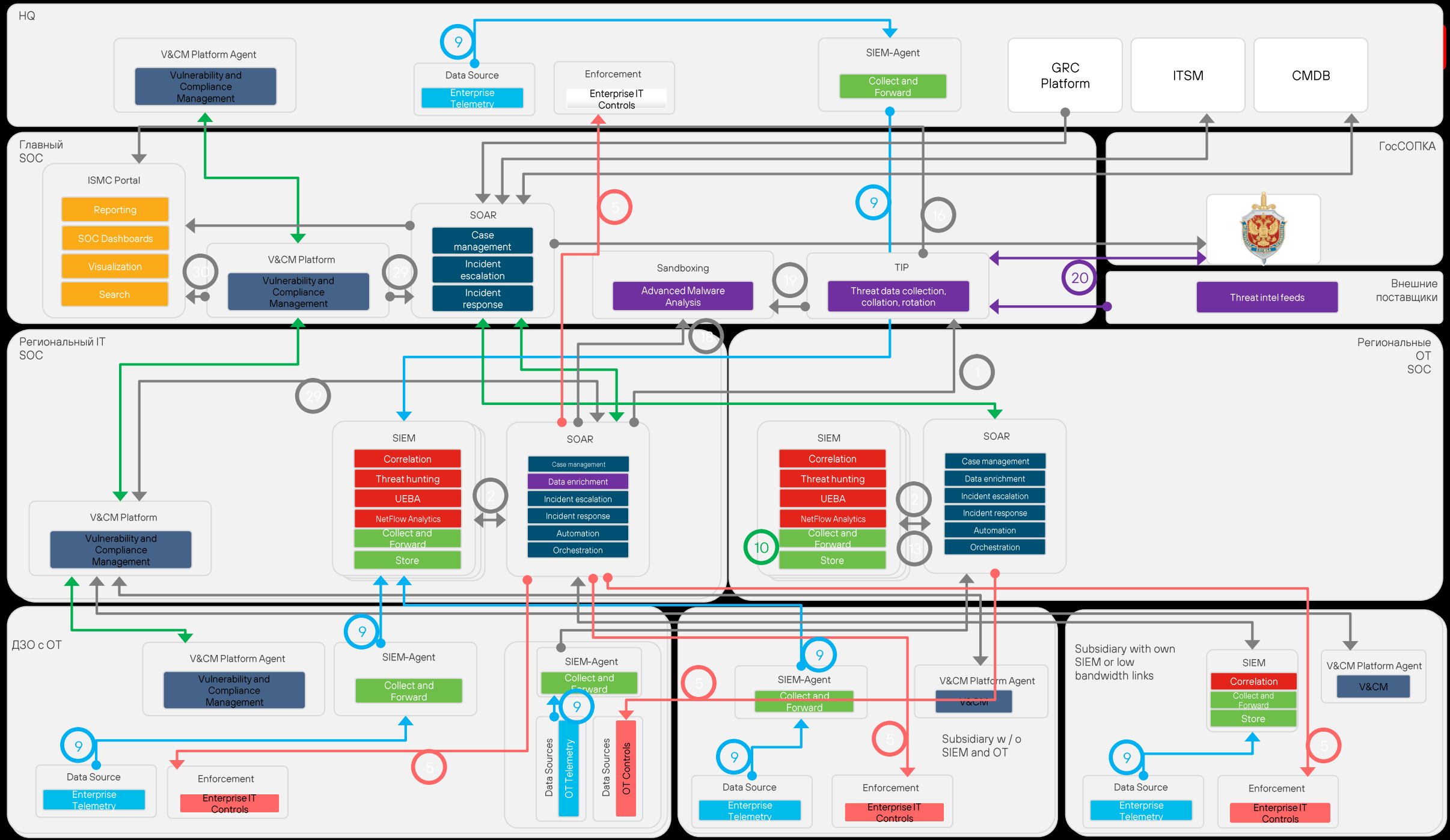
Алексей Лукацкий
Бизнес-консультант по безопасности

От чего зависит выбор технологий для SOC?

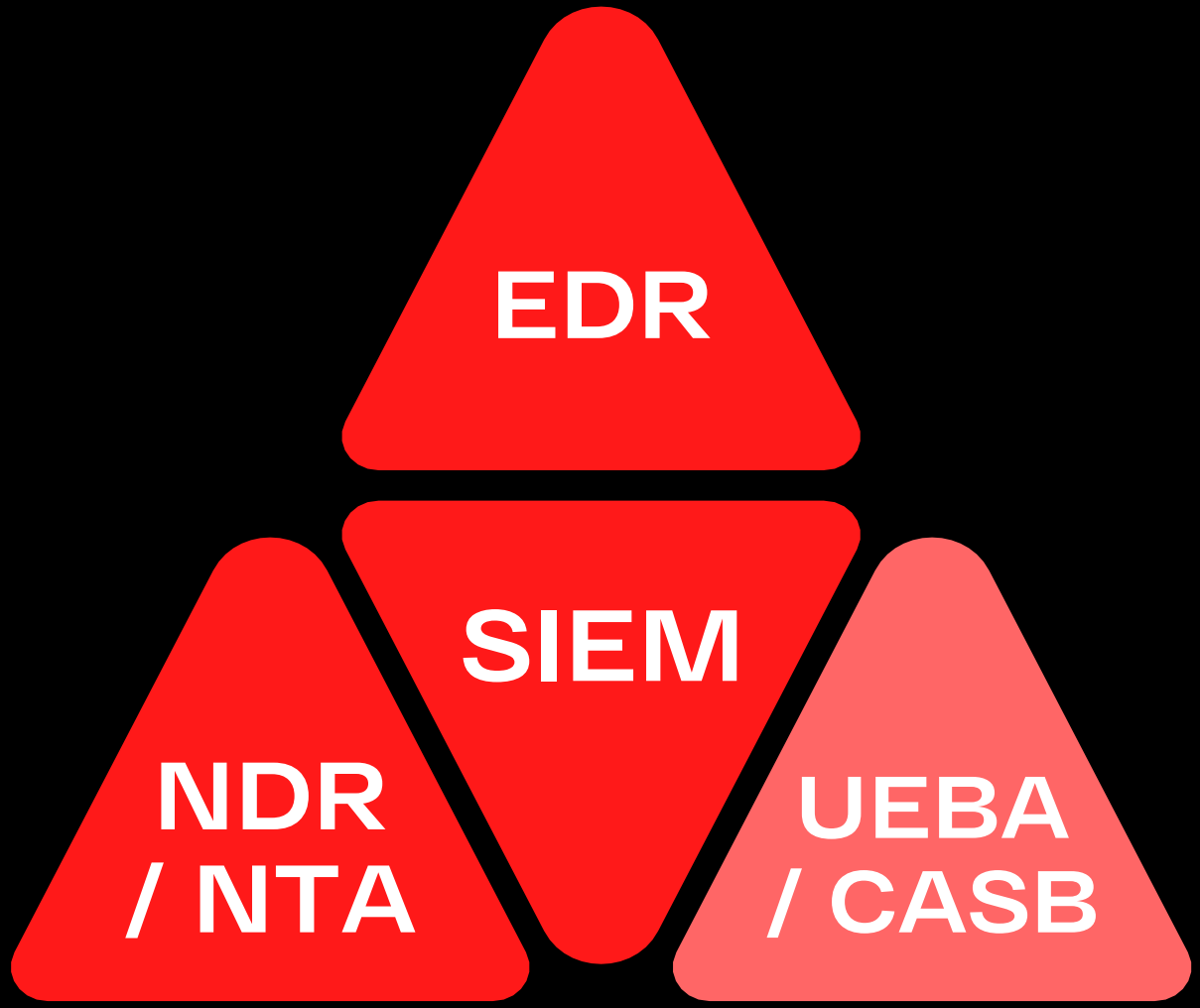
Составляем чеклист на основе участия в паре десятков проектов проектирования и аудитов SOC

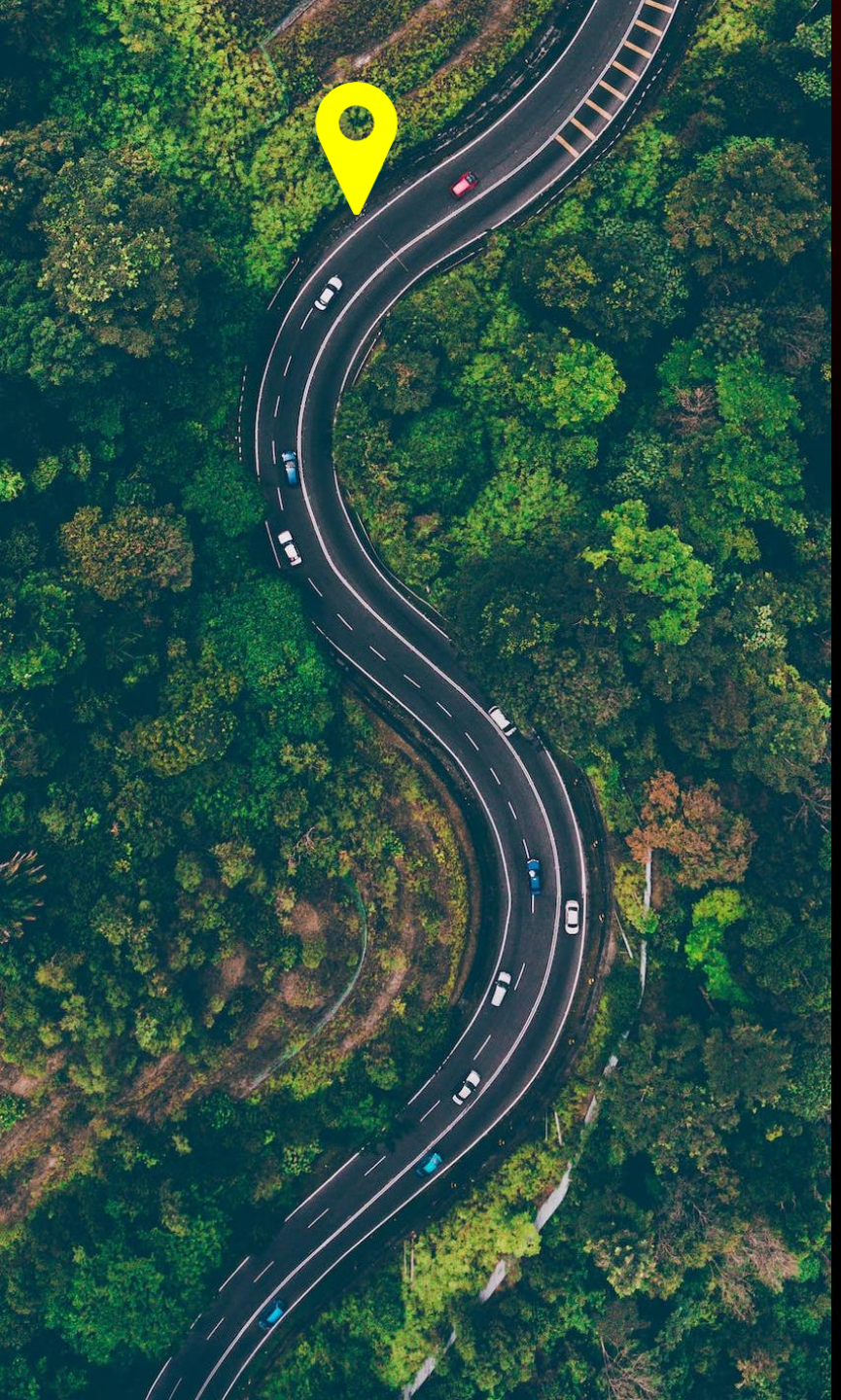
Who am I?

- Бизнес-консультант по безопасности в Positive Technologies
- Первый SOC строил в 1999-м в Украине
- Проектировал и аудировал SOCи в финансовом, энергетическом, нефтяном, телекоммуникационном, ИТ, государственном секторах, а также для спецслужб - в России, странах СНГ и Восточной Европы
- Участвовал в построении государственных CDC в странах СНГ


HQ
V&CM Platform Agent
Vulnerability and Compliance Management
Data Source
Enterprise Telemetry
Enforcement
Enterprise IT Controls
SIEM-Agent
Collect and Forward
GRC Platform
ITSM
CMDB
Главный SOC
ISMC Portal
Reporting
SOC Dashboards
Visualization
Search
V&CM Platform
Vulnerability and Compliance Management
SOAR
Case management
Incident escalation
Incident response
Sandboxing
Advanced Malware Analysis
TIP
Threat data collection, collation, rotation
ГосСОПКА
Threat intel feeds
Внешние поставщики
Региональный IT SOC
V&CM Platform
Vulnerability and Compliance Management
SIEM
Correlation
Threat hunting
UEBA
NetFlow Analytics
Collect and Forward
Store
SOAR
Case management
Data enrichment
Incident escalation
Incident response
Automation
Orchestration
Региональные OT SOC
SIEM
Correlation
Threat hunting
UEBA
NetFlow Analytics
Collect and Forward
Store
SOAR
Case management
Data enrichment
Incident escalation
Incident response
Automation
Orchestration
ДЗО с OT
V&CM Platform Agent
Vulnerability and Compliance Management
SIEM-Agent
Collect and Forward
Data Source
Enterprise Telemetry
Enforcement
Enterprise IT Controls
SIEM-Agent
Collect and Forward
Data Sources
OT Telemetry
Data Sources
OT Controls
SIEM-Agent
Collect and Forward
V&CM Platform Agent
V&CM
Subsidiary w / o SIEM and OT
Data Source
Enterprise Telemetry
Enforcement
Enterprise IT Controls
Subsidiary with own SIEM or low bandwidth links
SIEM
Correlation
Collect and Forward
Store
V&CM Platform Agent
V&CM
Data Source
Enterprise Telemetry
Enforcement
Enterprise IT Controls

Неувядающая классика?!..





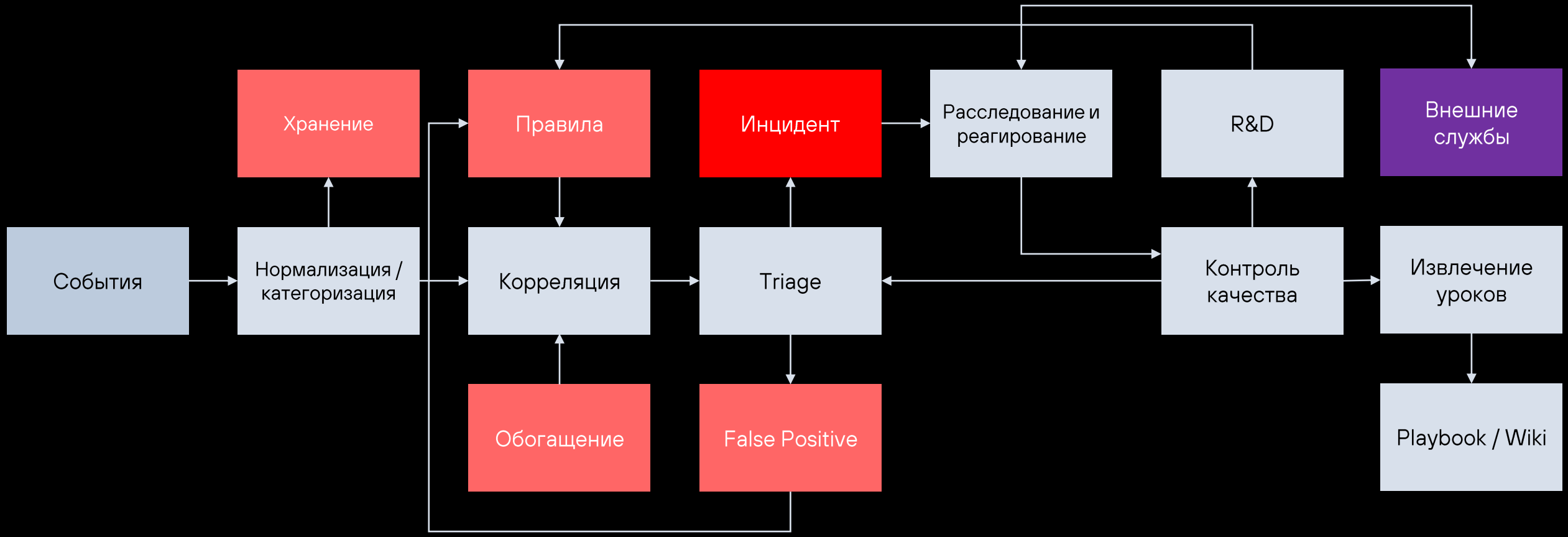
Формируем чеклист

- ❑ SIEM для анализа логов
- ❑ NDR/NTA для анализа трафика
- ❑ EDR для анализа событий на ПК

- ❑ CASB для анализа в облаках
- ❑ Обманные системы
- ❑ Анализ DNS / IP / AS
- ❑ XDR

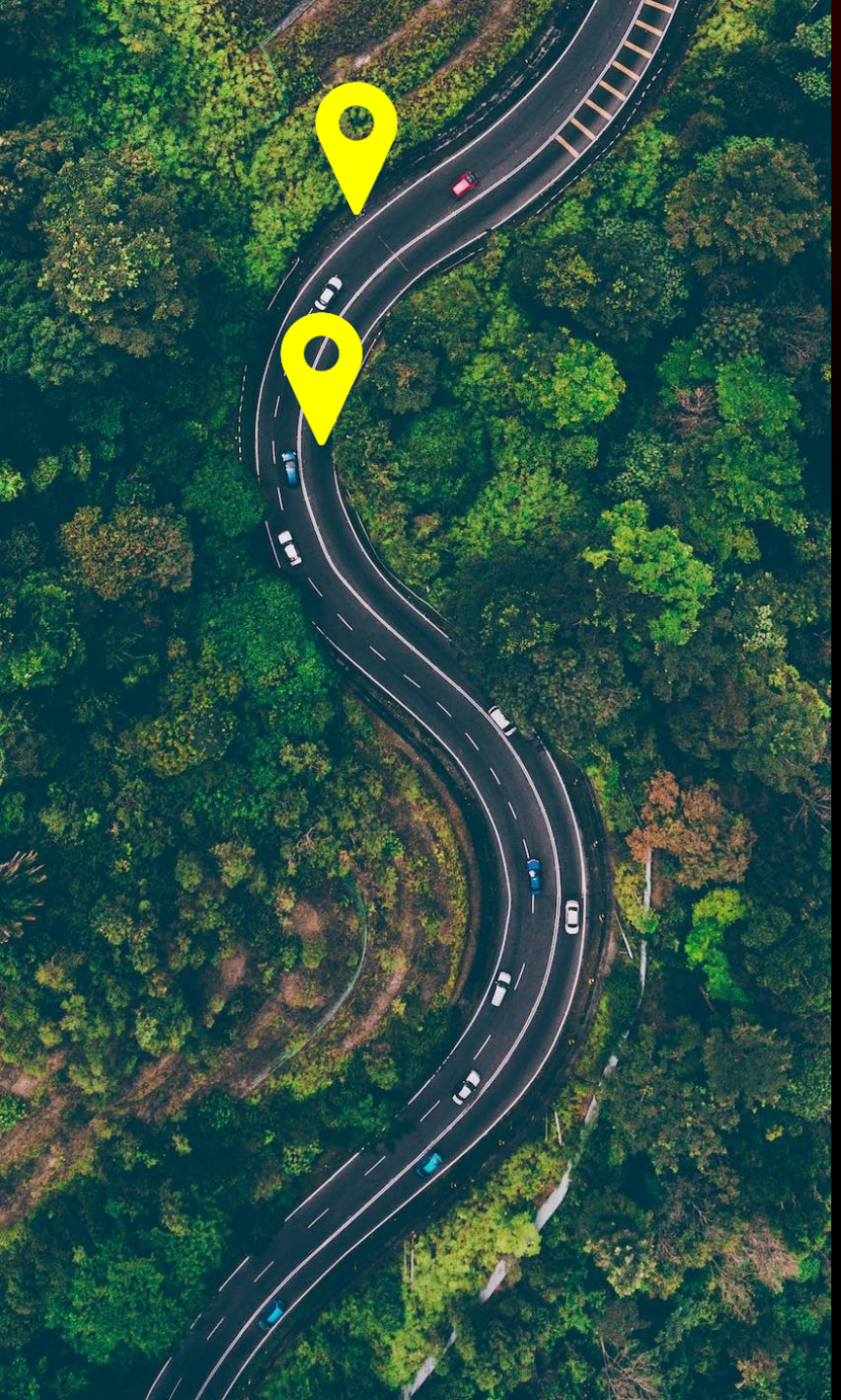
Не только обнаружение

Жизненный цикл Security Operations



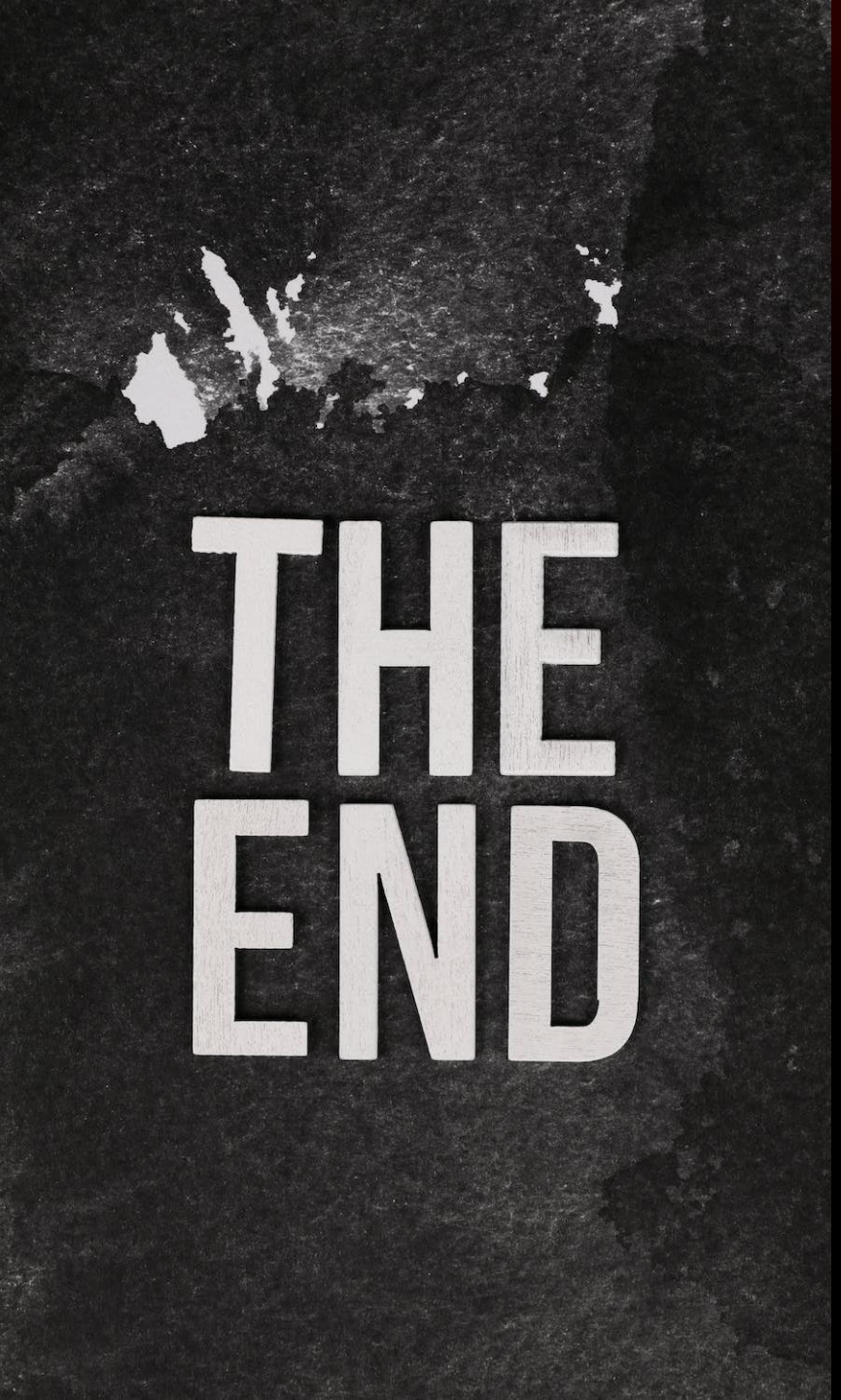
Security Operations объединяет множество решений в единый комплекс!

платных и бесплатных



Формируем чеклист

- TIP для обогащения данных
- IRP/SOAR для управления инцидентами
- Wiki для управления знаниями
- Коммуникации и групповая работа
- Хранилище данных



Можно ли на этом поставить точку?

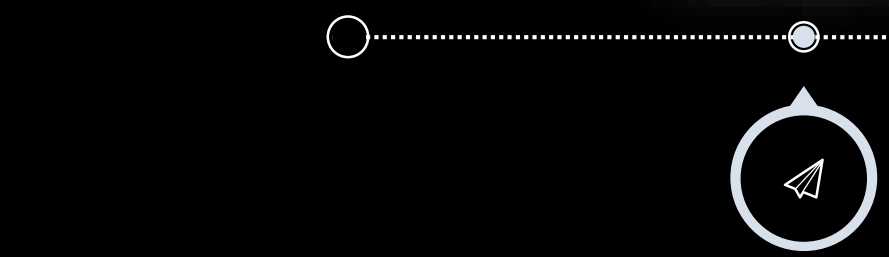
Знание классов технологий еще не является их выбором!

Методология проектирования SOC

Триггеры

Миссия SOC
Стратегия SOC
Сервисы SOC

Понимание целей SOC



Оценка возможностей

Анализ ключевых точек

Стратегия & Управление
Архитектура & Технологии
Процессы и процедуры
Люди & организация
Сервисы SOC

Стратегия & управление

Операционная модель SOC
Финансовая модель SOC
Программа управления SOC
Текущая дорожная карта SOC

Стратегия & управление

Люди & организация

Оргструктура
Роли & ответственность
Персонал SOC

Люди

Технологии

Архитектура & технология

Платформы SOC
Телеметрия SOC
Метрики & отчетность

Процессы

Процессы & процедуры

Ключевые процессы SOC
SOC Playbooks
Интеграция процессов

Сервисы SOC

Мониторинг & реагирование на инциденты
Управление сервисами
Threat Intelligence
...

Сервисы SOC

Зрелость возможностей

На базе CMMI

Анализ & зрелость

SOC Gaps

Разрыв в технологиях
Разрыв в людях
Разрыв в процессах

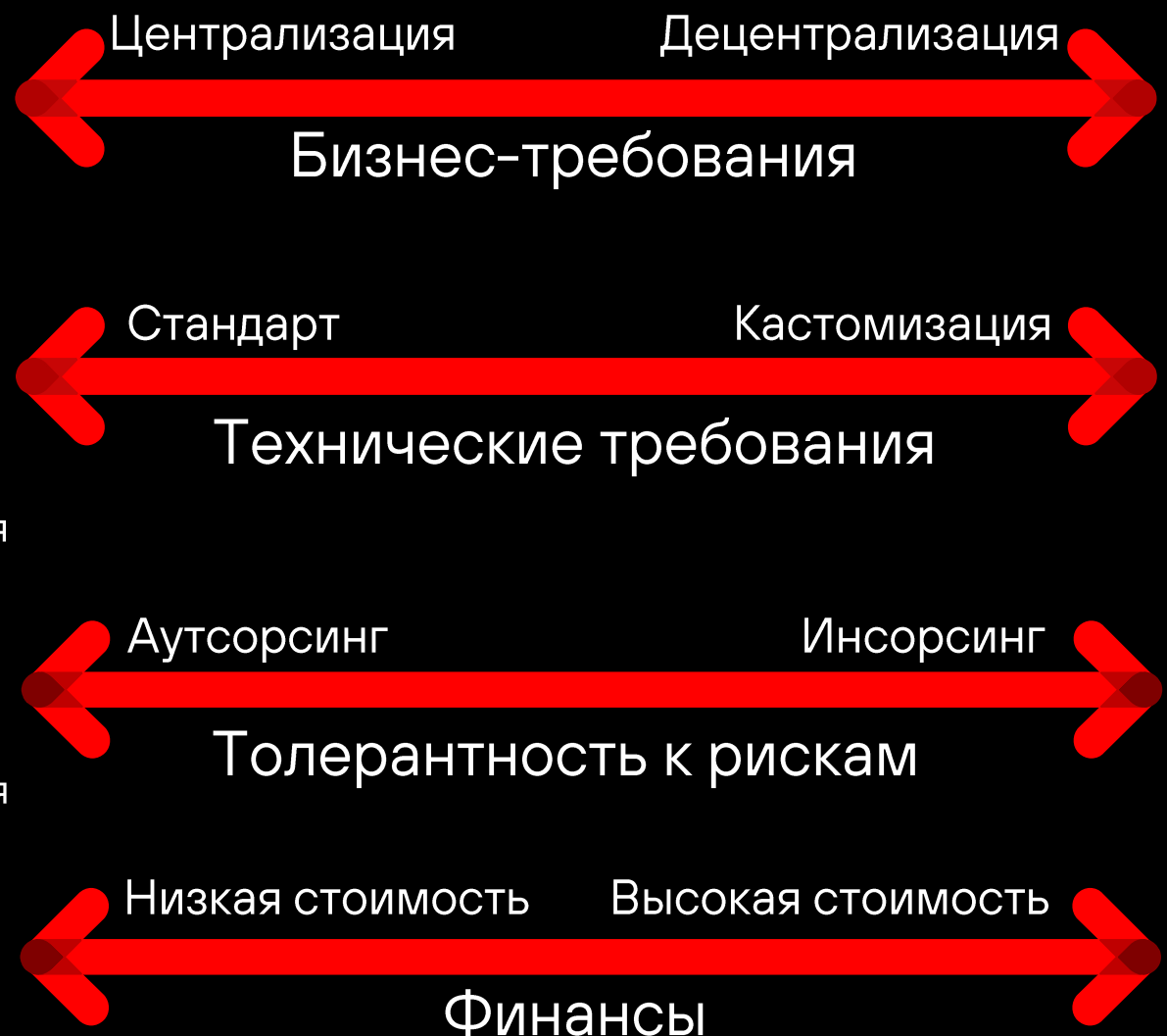
Анализ разрыва

SOC Roadmap & Development Plan

Тактические рекомендации
Стратегические рекомендации

Дорожная карта

Что влияет на технологический стек SOC?



Единый глобальный SOC
Разные центры (SOC/NOC)
Снижение стоимости
Простота управления

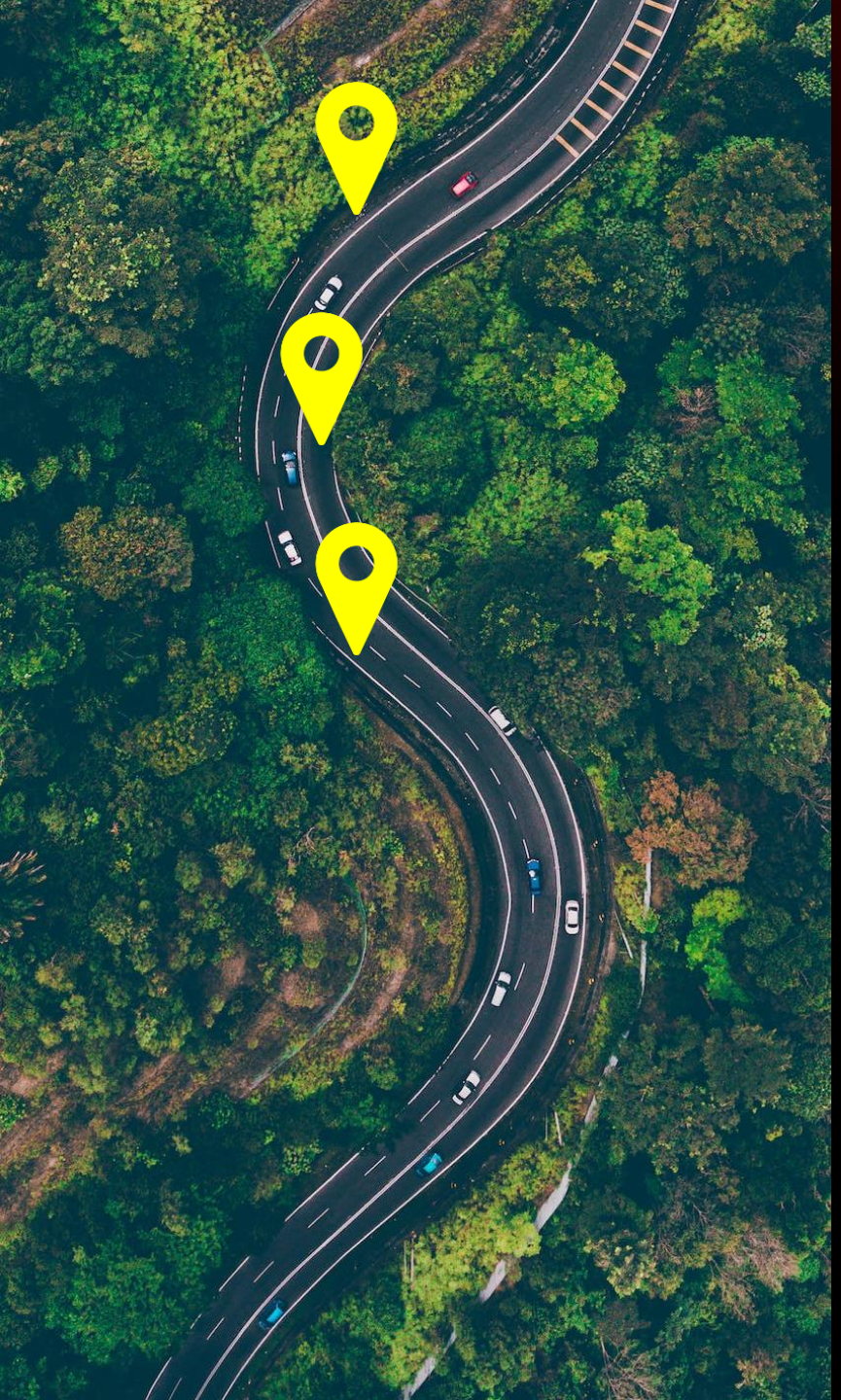
Множество SOCов
Единый центр (SOC/NOC)
Высокая стоимость
Сложность управления

Простая платформа
Простота масштабирования
Средние детали по угрозам
Низкая стоимость внедрения

Комплексная платформа
Сложность масштабирования
Глубокие детали по угрозам
Высокая стоимости внедрения

30-90 дней на внедрение
Некритично для бизнеса
Низкая стоимость внедрения
Внешняя сертификация

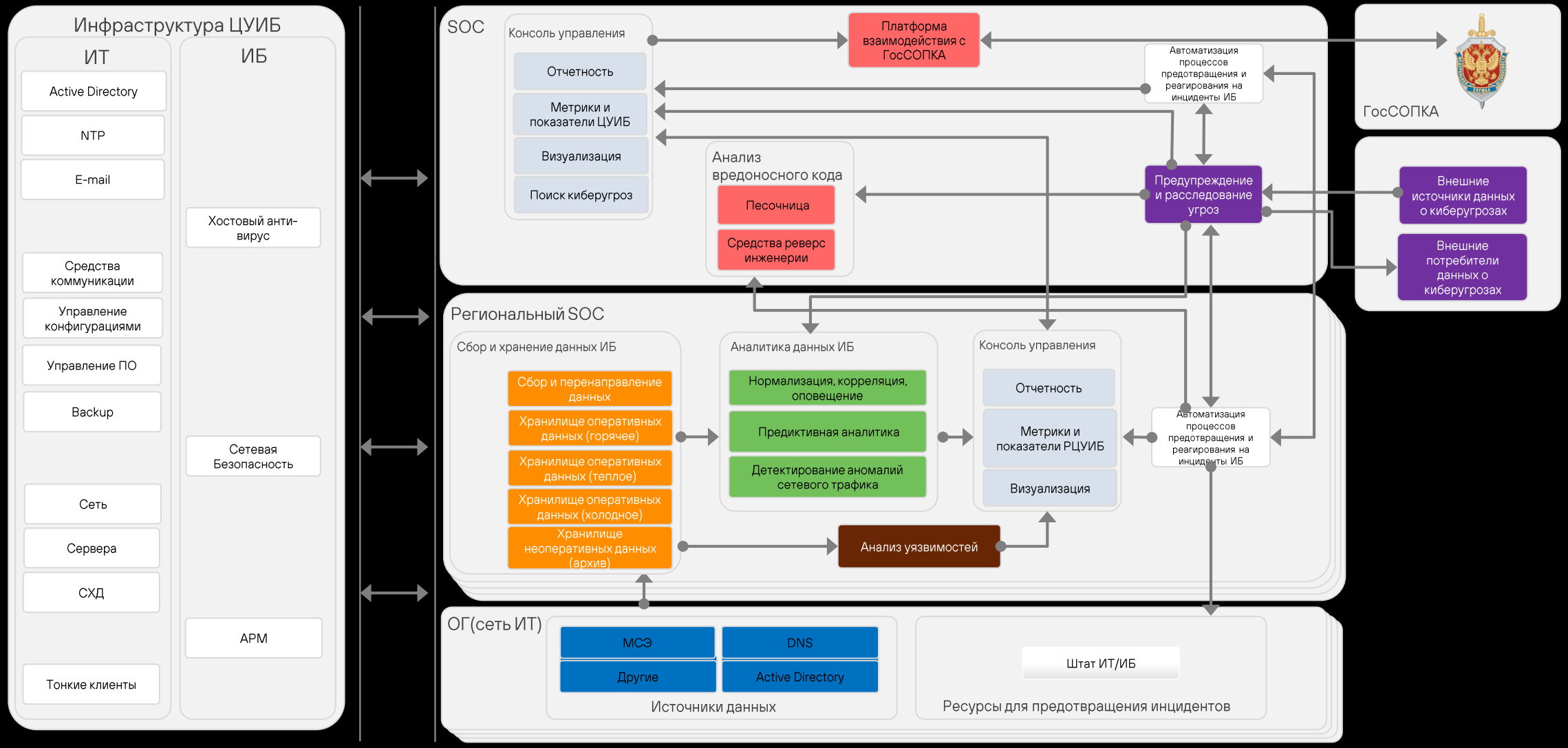
Долгое внедрение
Критично для бизнеса
Высокая стоимости внедрения
Регулярные аудиты

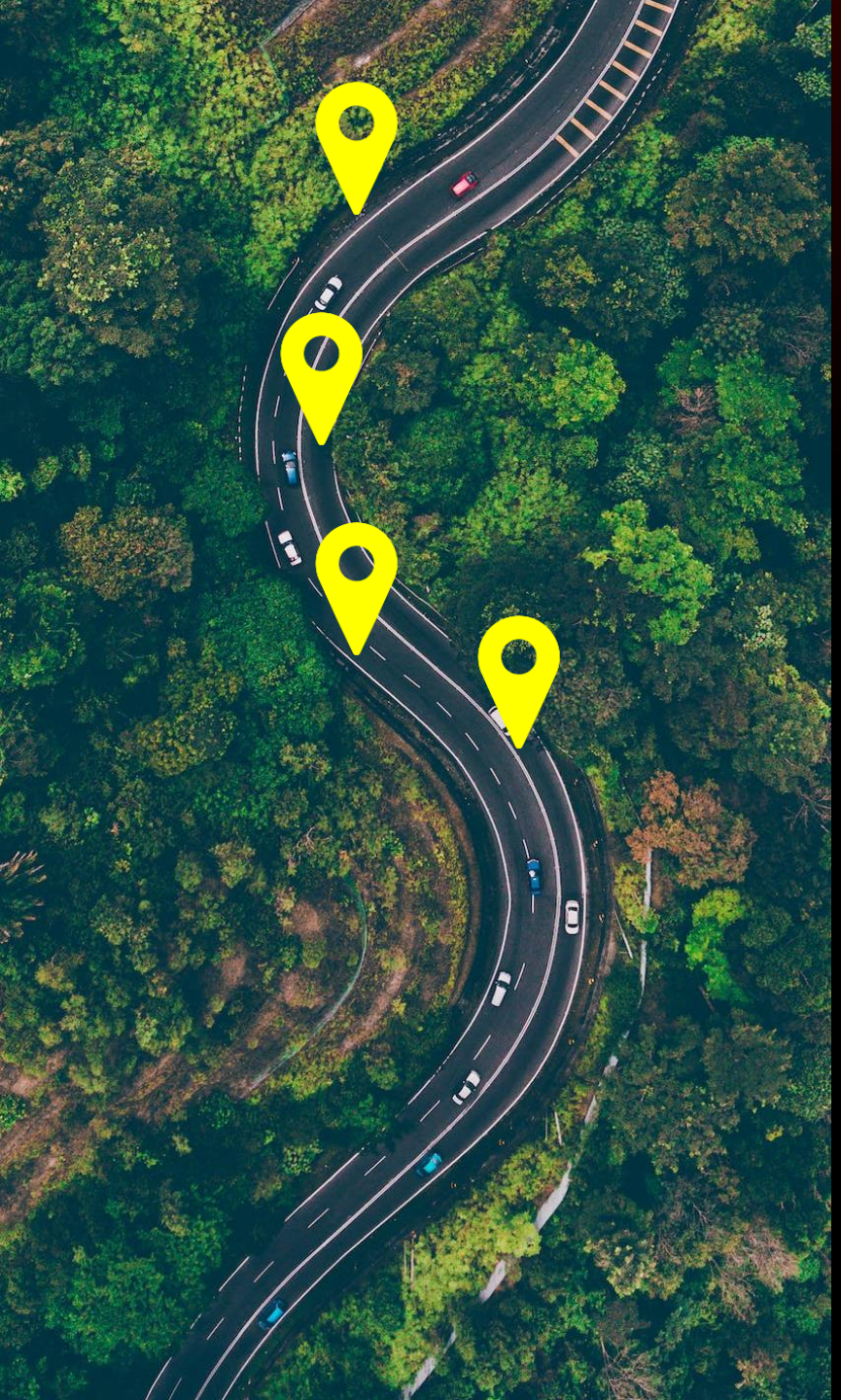


Формируем чеклист

- ❑ Архитектура компонентов
- ❑ Поддержка режима Air Gap
- ❑ Производительность (EPS/FPS)
- ❑ Иерархия управления
- ❑ Мультитенантность

Функциональная схема SOC





Формируем чеклист

- Взаимодействие с ГосСОПКА / ФинЦЕРТ / Минцифры
- Песочница
- Реверс-инжиниринг ПО
- Форензика
- API и интеграция с внешними решениями
- Threat Hunting
- Дашборды и отчетность

Сервисы SOC

Расследование инцидентов

- Cyber Security Monitoring
- Cyber Security Investigation and Escalation
- Cyber Threat Hunting
- Cyber Security Incident Remediation
- Post-Incident Analysis

Cyber Threat Intelligence

- Intelligence Collection, Evaluation and Collation
- Intelligence Analysis
- Intelligence Production
- Intelligence Reporting and Communications

Платформы и контент

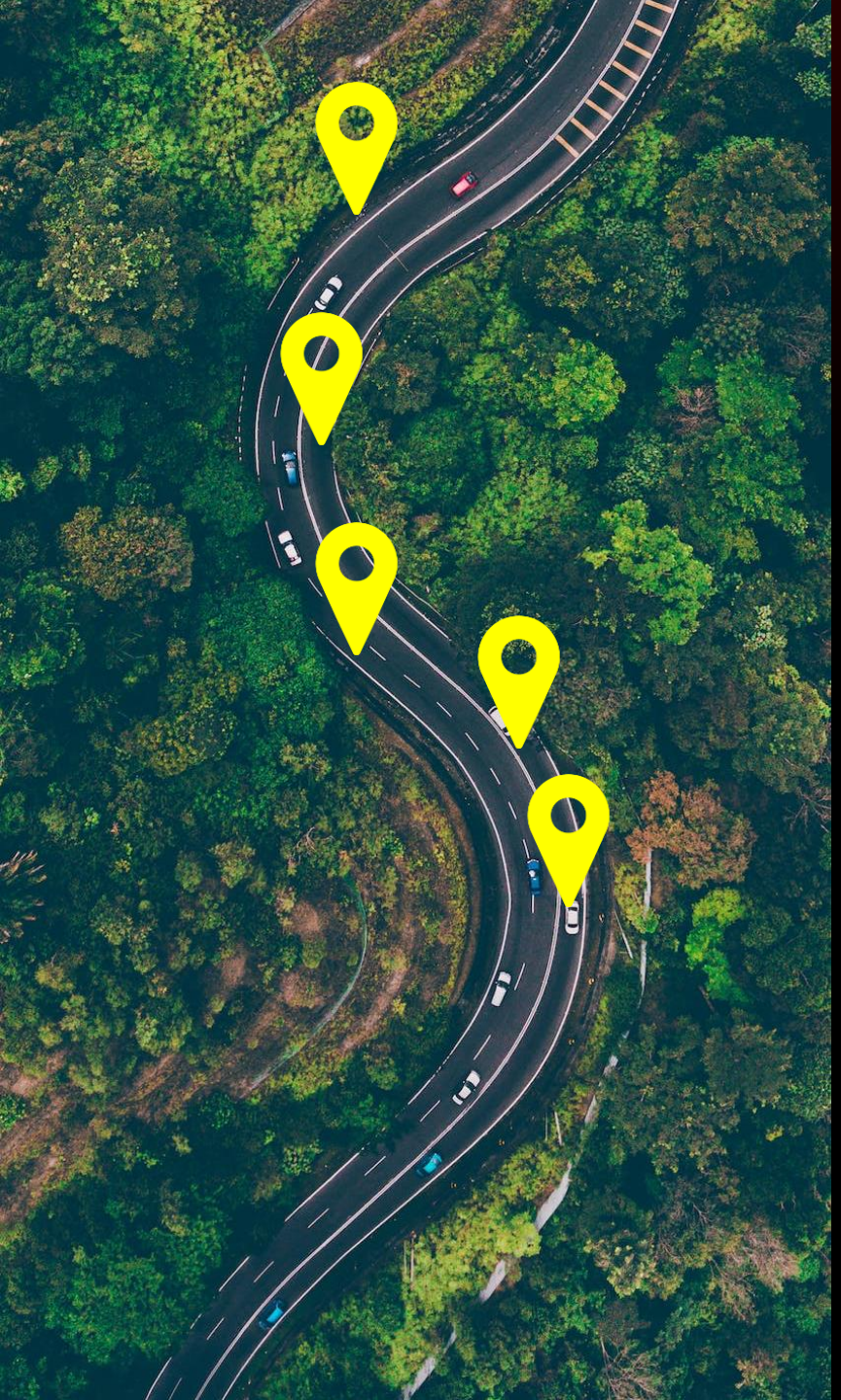
- Platform Development
- Platform Engineering
- Platform Operations
- Content Management

Аналитика безопасности

- Security Data Management
- Security Analytics

Управление сервисами

- Business Service Management
- IT Service Management
- Operations Management
- HR Management



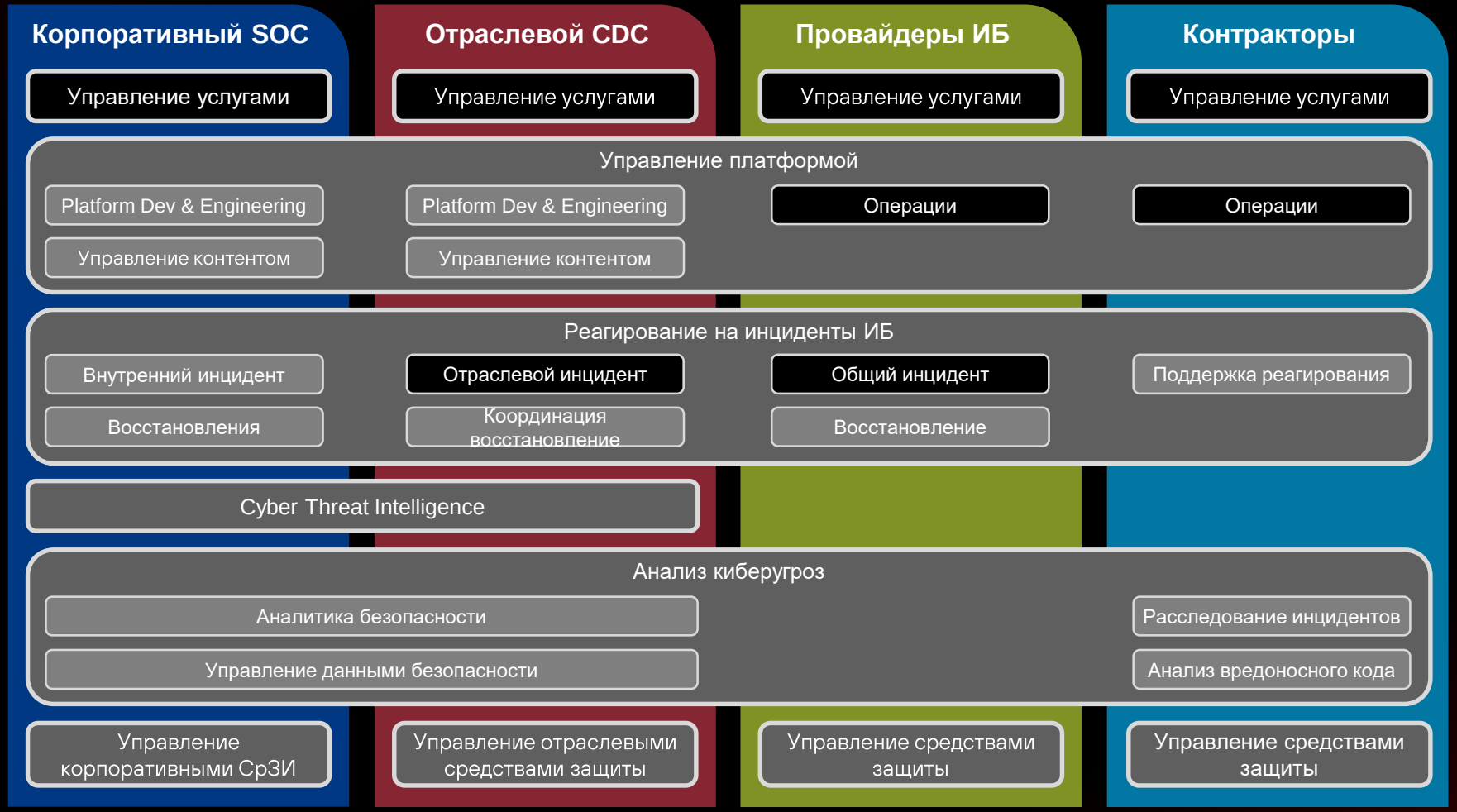
Формируем чеклист

- Управление обновлениями платформ для SOC
- Резервное копирование
- Моделирование угроз и управление use cases

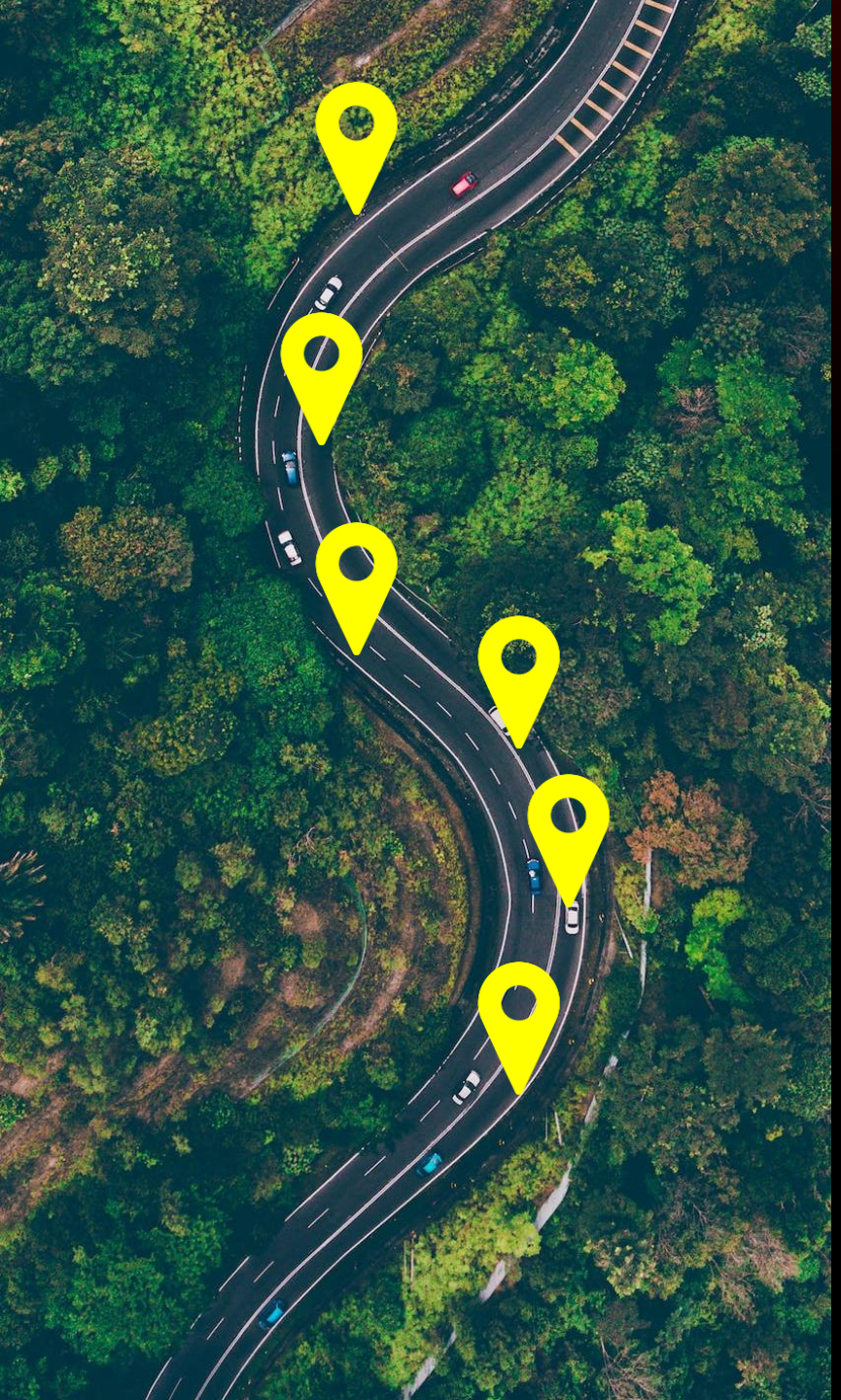
У вас есть кадры?

- Квалифицированные
- Нужное количество
- Для режима 24x7

Операционная модель SOC



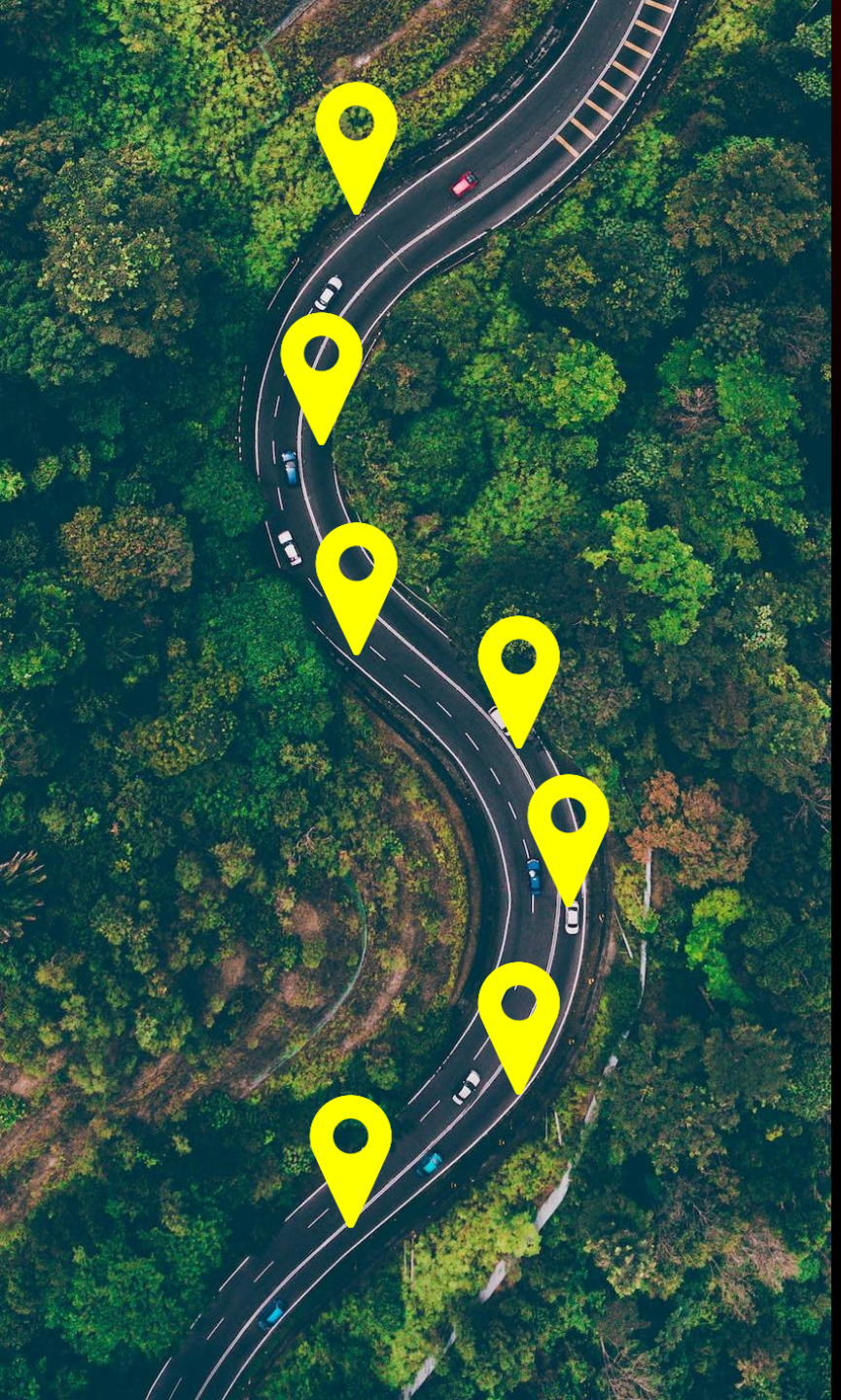
- Услуги объединяются между национальным, отраслевыми CDC и корпоративными SOCами
- Дополнительная поддержка от внешних организаций



Формируем чеклист

- IAM для ролевого управления
- VPN / PKI для защищенного взаимодействия с контракторами
- Конверторы правил обнаружения

Как вы тестируете ваш SOC?



Формируем чеклист

- BAS для тестирования
- MITRE Caldera для эмуляции хакерских группировок
- Тесты Atomic Red Team

Не забывайте про нормативку

- Импортозамещение
- Поддержка отечественных ОС
- Сертификация

Сервисная стратегия SOC определяет используемые технологии

Видение стратегии	Драйвера, ожидания заказчика, ключевые принципы и ожидаемый результат
Резюме по сервисам	Описание сервисов SOC – модель реализации, владелец, вход и выход для сервиса, компоненты
Ключевые процессы	Описание ключевых процессов, необходимых для реализации сервисов SOC
Организационная стратегия	Описание структуры команды SOC и всех ролей
Технологическая стратегия	Описание технологического стека SOC

Спасибо

alukatsky@ptsecurity.com