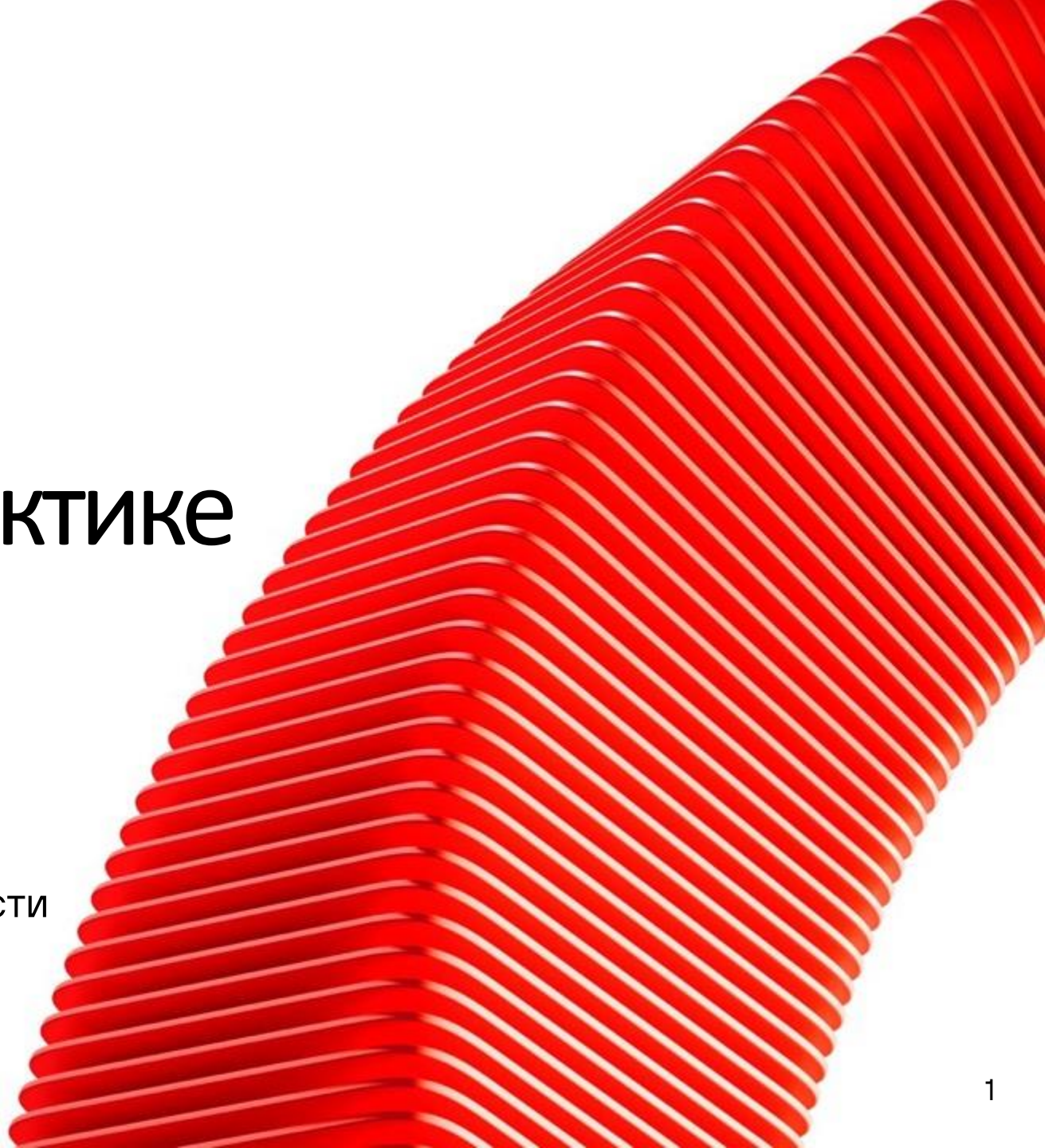
Базовые метрики киберустойчивости предприятия на практике



Михаил Кадер

Архитектор по информационной безопасности

О реальном авторе ;-)

Константин Смирнов
Советник управляющего директора по бизнес-консалтингу

Окончил МГТУ им. Баумана по специальности «инженер-системотехник», работал в Oracle, Symantec, Accenture, IBM. С 2022 – работает в Positive Technologies.

Занимался трансформацией ИТ, обеспечением бесперебойности ИТ и непрерывности бизнеса, оттуда перешёл в ИБ, в область построения SOC и реагирования на инциденты. Проектировал и внедрял решения и процессы, писал стратегии, в РФ и за рубежом.

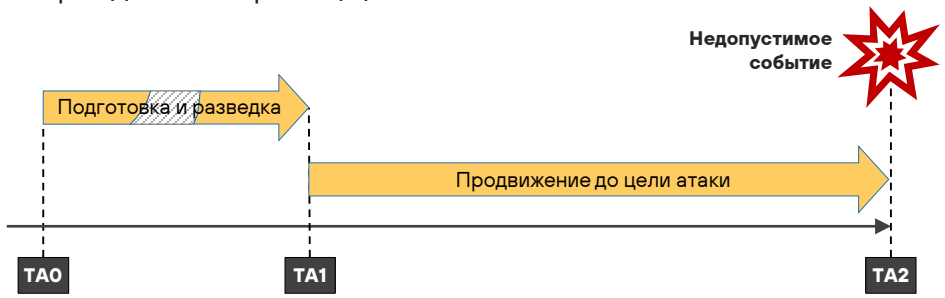
В прошлом - CISA, CBCP, MBCI :=)

ksmirnov@ptsecurity.com
@i94d44027

02.05. Время атаки (TTA)

Что такое TTA?

Время атаки (TTA, Time To Attack) – время от начала преодоления периметра сети до начала выполнения действий над целевой системой, фактически до момента преодоления границ целевой системы.



Примечание 1: Время разведки и подготовки к атаке – случайная неотрицательная величина (TA1-TA0). В силу того, что повлиять на это значение в рамках мер, рассматриваемых в данной концепции, невозможно, то этот параметр мы рассматривать не будем. Параметр приведён только для иллюстрации.

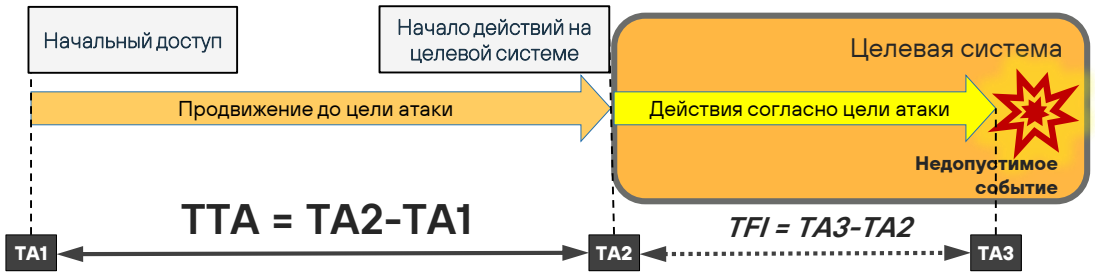
Примечание 2: Почему не измерять время до завершения атаки? Длительность действий атакующего может быть весьма различной, в зависимости от целей атаки, а также от необходимости соблюдать скрытность.

Как мы измеряем TTA?

Некоторые важные соображения

- Атака может привести к недопустимому событию, но сама по себе не является недопустимым событием.
- Недопустимые события могут иметь протяжённость во времени (например, прерывание сервиса на 24 часа)
- Некоторые НС могут практически не иметь длительности (например, дефейсмент сайта – скриншот и немедленная публикация или авария на производстве через нарушение конфигурации промавтоматики)
- Некоторые НС могут быть осуществлены не мгновенно, но достаточно быстро (нелегитимный перевод денег)
- Некоторые НС могут потребовать весьма существенного времени на реализацию (кража существенного объёма данных низким темпом, *syphoning data*, чтобы не привлекать внимание)

Время атаки – от и до



Время атаки (TTA, Time To Attack) – время от начала преодоления периметра сети [TA1] до начала выполнения действий согласно цели атаки на целевой системе [TA2].

Примечание: в ряде случаев, когда мы точно знаем, сколько времени может занять реализация самого НС, мы можем используем дополнительный параметр – время, затрачиваемое на выполнение действий согласно цели атаки, Time For Impact, TFI = TA3-TA2.

02.06. Прочие важные метрики инцидента ИБ (1/2)

Метрики атаки

Метрика	Начало	Конец	Формула	Определение	Примечание
TTA	Первоначальный доступ атакующего в ИТ-инфраструктуру	Начало реализации НС	**TA2-TA1**	Time To Attack, время атаки – время от первоначального доступа до момента начала реализации НС.	До момента, когда агент угрозы может приступить к нанесению ущерба, являющегося целью атаки.
TPT	Первоначальный доступ атакующего в ИТ-инфраструктуру	Окончание устранения агента угрозы	**TR7-TA1**	Threat Presence Time, время присутствия агента угрозы в ИТ-инфраструктуре.	
TAT	Первоначальный доступ атакующего в ИТ-инфраструктуру	Окончание локализации агента угрозы	**TR6-TA1**	Threat Active Time, время активной деятельности агента угрозы. Временной отрезок в котором агент угрозы может продолжать своё продвижение к цели атаки.	
GT	Первоначальный доступ атакующего в ИТ-инфраструктуру	Первичная сработка СЗИ (первые события)	**TR0-TA1**	Ghost Time, время невидимого (для защитников) присутствия агента угрозы (до начала обнаружения).	

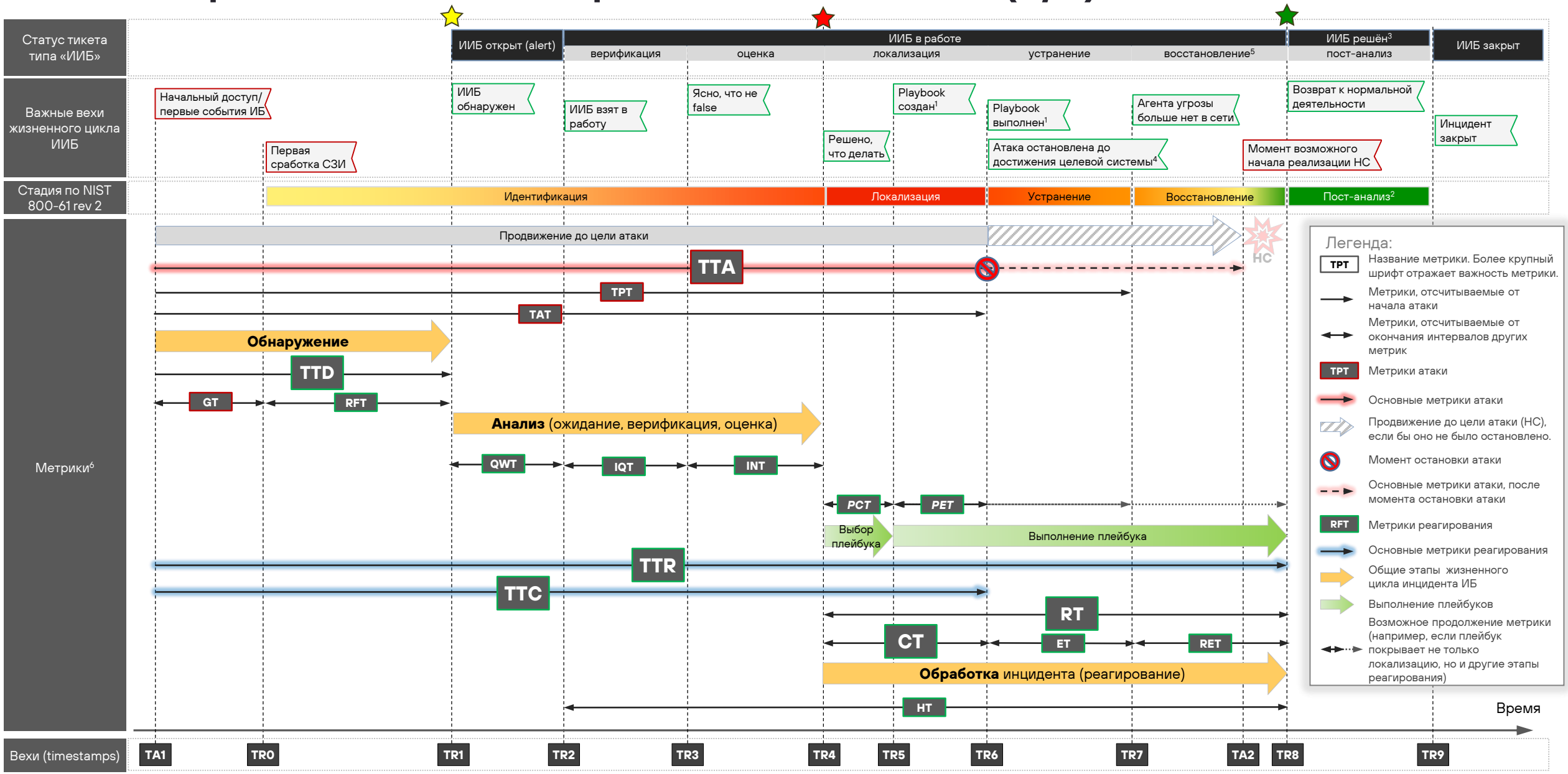
Метрики реагирования

Метрика	Начало	Конец	Формула	Определение	Примечание
TTR	Первоначальный доступ атакующего в ИТ-инфраструктуру	Окончание восстановления после инцидента	**TR8-TA1**	Time To Respond, время до завершения реагирования.	Агент угрозы более не присутствует в ИТ-инфраструктуре, восстановление завершено.
TTC	Первоначальный доступ атакующего в ИТ-инфраструктуру	Окончание локализации угрозы	**TR6-TA1**	Time To Contain, время до окончания локализации угрозы.	Агент угрозы изолирован и более не может продвигаться в ИТ-инфраструктуре.
RFT	Первичная сработка СЗИ (первые события)	Сработка правила корреляции (алерт)	**TR1-TR0**	Rule Fire Time, время сработки правила. От первых событий, обработанных правилом, до его сработки (выдачи алерта, подозрения на инцидент).	Зависит от множества параметров, в частности – от use case.
QWT	Появление заявки (ticket) в очереди	Назначение заявки на исполнителя	**TR2-TR1**	Queue Wait Time, время ожидания в очереди.	Используется для определения численности персонала.
HT	Назначение заявки на исполнителя	Окончание восстановления после инцидента	**TR8-TR2**	Handle Time Время, которое инцидент находится в руках команды реагирования.	Используется для определения численности персонала.
IQT	Назначение заявки на исполнителя	Окончание верификации инцидента	**TR3-TR2**	Incident Qualification Time, время верификации - время определения легитимности активности (исключение ложноположительного срабатывания).	
INT	Окончание верификации инцидента	Окончание оценки инцидента	**TR4-TR3**	Incident iNvestigation Time, время оценки – сбор информации об инциденте, его масштабе, приоритете и иной информации, принятие решения о реагировании.	Необходимо для принятия решения о дальнейшем реагировании.
RT	Окончание оценки инцидента	Окончание восстановления после инцидента	**TR7-TR6**	Response Time, время реагирования – время от начала локализации до окончания восстановления (перевода инцидента в статус «Решён»).	Отрезок времени, включающий локализацию, устранение угрозы и восстановление. Может быть использован как часть метрики RTO (Reovery Time Objective, целевое вреям восстановления) для системы, сервиса, приложения или бизнес-процесса.
CT	Окончание оценки инцидента	Окончание локализации угрозы	**TR6-TR4**	Containment Time, время локализации (угрозы) – время, затрачиваемое на изоляцию агента угрозы в ИТ-инфраструктуре и блокирование его дальнейшего продвижения.	Наряду с TTR используется для сравнения с TTA
ET	Окончание локализации угрозы	Окончание устранения присутствия атакующего в ИТ-инфраструктуре	**TR7-TR6**	Eradication Time, время устранения (угрозы) – время, затрачиваемое на устранение присутствия атакующего (агента угрозы) в ИТ-инфраструктуре.	В зависимости от типа ущерба (C/I/A) может иметь существенно разную длительность. Исходя из этого соображения для сравнения с TTA может использоваться не TTR, а TTC.
RET	Окончание устранения присутствия атакующего в ИТ-инфраструктуре		**TR8-TR7**	REcovery Time (time from the end of threat eradication till the end of recovery, i.e. when the condition of the affected IT Infrastructure is back to where it was before the attack)	ibid

Метрики выполнения плейбуков

Метрика	Начало	Конец	Формула	Определение	Примечание
PCT	Окончание оценки инцидента	Плейбук создан (выбран)	**TR5-TR4**	Playbook Creation Time, время выбора/создания плейбука – время, затрачиваемое аналитиками SOC для выбора готового или сборки/создания плейбука (из готовых модулей или с нуля).	
PET	Плейбук создан (выбран)	Плейбук выполнен	**TR6-TR5**	Playbook Execution Time, время выполнения плейбука – время, затрачиваемое аналитиками и/или автоматизирвоанными системами на выполненеи выбранного плейбука.	Может заканчиваться на локализации, устранении или восстановлении угрозы.

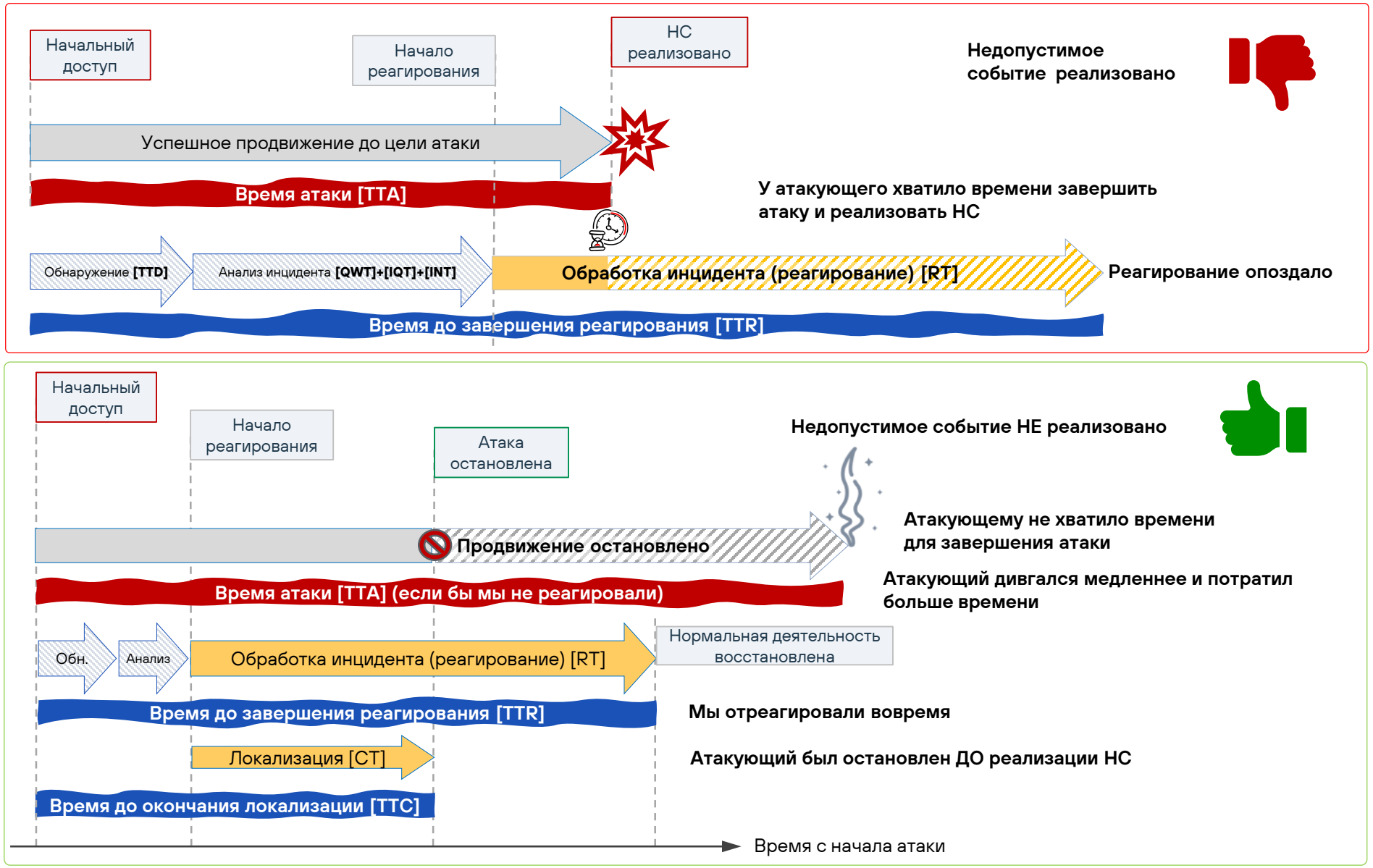
02.06. Прочие важные метрики инцидента ИБ (2/2)



Примечания:

1. Автоматическое реагирование. При ручном реагировании, плейбук может собираться как последовательность уже существующих типовых модулей (элементов) других плейбуков.
2. Пост-анализ применяется к новым инцидентам, известные типы можно пропускать.
3. Статус «Решён» может автоматически стать «Закрыт» при отсутствии замечаний через определённое время.
4. Плейбук может завершаться на этапе устранения или восстановления, не обязательно на локализации.
5. Восстановление бизнес-операций включает больше, чем просто восстановление ИТ-инфраструктуры. (Метрика может быть добавлена в следующем обновлении)
6. Взаимный масштаб метрик может не отражать реальность, продолжительность временных отрезков выбрана только для иллюстрации их расположения.

02.07. Когда случится и не случится НС?



В общем случае НС происходит тогда, когда атакующий успевает достичь цели ДО того, как защитники успевают отреагировать

Даже интуитивно понятно: чтобы НС не произошло, нужно успеть отреагировать ДО того, как атакующий достигнет цели

Таким образом, задача своевременного реагирования может быть выражена как **удлинение времени атаки и/или сокращение времени реагирования и как можно более ранее начало реагирования**

Это можно выразить следующим образом:

TTR < TTA
TTC << TTA

TTC = TTD+QWT+IQT+INT+CT
"<<" значит «значительно, заметно меньше»

Пообсуждаем?
Посчитаем?