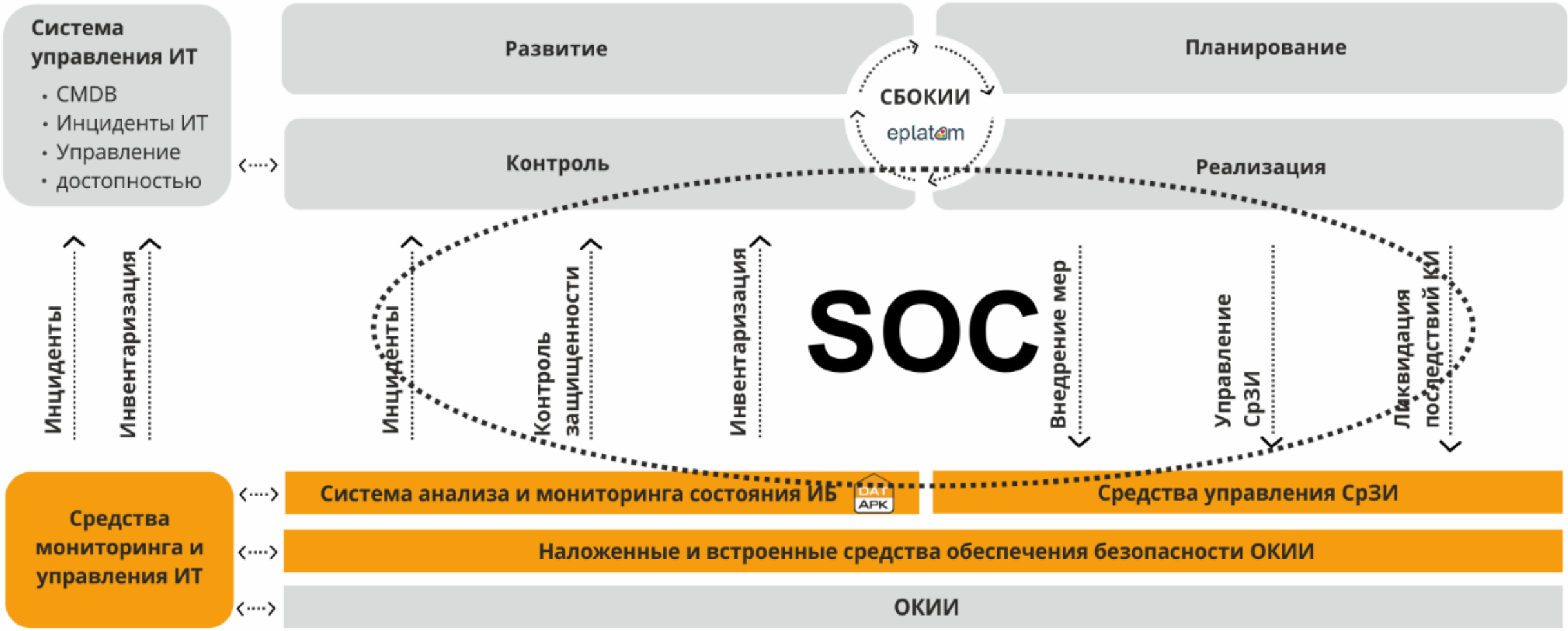
Центр обеспечения безопасности:

как не утонуть в потоке событий ИБ?

Николай Домуховский
Заместитель генерального директора ООО «УЦСБ»

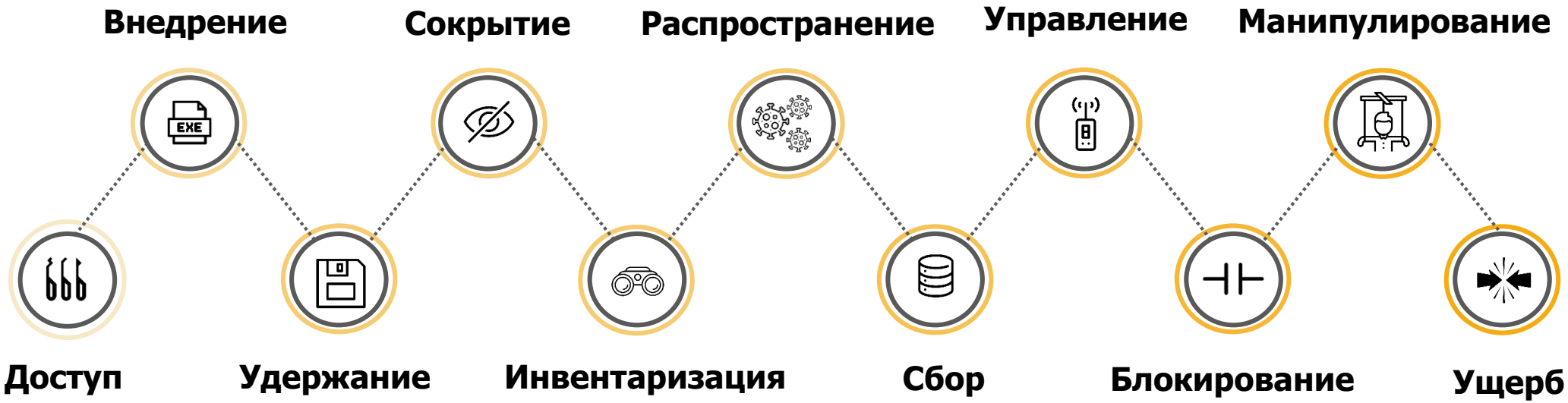
Гладко было на бумаге...



… да забыли про овраги

Взгляд со стороны Заказчика:

С чем сталкивается SOC в реальном мире?



Жизненный цикл инцидента ИБ в соответствии с MITRE ATT&CK® for Industrial Control Systems

77% Компаний подвергаются успешной атаке в течение одного года

77% На столько уменьшиться ущерб, если инцидент будет выявлен в течение недели

10k Оповещений получают более половины корпоративных центров управления безопасностью каждый день

101 День в среднем уходит на обнаружение инцидента

96% На столько уменьшиться ущерб, если инцидент будет выявлен в течение дня

30 Минут в среднем уходит у аналитика на обработку оповещения

Какой SOC работает хорошо?

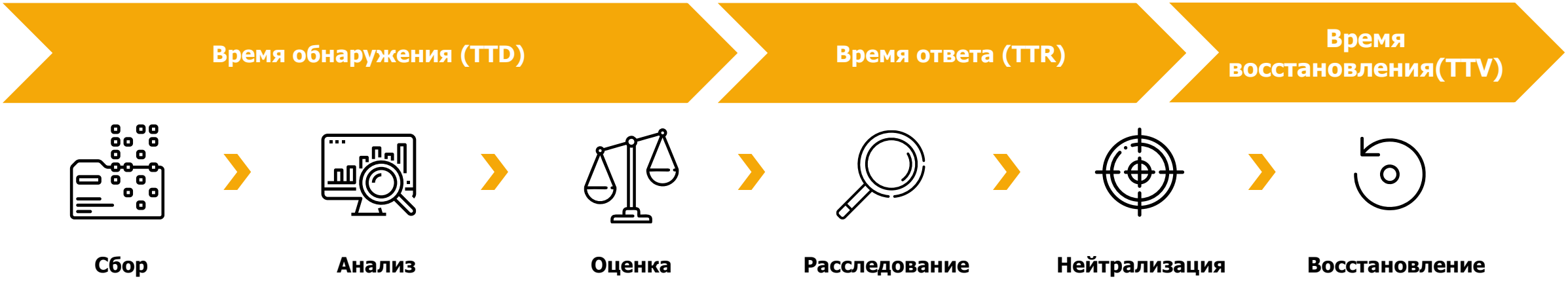
От SOC требуется:

- Обнаружить признак инцидента как можно раньше
- Обработать его как можно быстрее
- Нейтрализовать вредоносное воздействие пока не нанесен ущерб

Какой SOC работает хорошо?

От SOC требуется:

- Обнаружить признак инцидента как можно раньше
- Обработать его как можно быстрее
- Нейтрализовать вредоносное воздействие пока не нанесен ущерб
- … или оперативно устранить последствия нанесения ущерба



Детальные показатели эффективности SOC

Каждая стадия ЖЦ инцидента реализуется собственными средствами и подходами

Стадия ЖЦ инцидента	TTT	TTQ	TTI	TTM	TTV	TTD	TTR
Сбор признаков (событий)							
Обнаружение							
Квалификация							
Расследование							
Нейтрализация							
Восстановление							

Дополнительные метрики позволяют выявить узкое место для адресной работы с ним.

SOC субъекта КИИ – дополнительные требования

2. Субъекты критической информационной инфраструктуры обязаны:

1) незамедлительно информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации…

Ст. 9 Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

2. Основными задачами системы безопасности значимого объекта критической информационной инфраструктуры являются:

…

4) непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Ст. 9 Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Итоговый план создания SOC

Внедрение средств сбора → Внедрение средств анализа → Найм и обучение персонала → Подключение к ГосСОПКА → Оптимизация процессов SOC

Итоговый план создания SOC

Внедрение средств сбора → Внедрение средств анализа → Найм и обучение персонала → Подключение к ГосСОПКА → Оптимизация процессов SOC

Либо…

Приобрести услугу SOC

Свой SOC или услуга, что выбрать?

Аутсорсинг SOC

- \+ Быстрый запуск
- \+ Нет необходимости подбора сотрудников в штат
- \+ Есть необходимые лицензии, выстроено взаимодействие с НКЦКИ
- \+ «Перенос» опыта с других объектов, подключенных к SOC
- — Операционные затраты
- — Нет накопления собственной компетенции

Собственный SOC

- \+ Минимизация операционных затрат
- \+ Развитие собственной экспертизы ИБ
- \+ Гибкая адаптация под требования бизнеса
- — Запуск собственного SOC – длительный процесс
- — Сложно найти квалифицированные кадры
- — Высокие капитальные затраты
- — Необходимо получать лицензии ФСТЭК, обеспечивать подключение к ГосСОПКА

SOC УЦСБ – преимущества сотрудничества

УЦСБ – системный интегратор в области ИБ

- опыт работы со множеством средств и систем обеспечения ИБ
- наличие собственного оборудования и ПО, которое может быть передано в аренду для «быстрого старта» SOC
- комплексный подход к обеспечению ИБ – от аудита и проектирования до внедрения и сопровождения

Экспертиза в ИБ АСУ ТП

- реализовано более 1000 проектов в области ИБ АСУ ТП
- выделенное подразделение по кибербезопасности промышленных систем
- наличие собственных стендов АСУ ТП
- опыт взаимодействия с производителями АСУ ТП

Дополнительные услуги в области ИБ

- проведение аудитов, оценки соответствия систем защиты с использованием сведений накопленных SOC
- расследование и устранение последствий критичных инцидентов ИБ
- Проведение тестирований на проникновение для повышения защищенности систем Заказчика

Корпоративный центр ГосСОПКА (SOC) на базе УЦСБ

ГосСОПКА за

3 месяца

Запуск базовых функций корпоративного центра ГосСОПКА менее чем за 3 месяца

8x5

с 9:30 до 18:30 в рабочие дни

10x5

с 8:00 до 19:00 в рабочие дни

24x7

круглосуточно

Время обслуживания
Определяется регламентом предоставления услуги

Время реагирования на инцидент

<60 мин

USSC

СПАСИБО ЗА ВНИМАНИЕ

ВОПРОСЫ?

Николай Домуховский

Заместитель генерального
директора ООО «УЦСБ»

ndomukhovsky@ussc.ru

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU