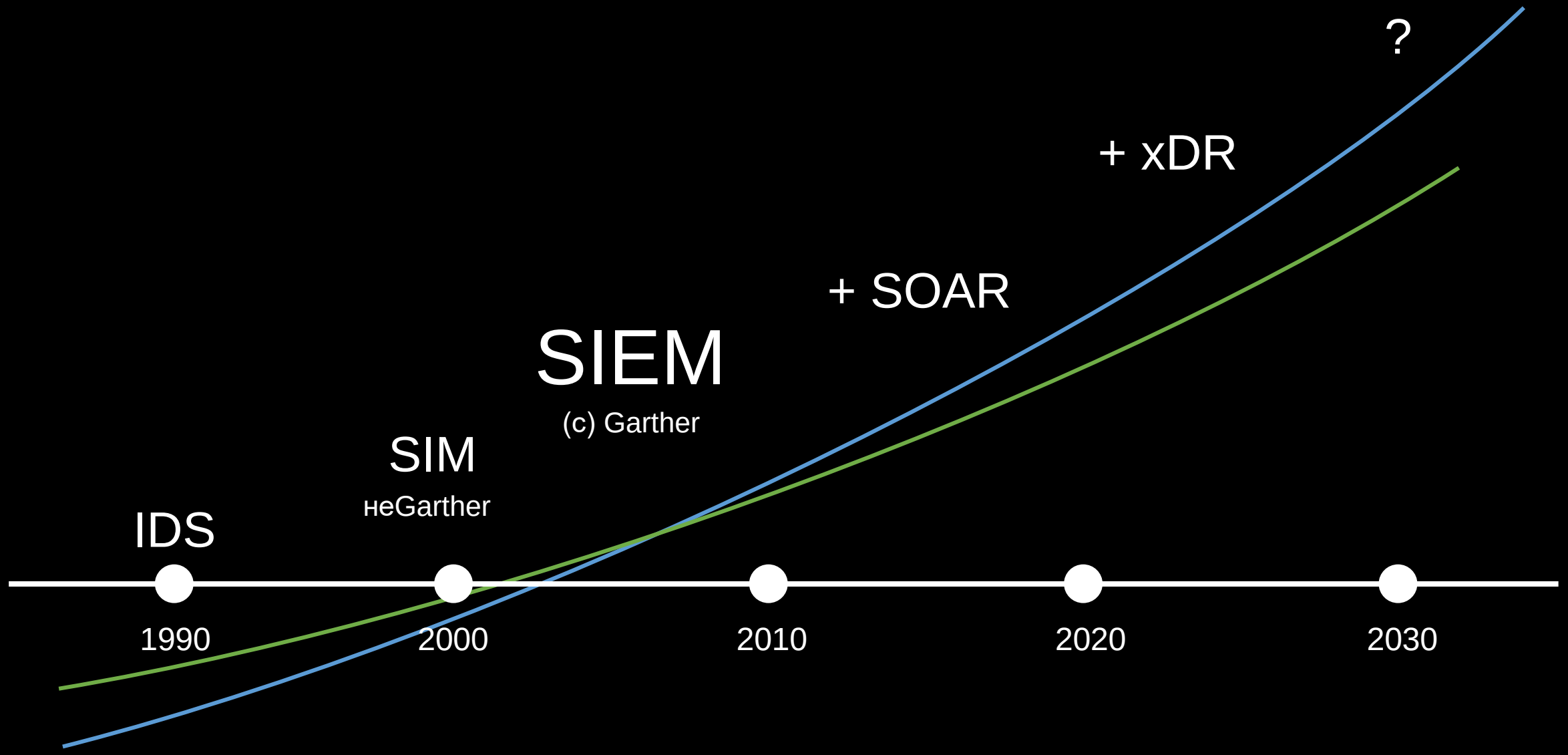
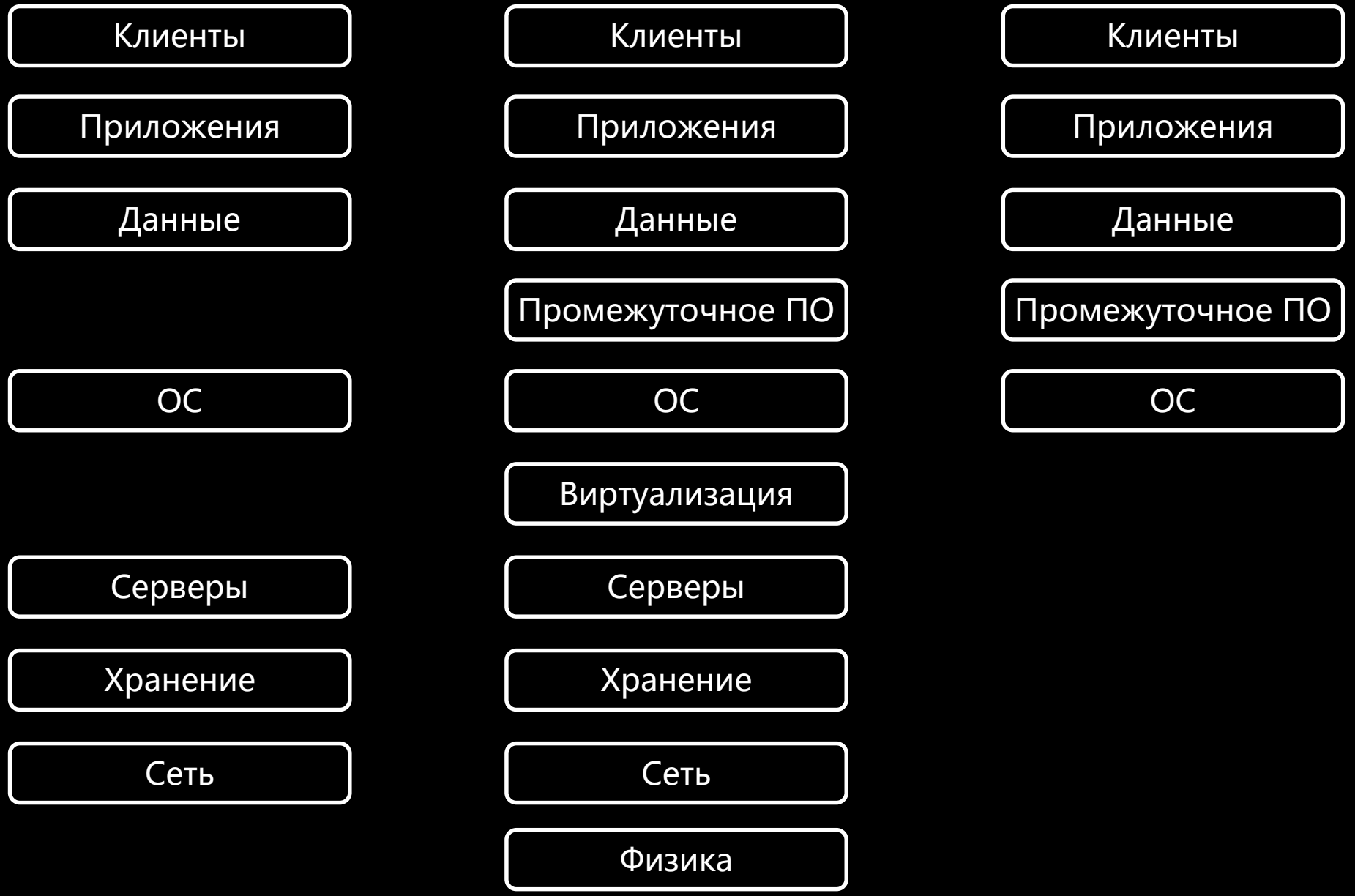
ЖИЗНЬ ПОСЛЕ

SIEM

ЖИЗНЬ ПОСЛЕ SIEM

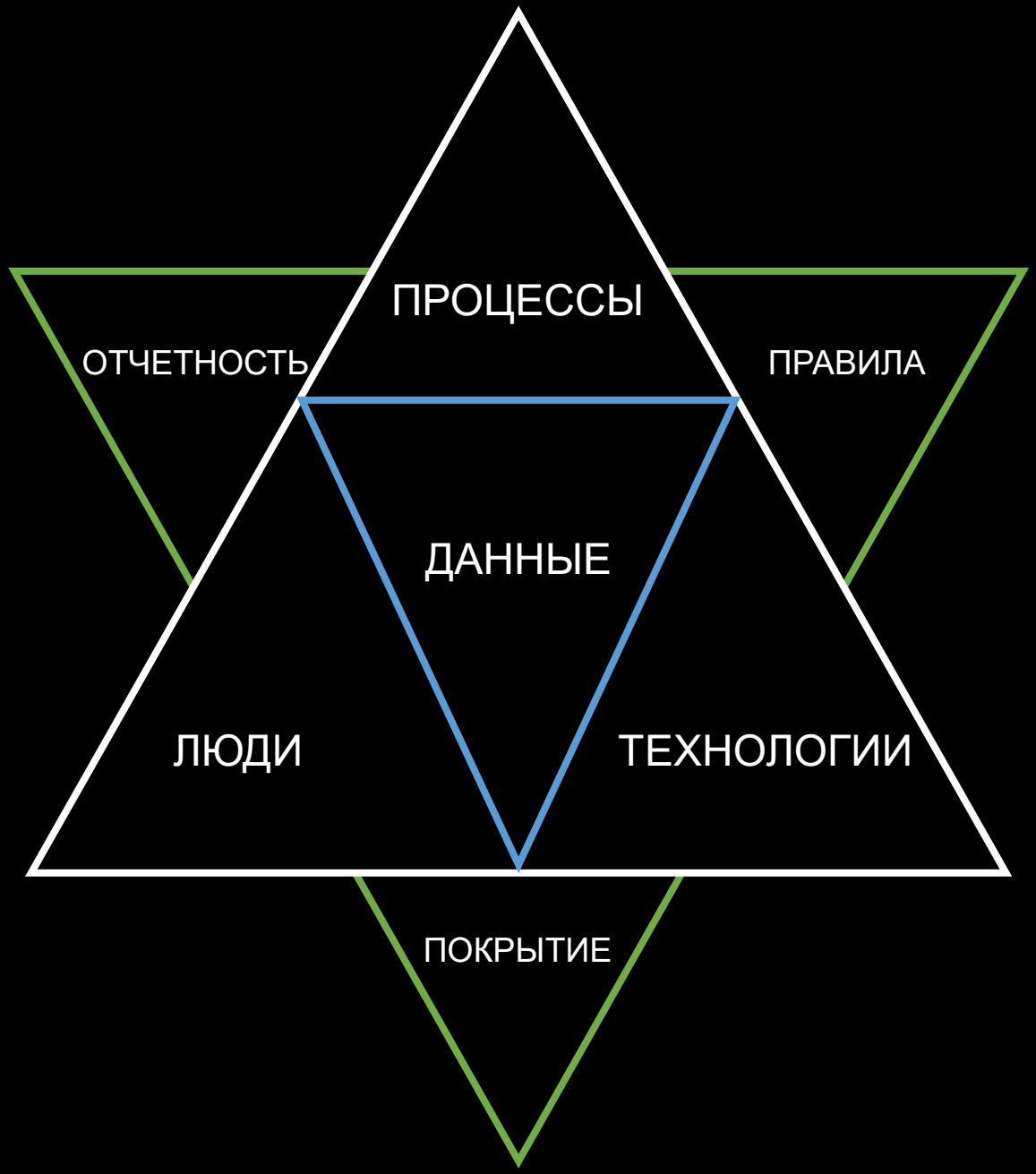

?
+ xDR
+ SOAR
SIEM
(c) Garther
SIM
неGarther
IDS
1990
2000
2010
2020
2030
Масштаб и сложность инфраструктуры
Объем обрабатываемых данных
… а также объем трафика, количество приложений, пользователей, клиентов, кибератак – да все растет


Клиенты
Приложения
Данные
ОС
Серверы
Хранение
Сеть
Клиенты
Приложения
Данные
Промежуточное ПО
ОС
Виртуализация
Серверы
Хранение
Сеть
Физика
Клиенты
Приложения
Данные
Промежуточное ПО
ОС

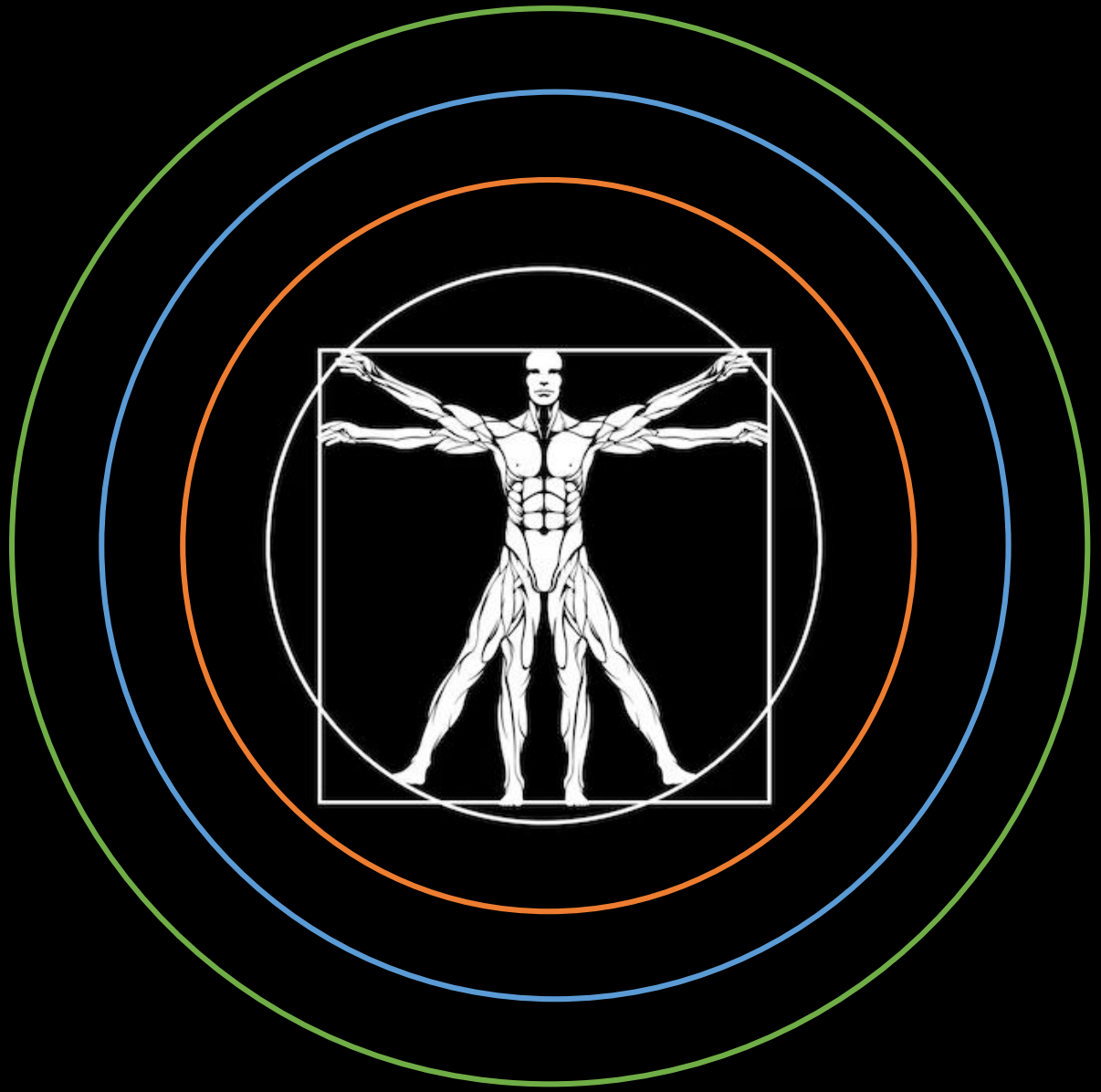
5 SIEMов в SOCe. Кто больше?

ЗЫ. Скоро должен быть шестой ;-)

t.me/alukatsky


ПРОЦЕССЫ
ОТЧЕТНОСТЬ
ПРАВИЛА
ДАННЫЕ
ЛЮДИ
ТЕХНОЛОГИИ
ПОКРЫТИЕ


AI Response
Data driven Defense
Response Automation
SIEM
xDR
Threat Hunting
Forensics
Analytics
Engineering
SOAR
Red Team
Vulnerability management
Threat Intel



Пользователи

Приложения

Данные

Инфраструктура

U E B A*

User and Entity Behavior Analytics

Управление архитектурой	Управление архитектурой организации
Непрерывное улучшение и управление качеством IT	Планирование деятельности
	Управление улучшениями и качеством
	Координация процессов
	Контроль процессов
	Предоставление отчетности
Управление информационной безопасностью	Внедрение контролей безопасности
	Валидация ИТ-безопасности
	Обзор безопасности и отчетность
Управление знаниями	Управление знаниями
Метрики и отчетность	Обзор сервисов
	Обзор процессов
Управление организационными изменениями	Управление организационными изменениями
Управление портфелем	Подготовка к проектированию услуг
	Начало проектирования услуг
	Обзор и обслуживание портфеля услуг
Управление проектами	Создание проекта
	Планирование проекта
	Контроль над проектом
Управление отношениями	Забота о клиентах
	Прогноз потребностей
	Контроль потребностей
	Заключение контракта на стандартное ИТ-услуги
	Изучение удовлетворенности клиентов
	Управление отзывами клиентов
	Мониторинг жалоб клиентов
Управление финансами	Финансовая организация ИТ
	Бюджетирование ИТ
	Прогноз развития ИТ
	Мониторинг IT-расходов
	Счет-фактуры за IT-услуги
	Анализ прибыльности ИТ
	Финансовая отчётность ИТ
Управление стратегией	Оценка стратегии ИТ
	Концепция стратегии ИТ
	Внедрение стратегии ИТ
Управление поставщиками	Организация управления поставщиками
	Оценка поставщиков
	Подготовка договоров с поставщиками
	Запрос требований
	Выбор поставщиков
	Управление жизненным циклом для контрактов с поставщиками
	Обзор поставщиков и отчетность
Управление персоналом и талантами	Актуализация квалификационных требований
	Планирование мероприятий по повышению квалификации персонала
	Мониторинг деятельности и отчетность
Управление доступностью	Планирование и мониторинг доступности
	Тестирование доступности
	Отчетность о доступности
Бизнес-аналитика	Бизнес-анализ
	Управление профилями пользователей
Управление мощностями и эффективностью деятельности	Прогнозирование емкости
	Мониторинг емкости и производительности
	Отчетность о емкости и производительности
Управление изменениями	Организация контроля за изменениями
	Регистрация и классификация изменений
	Оценка изменений
	Планирование изменений
	Оценка изменений до планирования
	Оценка изменений до реализации
	Оценка изменений перед развертыванием
	Оценка изменений после развёртывания
	Обзор изменений и отчетность
Управление инцидентами	Организация управления инцидентами
	Поиск и устранение неисправностей второго уровня
	Мониторинг инцидентов и эскалация
	Управление масштабными инцидентами
	Отслеживание инцидентов и закрытие
	Информирование пользователей
	Отчетность об инцидентах
Управление ИТ-активами	Идентификация ИТ-активов
	Инвентаризация ИТ-активов
Мониторинг и управление событиями	Организация мониторинга и управления событиями
	Мониторинг событий
	Отслеживание и закрытие событий
Управление проблемами	Регистрация проблемы
	Решение проблемы
	Отслеживание и закрытие проблемы
	Обзор крупных проблем
	Отчетность о проблемах
Управление релизами	Организация управления выпуском релизов
	Подготовка релиза
	Поддержка при запуске и закрытие релизов
	Окончание срока службы для ИТ-услуг
	Отчетность о переходе
Управление каталогом сервисов	Управление каталогом сервисов
Управление рисками	Анализ рисков с точки зрения бизнеса
	Анализ рисков с точки зрения ИТ
	Оценка риска
	Деятельность по предотвращению риска
	Мониторинг рисков и отчетность
Управление конфигурацией сервисов	Организация управление конфигурацией
	Идентификация элемента конфигурации
	Аудит и отчетность по управлению конфигурацией
Управление непрерывностью обслуживания	Планирование действий в чрезвычайных ситуациях
	Тренировки действий в условиях катастрофы
	Обзор и отчетность по управлению непрерывностью обслуживания
Проектирование услуг	Организация проектирования услуг
	Планирование проектирования услуг
	Мониторинг проектирования услуг
	Техническое и организационное проектирование услуг
	Пересмотр дизайна услуг
Служба поддержки	Регистрация инцидентов и заявок
	Решение на первом уровне
Управление уровнем сервиса	Организация управления уровнем сервиса
	Требования к уровню сервиса
	Соглашения об уровне сервиса
	Одобрение уровня сервиса
	Пересмотр уровня сервиса и отчетность
Управление запросами на обслуживание	Запрос на услугу
	Запрос на восстановление резервной копии
	Включение и исключение из списков
	Запрос разрешения пользователя
Проверка и тестирование услуг	Определение процедур тестирования
	Тестирование компонентов
	Интеграционное тестирование
	Приемочное тестирование
Управление развёртыванием	Развертывание
	Минорное развертывание
Управление инфраструктурой и платформами	Определение портфеля ИТ-технологий
	Управление портфелем ИТ-технологий
	Управление ИТ-операциями
	Непредвиденные действия
Разработка и управление программным обеспечением	Разработка и настройка приложений

СПАСИБО