НТЦ ВУЛКАН

Оптимизация подходов к проектированию комплексной системы ИБ: Работа над ошибками

www.ntc-vulkan.ru

НТЦ «Вулкан» - независимый эксперт и интегратор технологий информационной безопасности

На рынке с **2010** года

150+ сотрудников в штате

Комплексные решения в сфере экономической и информационный безопасности

Сертифицированная система менеджмента качества

500+ реализованных проектов в ИБ

Входит в **40** крупнейших компаний РФ в сфере защиты информации

По версии TAdviser, 2022

20+ проектов внедрения SIEM

Допуски и лицензии ФСТЭК, ФСБ, Минобороны, Минпромторг

НАШИ ЗАКАЗЧИКИ – ВСЕГО БОЛЕЕ 200 ОРГАНИЗАЦИЙ

Финансовый сектор: кредитные и некредитные финансовые организации

СБЕР · Тинькофф Банк · Банк России · Банк Санкт-Петербург · МТС Банк · Financial Services Toyota

СБЕР СТРАХОВАНИЕ · Тинькофф Страхование · ДОМ РФ · Инфинитум · СОГАЗ Страховая группа · ИНГОССТРАХ

Спасибо · Московская Биржа · Национальный расчетный депозитарий · Национальный клиринговый центр · QIWI · БКС

Телекоммуникации и связь

Ростелеком · МегаФон · МТС · Билайн · TELE2 · МТТ

Государственные структуры и организации

ДИТ · Информационный город · ТУРИЗМ.РФ

ТЭК и производственные предприятия

ЛУКОЙЛ · РусГидро · Мосэнерго · РОС РАО · Роскосмос · Сухой

Прочие компании широкого спектра отраслей

Связной · B2B Center · ОТС.ru · Сибинтек · nexters · Микроген

ТЕКУЩЕЕ ПОЛОЖЕНИЕ ВЕЩЕЙ

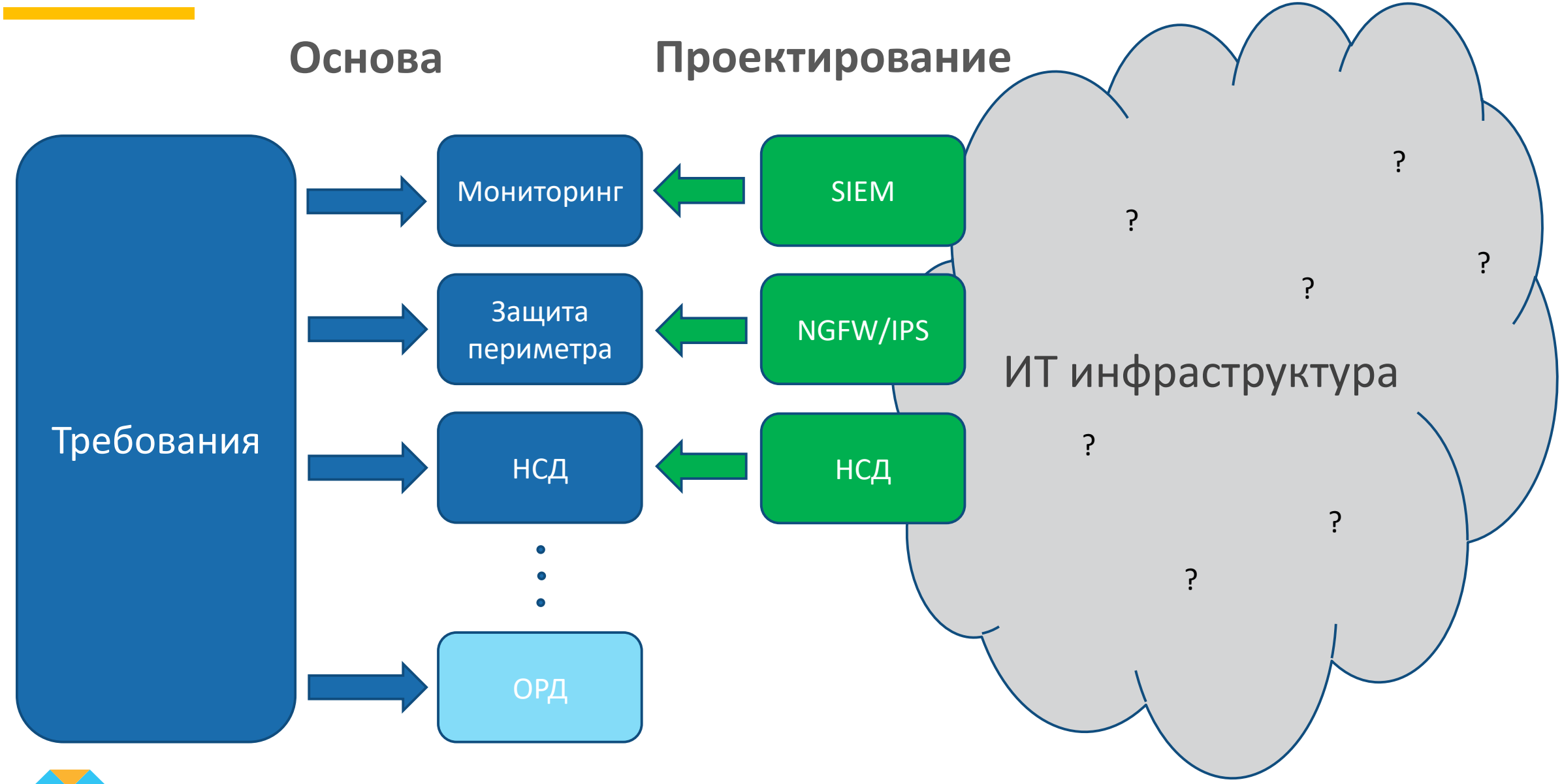


- Необходимость замены/модернизации средств защиты по причине изменяющихся требований и импортозамещения
- Низкий уровень адаптации «типовых» проектов комплексных систем ИБ к ИТ- и бизнес-ландшафту конкретного заказчика
- Существенные проблемы совместимости наложенных средств защиты со стационарно-эксплуатируемыми критическими информационными системами и затраты на их приобретение
- **Низкий уровень заинтересованности ИТ службы и службы эксплуатации АСУ ТП**
- Необходимость постоянного наращивания «дорогостоящих компетенций» сотрудников для эксплуатации наложенных средств

ПРОСТЫЕ ЖЕЛАНИЯ



УСТОЯВШИЙСЯ ПОДХОД К ПРОЕКТИРОВАНИЮ



АЛГЕБРОЙ ГАРМОНИЮ ПОВЕРИТЬ…



Требования Приказа 239
на первый взгляд «закрываемые»
наложенными средствами

Установление четкого (табличного) соответствия между требованиями и возможностями настройки элементов инфраструктуры в рамках следующих «доменов»:

- Linux – Серверы и Рабочие станции
- Windows – Серверы и Рабочие станции
- Межсетевые экраны
- и т.д.

MITRE ATT&CK™

НТЦ ВУЛКАН

ОПТИМИЗАЦИЯ ПОДХОДОВ К ПРОЕКТИРОВАНИЮ

ОБЩАЯ ИДЕЯ ПОДХОДА

Основной новацией является использование при обследовании специально разработанной «Матрицы», увязывающей векторы атак и виды (типы) элементов инфраструктуры и необходимые для идентификации и противодействия этим атакам настройки вышеуказанных элементов

Снижение стоимости и ускорение внедрения

- Максимальное и эффективное использования встроенных возможностей элементов инфраструктуры в части настроек при обнаружении и предотвращении атак на основе «Матрицы»

Повышение «реализуемости» проекта

- Максимальное вовлечения в проект всех заинтересованных служб, что обеспечит комфортную реализацию проекта

ЧТО В РЕЗУЛЬТАТЕ?

В зависимости от потребностей Заказчика результатами проведения работ могут стать:

1. Комплексное заключение о безопасности обследуемой инфраструктуры/объекта с рекомендациями по модернизации
2. Входные данные для ОПТИМАЛЬНОГО проектирования комплексной системы ИБ
3. Выводы о соответствии требованиям ФСТЭК и пути совершенствования
4. Структурированные рекомендации по настройке элементов инфраструктуры

Любой вариант результата будет содержать в себе обоснованные предложения по смещению акцента с наложенных средств защиты в сторону оптимальных и безопасных настроек элементов инфраструктуры

ПРЕИМУЩЕСТВА ПОДХОДА

- **Максимум эффекта** при минимальных временных и финансовых затратах – повышение уровня защищенности посредством **осмысленной настройки существующих ИТ-активов**
- **Снижение затрат** на внедрение/модернизацию комплексной системы ИБ и отдельных подсистем, а так же обеспечение минимальных **сроков реализации**
- Повышение степени «реализуемости» запроектированного решения, что повышает **уровень реальной безопасности** и **рисков невыполнения требований** регулятора
- **Консолидация усилий** служб ИБ и ИТ организации-заказчика
- **Снижения издержек** на администрирование, закупку, переобучение персонала и изменение моделей лицензирования
- «Автоматическая» готовность и **упрощение процесса** внедрения/реанимации систем SIEM или SOAR.

СПАСИБО ЗА ВНИМАНИЕ!



НТЦ ВУЛКАН

www.ntc-vulkan.ru

marketing@ntc-vulkan.ru