R-Vision

Этапы построения SOC на базе R-Vision

Шоленберг Ольга Алексеевна

Руководитель группы пресейл

О чем поговорим

01 Кому нужен?

02 Какие бывают?

03 Этапы развития

SOC

01

Кому нужен SOC

Ключевые пользователи центров

Корпоративный SOC

Сам себе бригадир и подрядчик

Собственная экспертиза

Вся критическая информация в периметре

Необходима команда аналитиков

Затратно по ресурсам

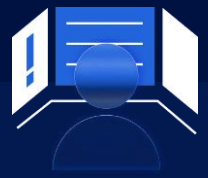
Коммерческий SOC

Доверие превыше всего

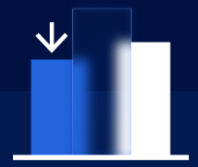
Готовая экспертиза

Ответственность в рамках SLA

Облачные решения



Доступная инфраструктура извне



Нет развития собственной экспертизы

Гибридный SOC

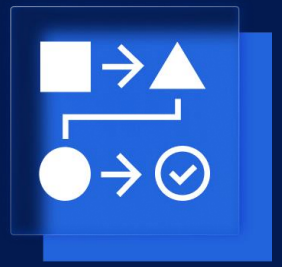
Баланс или переплата?

✓ Решаем проблему кадров	✗ Потребность в команде аналитиков
✓ Пользуемся экспертизой MSSP	✗ Двойная стоимость
✓ Наращиваем свою экспертизу	✗ Доступ к инфраструктуре извне
✓ Контроль и прозрачность	✗ Зависимость от сторонних организаций

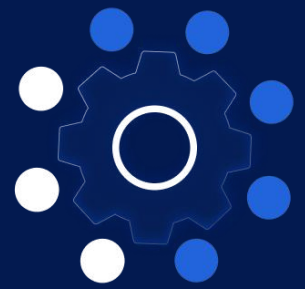
Эффективный SOC

Три компонента любого центра

Люди



Процессы



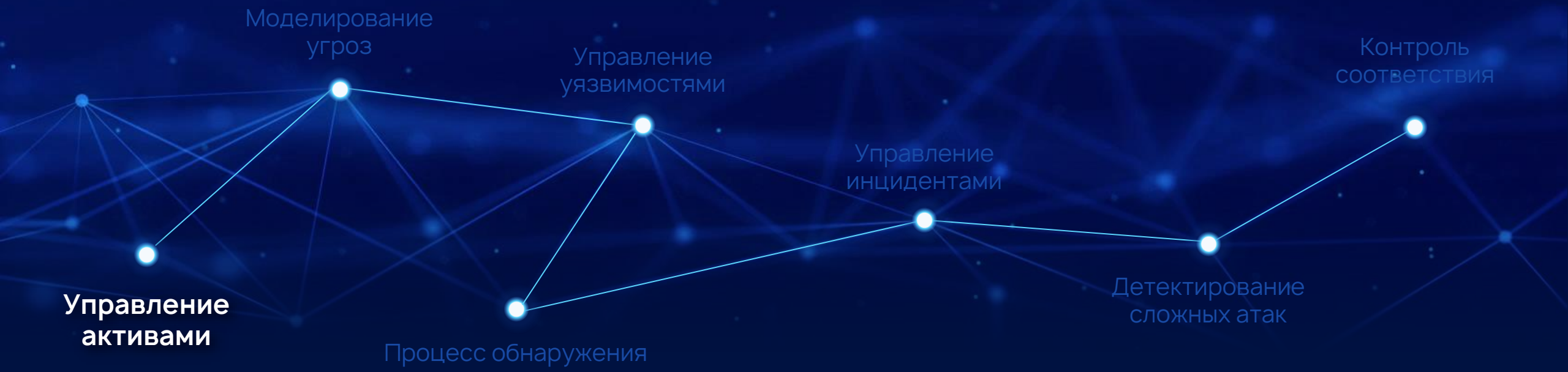
Технологии

Этапы строительства SOC

Через тернии к SOC

Управление активами

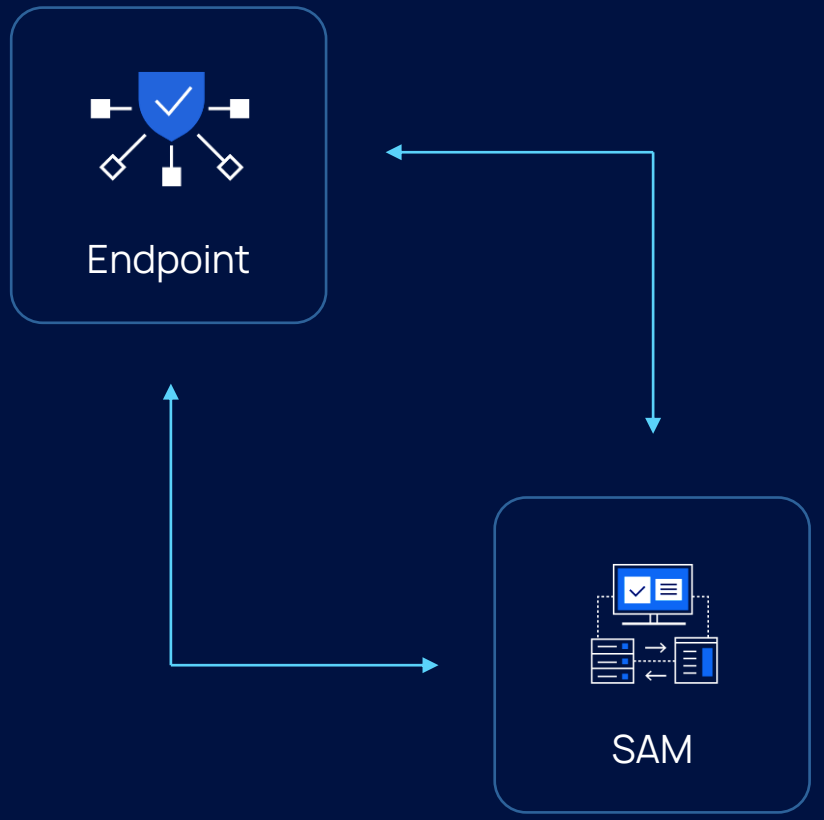
Этапы строительства SOC: 1/7



Управление активами

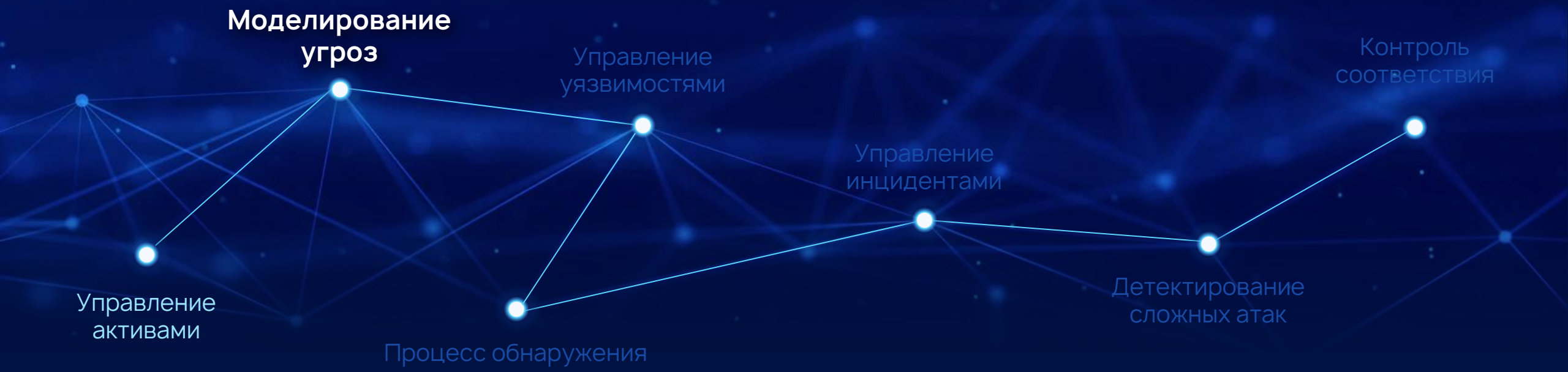
Знать, что защищать

- Инвентаризация и сбор данных с IT-систем
- Формирование модели активов
- Мониторинг активов



Моделирование угроз

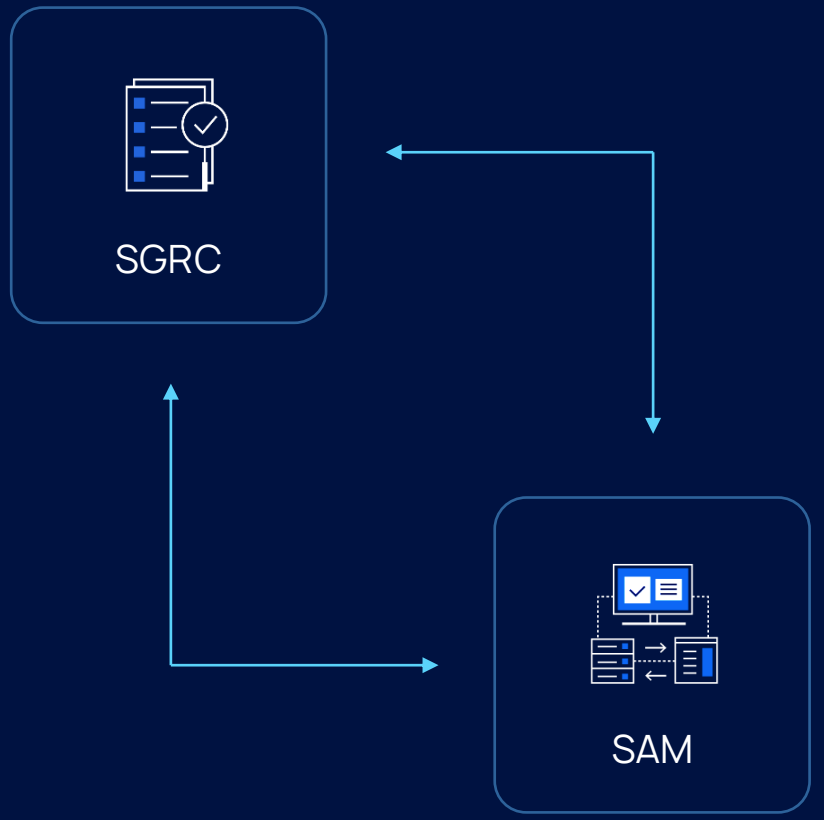
Этапы строительства SOC: 2/7



Моделирование угроз

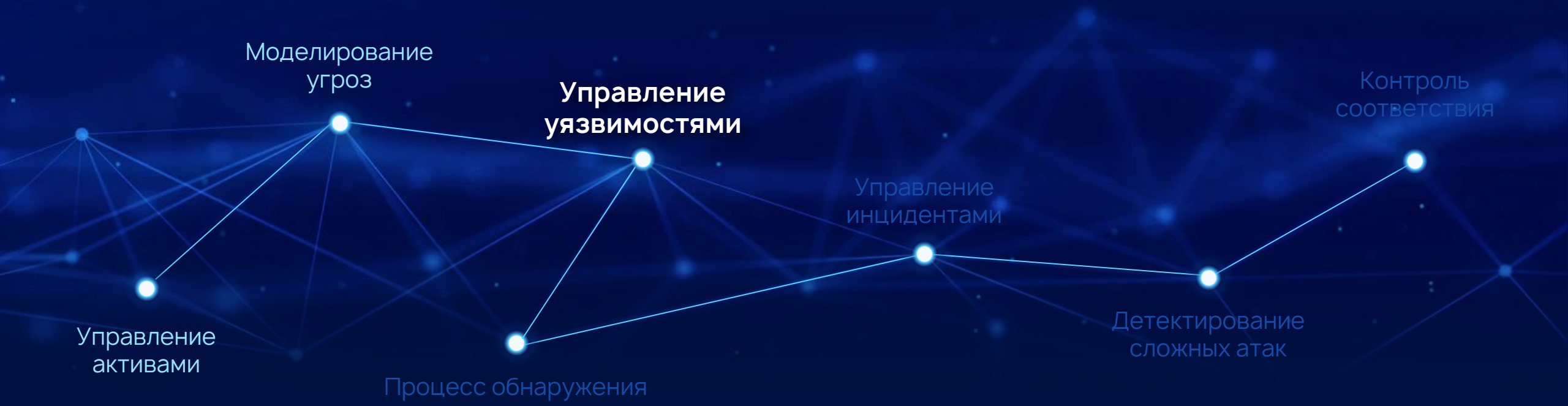
Знать, от чего защищать

- Моделирование угроз для компании
- Оценка рисков для ключевых бизнес процессов
- Оценка текущего состояния защиты и выбор мер защиты



Управление уязвимостями

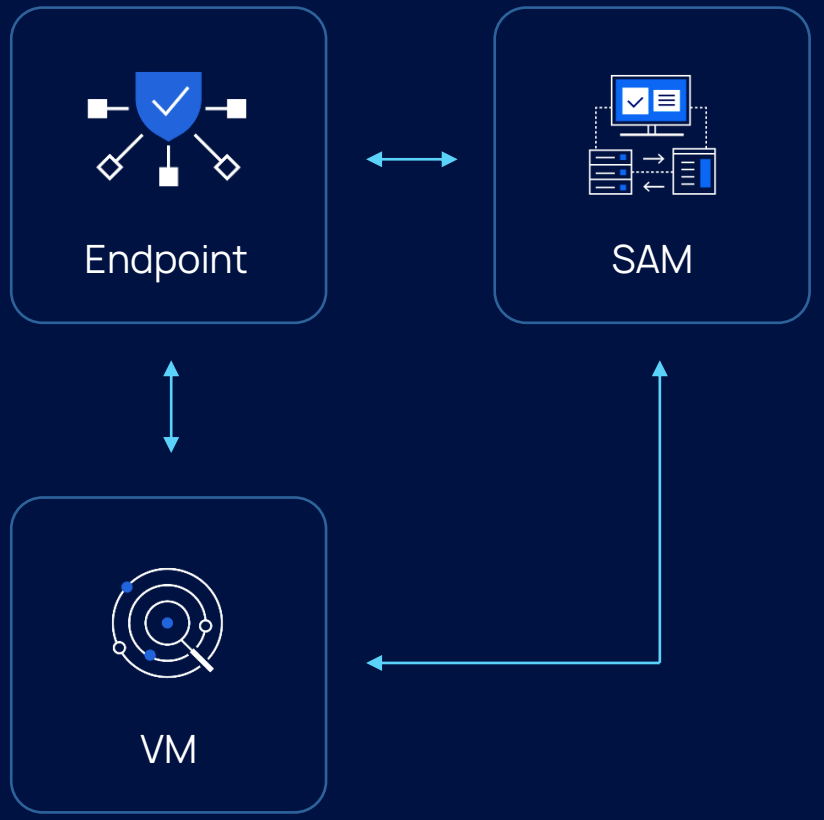
Этапы строительства SOC: 3/7



Управление уязвимостями

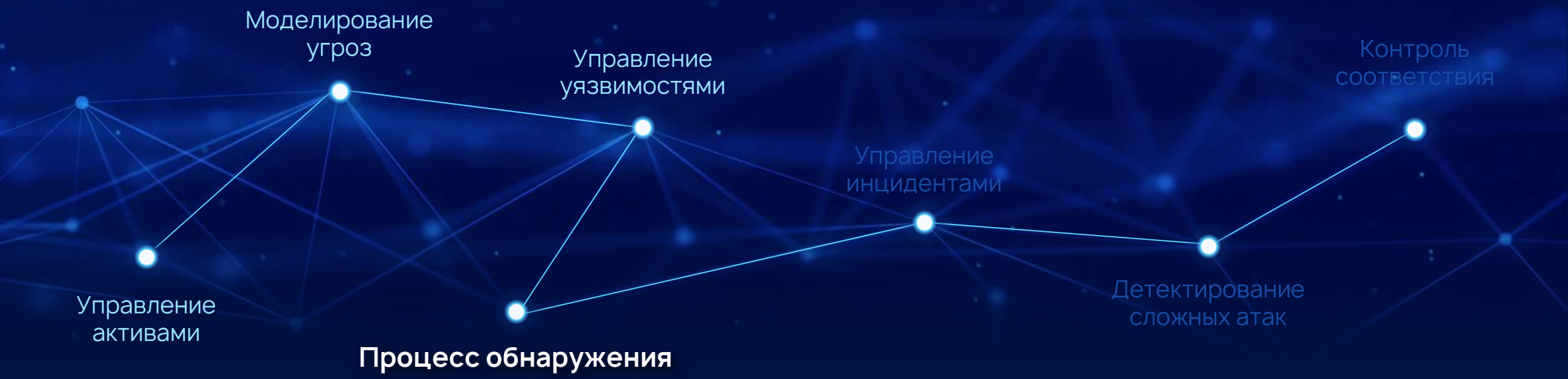
Больше, чем сканирование

- Сканирование устройств на наличие уязвимостей
- Приоритизация уязвимостей
- Формирование задач по устранению



Процесс обнаружения

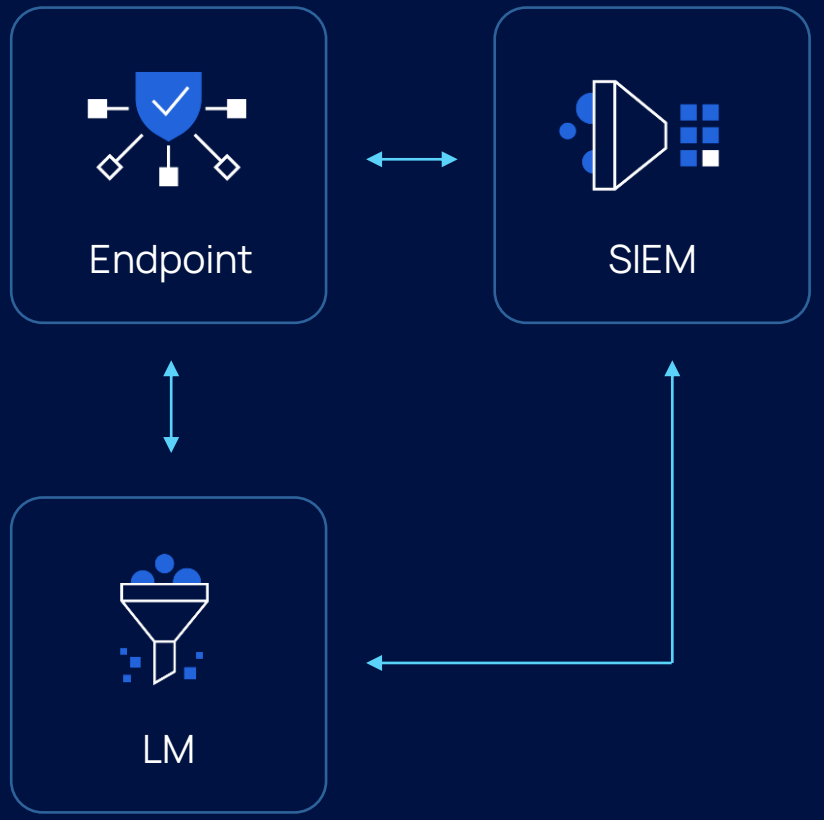
Этапы строительства SOC: 4/7



Процесс обнаружения

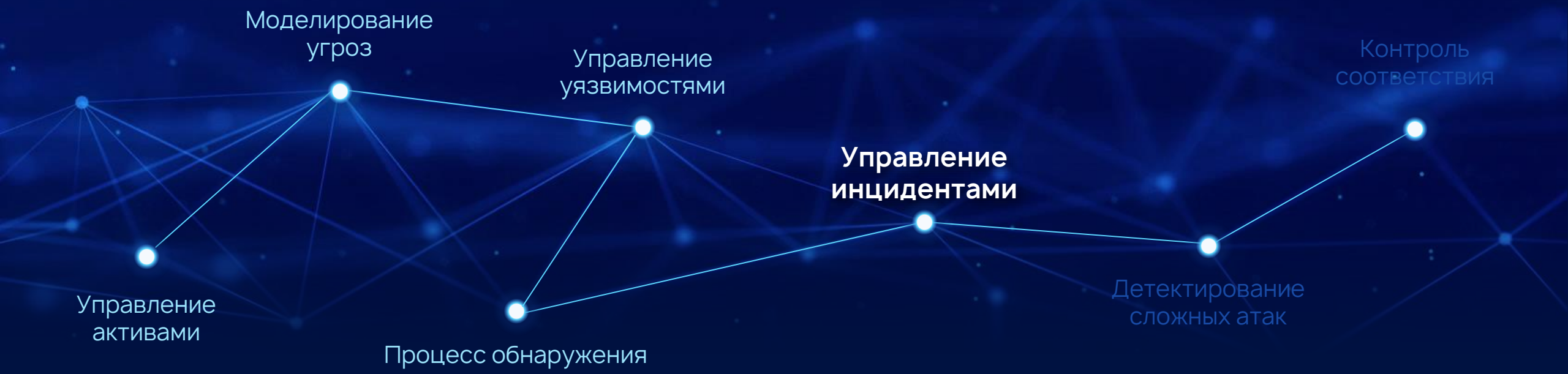
Полный контроль инфраструктуры

- **Централизованный сбор и хранение событий**
- **Создание корреляционных правил**
- **Обнаружение инцидентов**



Управление инцидентами

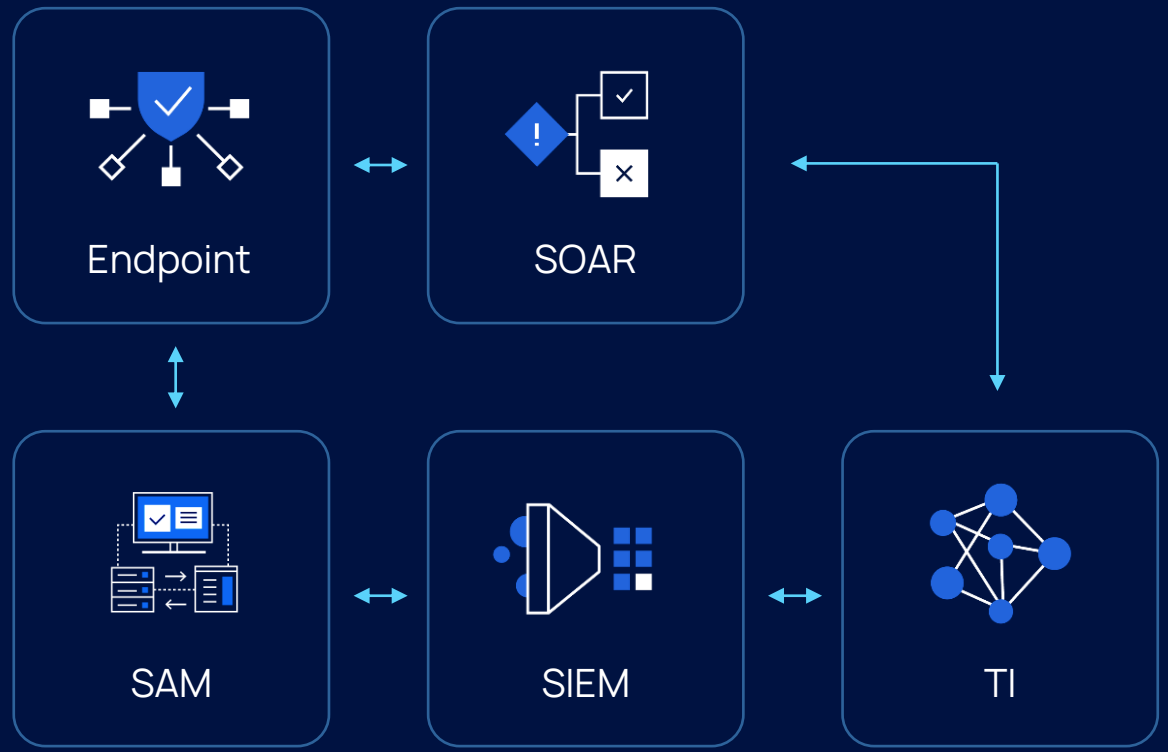
Этапы строительства SOC: 5/7



Управление инцидентами

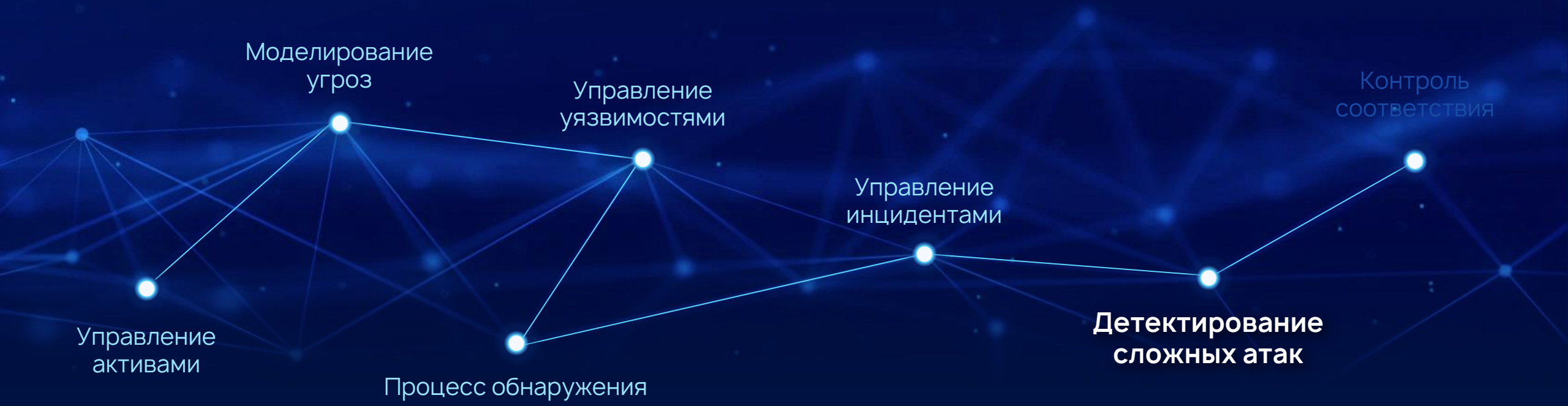
Автоматизации много не бывает

- **Автоматизация действий аналитика, инструменты для совместной работы**
- **Оркестрация СЗИ**
- **Работа с TI**



Детектирование сложных атак

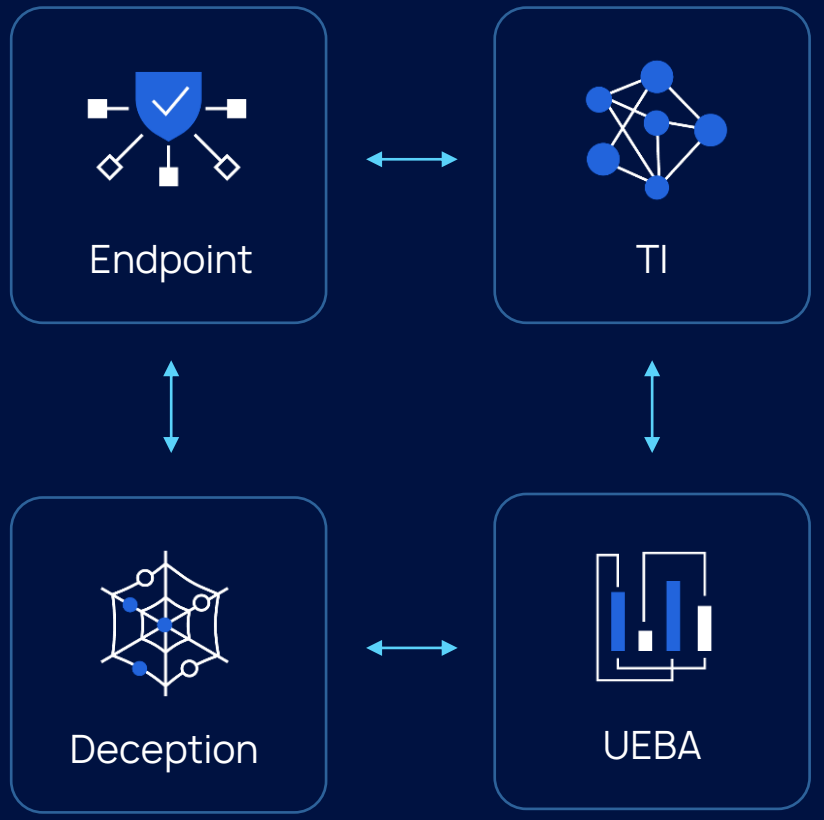
Этапы строительства SOC: 6/7



Детектирование сложных атак

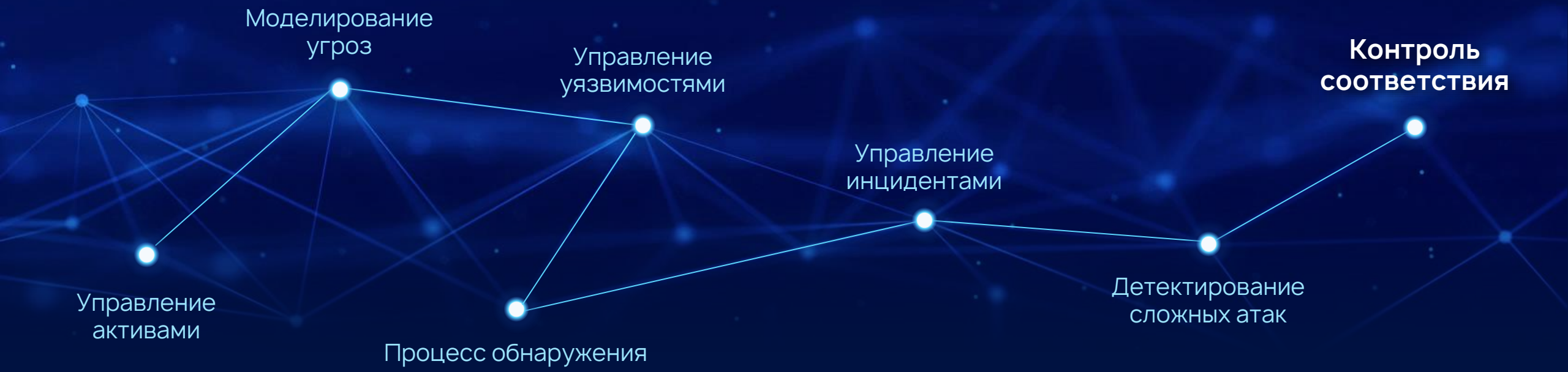
Когда нужно больше, чем базовая защита

- Раннее обнаружение APT и 0-day атак
- Инструменты машинного обучения
- Снижение скорости распространения и работа с TI



Процесс аудита

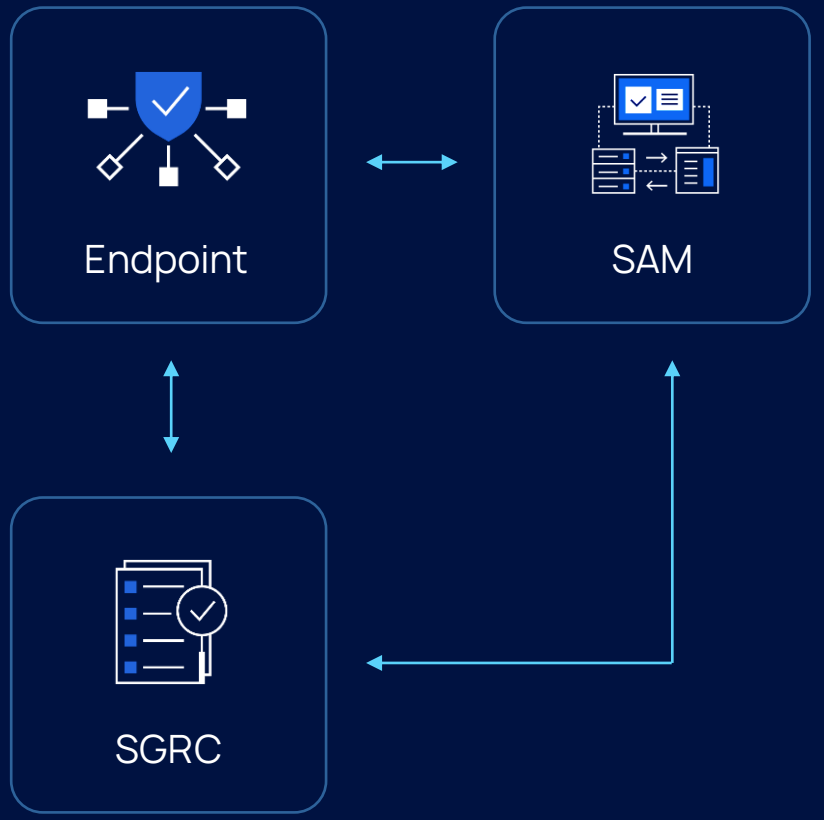
Этапы строительства SOC: 7/7



Процесс аудита

Важная бумажная безопасность

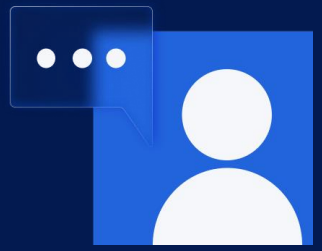
- Аудит организационных мер защиты
- Аудит технических мер защиты
- Оценка текущего состояния и выбор мер защиты



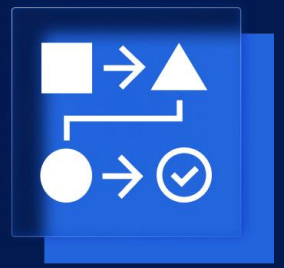
Стратегия R-Vision

Ключевые направления

Развитие комплекса технологий и выстроенных между ними процессов

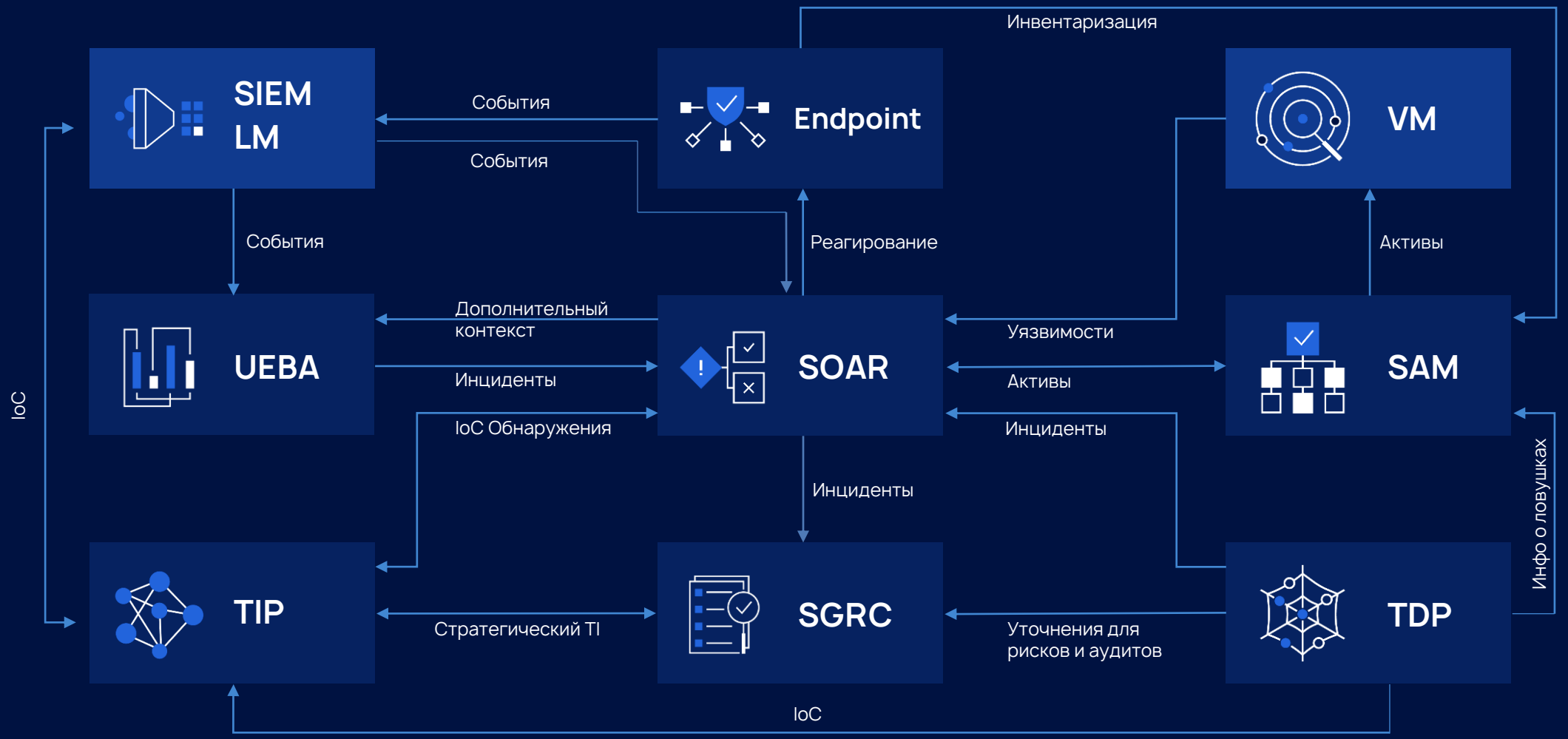


Акцент на задачи клиента



Формирование стратегии развития SOC

Технологии R-Vision



R-Vision

Свяжитесь с нами удобным способом:

+7 (499) 322 80 40

sales@rvision.ru

Читайте наш Дайджест ИБ:

rvision.ru/blog

t.me/rvision_pro

vk.com/rvision_ru

rvision.ru