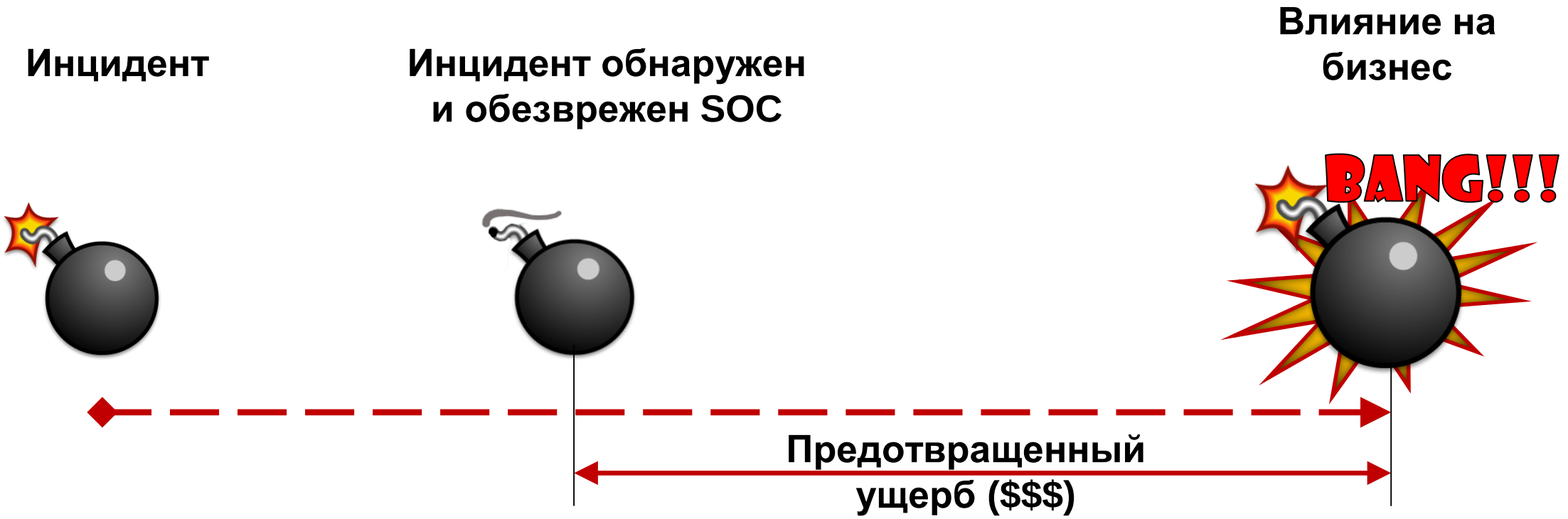
Зона покрытия центра кибербезопасности SOC МТС

- 11 часовых поясов
- Десятки тысяч сотрудников
- Десятки тысяч ПК/ноутбуков
- Десятки тысяч серверов
- Тысячи единиц активного сетевого оборудования
- >1000 диапазонов внешних IP

Этапы развития центра кибербезопасности SOC в МТС



Ценность центров кибербезопасности SOC для бизнеса

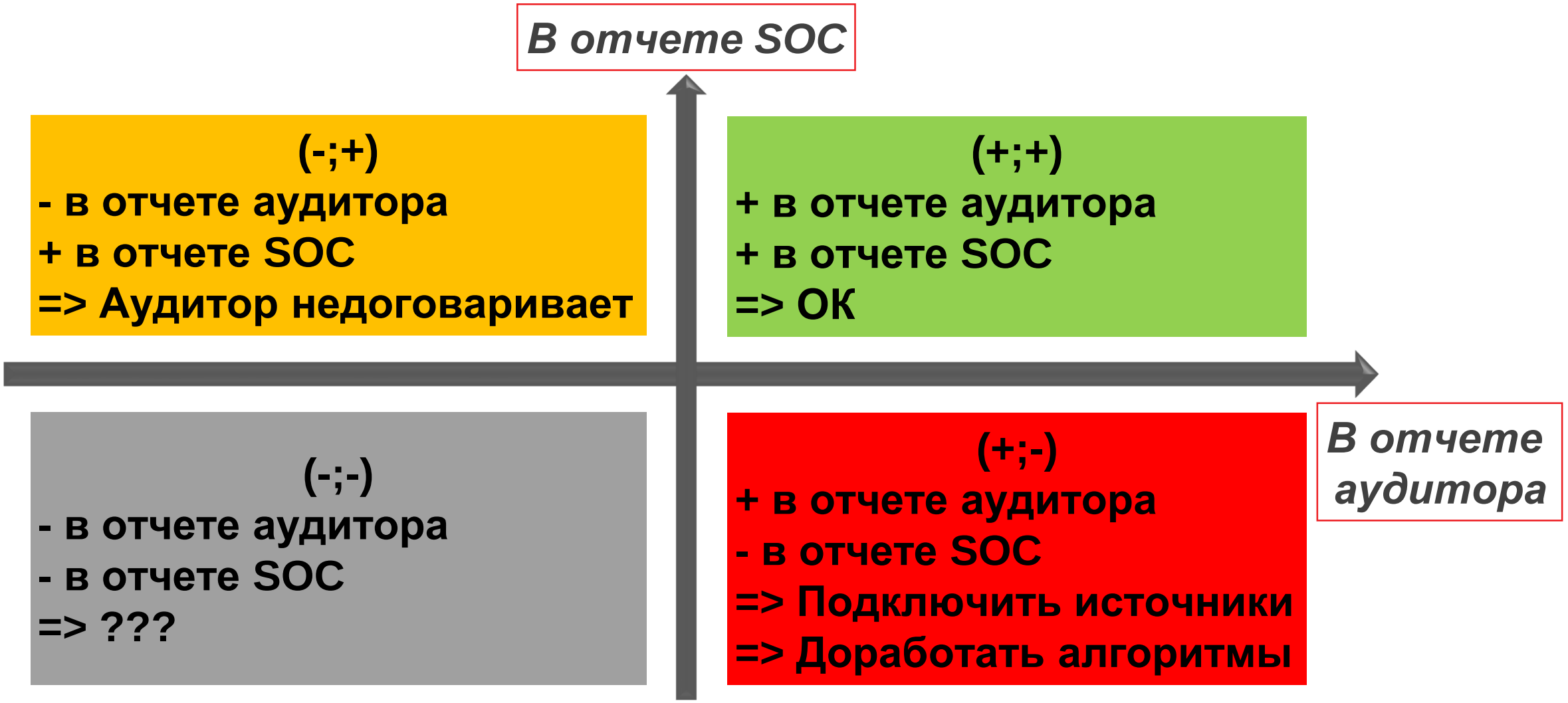


Качество и полнота данных 100%

Качество и полнота данных менее 100%

Время как критерий эффективности SOC

Аудит как критерий эффективности зоны покрытия SOC



Базовые критерии эффективности центров кибербезопасности SOC

- Время реагирования на атаки
- Время отражения атак
- Качество сбора и хранения данных
- Качество зоны покрытия
- Качество алгоритмов генерации инцидентов ИБ
- Степень автоматизации рутинных операций
- % ложных срабатываний
- % пропусков атак

Q&A