19/07/2018

JET CSIRT

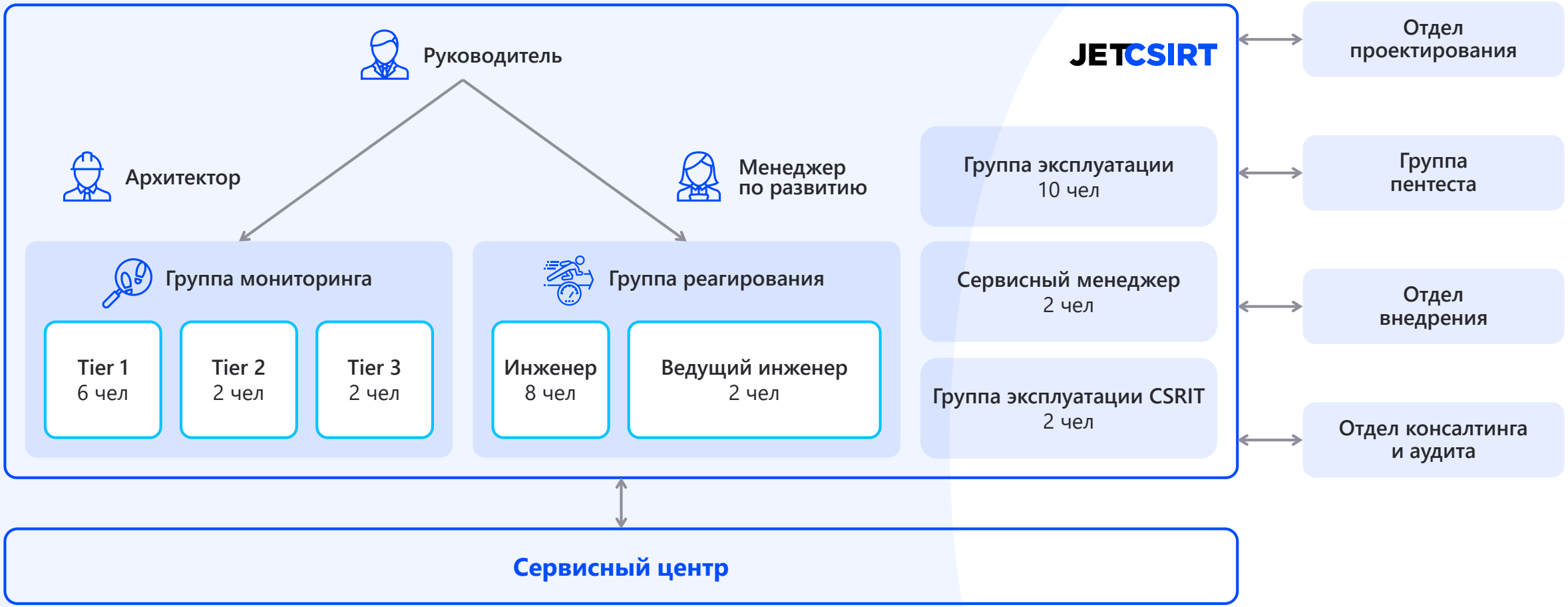
Jet Computer Security Incident Response Team

Алексей Мальнев
Начальник отдела аутсорсинга ЦИБ АО «Инфосистемы Джет»
ay.malnev@msk.jet.su / +7 985 849-89-33

ЧТО ТАКОЕ JET CSIRT?

JET CSIRT В СОСТАВЕ УСЛУГ ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КОМАНДА JET CSIRT. ОРГСТРУКТУРА

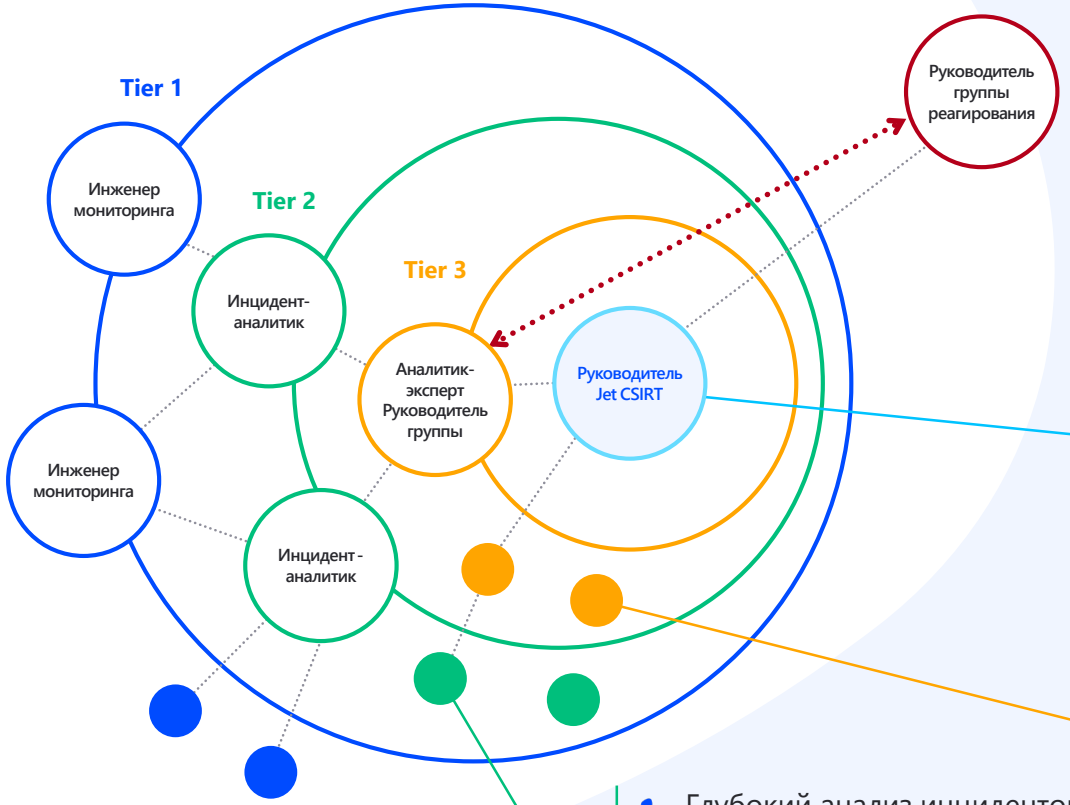


КОМАНДА JET CSIRT. ГРУППА МОНИТОРИНГА

Сервисный центр (операторы)

Передовая

Передовая



- Управление командой
- Разработка стратегии развития
- Пресейл/маркетинг
- SLA
- Координация с руководством
- Точка координации по оргвопросам и критичным инцидентам

- Мониторинг (Alert Monitoring)
- Оповещение Заказчика
- Контроль состояния SIEM
- Сбор данных для Tier 2

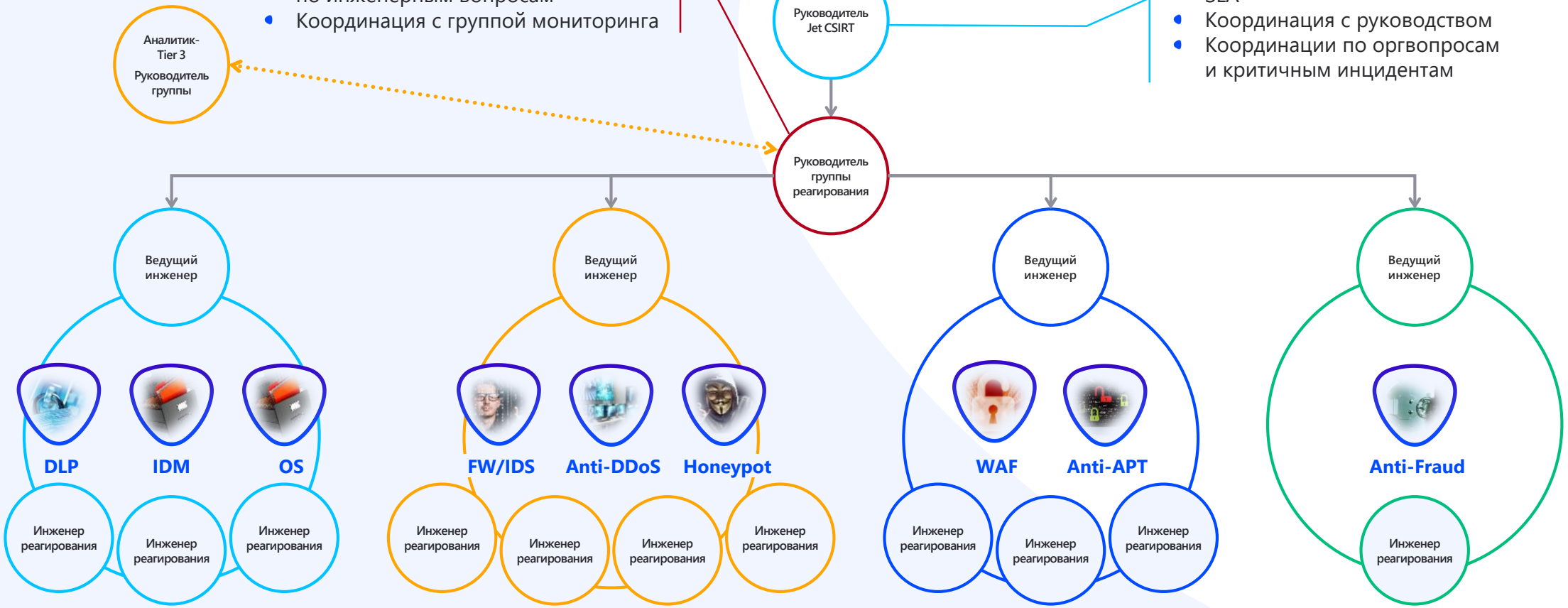
- Глубокий анализ инцидентов
- Определение атакованных активов/ систем и фиксация атакующих
- Консультации по вопросам восстановления
- Участие в поиске новых аналитических методов для обнаружения угроз
- Vulnerability Management

- Глубокое изучение инфраструктуры
- Threat Intelligence
- Расследование инцидентов
- Malware Reverse Engineering
- Incident Hunting
- Threat Detection Tuning
- Координация с группой реагирования

КОМАНДА JET CSIRT. ГРУППА РЕАГИРОВАНИЯ

- Руководство сменами
- Экспертная консультация по инженерным вопросам
- Координация с группой мониторинга

- Управление командой
- Разработка стратегии развития
- Пресейл/маркетинг
- SLA
- Координация с руководством
- Координации по оргвопросам и критичным инцидентам



ОПЦИИ JET CSIRT

Премиум

Стандартный

Базовый

- Мониторинг событий ИБ
- Подключение источников событий
- Расследование инцидентов ИБ
- Кибераналитика по внешним угрозам

- Управление уязвимостями
- Разработка уникальных сценариев выявления инцидентов
- Техническое реагирование Сдерживание и нейтрализация
- Проактивный поиск и обнаружение угроз
- Администрирование СЗИ
- Предоставление СЗИ по подписке
- Управление жизненным циклом инцидента (IRP Jet Signal)

- Изучение вредоносного кода
- Аналитика по открытым данным (OSINT)
- Бизнес-ориентированная аналитика
- Комплексное ИБ консультирование
- Аудит и анализ защищенности
- Форензика

СХЕМА ПОДКЛЮЧЕНИЯ JET CSIRT. ВАРИАНТ 1 ЭКСПЛУАТАЦИЯ SIEM И СРЕДСТВ ИБ ЗАКАЗЧИКА

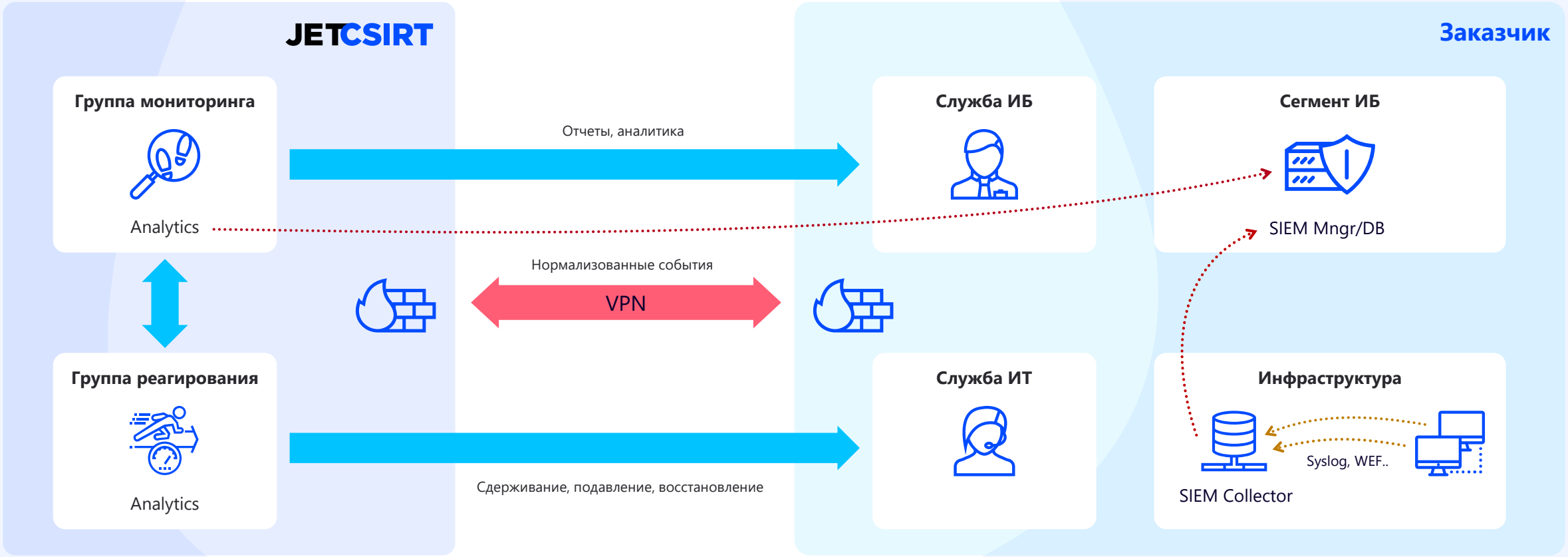
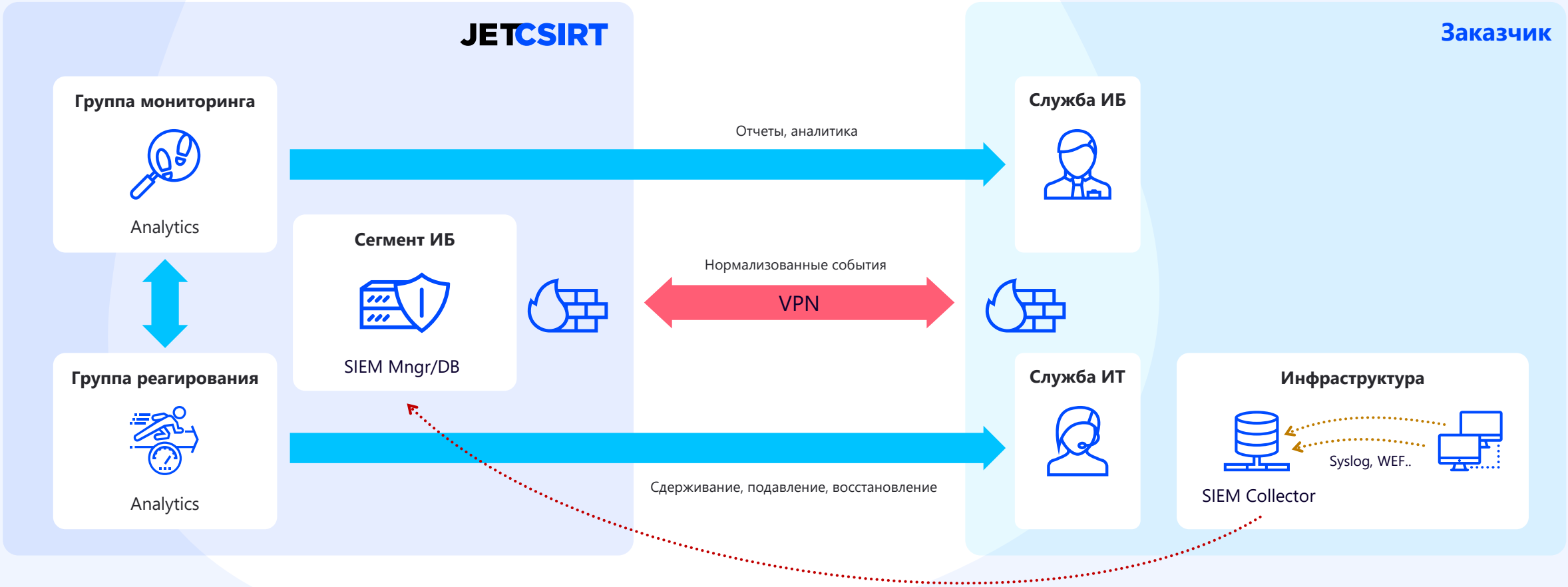


СХЕМА ПОДКЛЮЧЕНИЯ JET CSIRT. ВАРИАНТ 2 ОБЛАЧНОЕ РЕШЕНИЕ ОТ ИНФОСИСТЕМЫ ДЖЕТ



ИНСТРУМЕНТЫ JET CSIRT

Источники данных (телеметрия)

- Сетевая инфраструктура
- Серверы
- Рабочие станции
- Приложения
- Средства защиты информации
- Базы данных

Мониторинг

FORTINET
POSITIVE TECHNOLOGIES
MICRO FOCUS
IBM
splunk>

Управление жизненным циклом инцидента

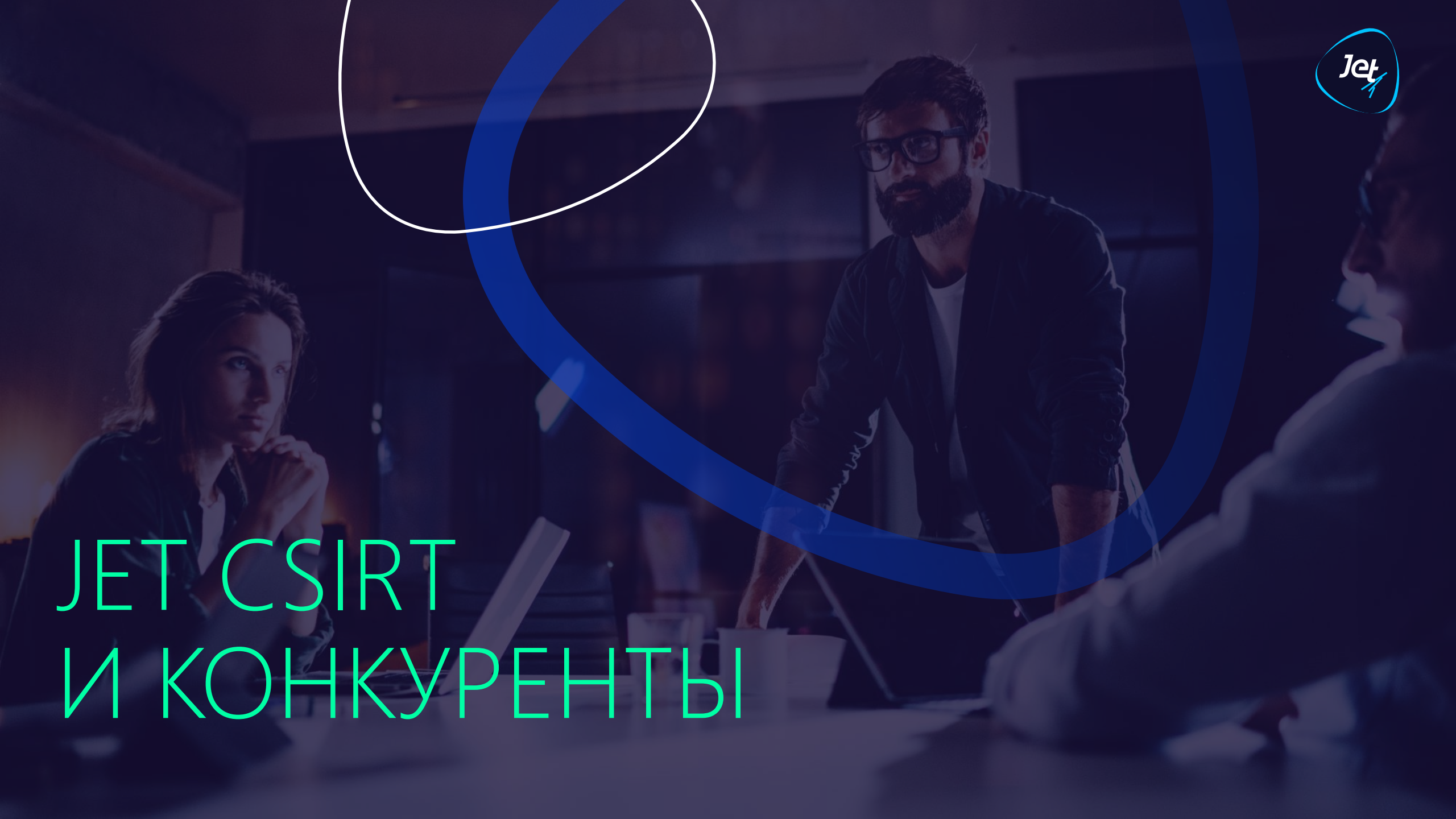
JET SIGNAL
bmc Remedy

Средства реагирования

CISCO
paloalto
McAfee
Check Point
POSITIVE TECHNOLOGIES
Dozor
FORTINET
IMPERVA
INFOWATCH
KASPERSKY lab
radware
ARBOR NETWORKS
SKYBOX SECURITY

Средства визуализации

Qlik Sense



JET CSIRT
И КОНКУРЕНТЫ

JET CSIRT И КОНКУРЕНТЫ

Название	Jet CSIRT	JSOC	SOC	Центр Мониторинга	Kaspersky Managed Protection	CERT, Защита бренда, лаборатория криминалистики	Positive Technologies Expert Security Center (PT ESC)
Сервис мониторинга SOC облачный	✓	✗	✓ декларативно	✗ есть TIAS	✓	✗	✗
Сервис мониторинга SOC на стороне клиента	✓	✓ только ArcSight	✗	✗ преимущественно VipNet	✗	✗	✗
Сервис реагирования / эксплуатация СЗИ	✓ / ✓	✗ / ✓	✗ / ✓ декларативно	✗ / ✓ преимущественно VipNet	✗ / ✗	✗ / ✗	✓ / ✗

СРАВНЕНИЕ JET CSIRT И КОММЕРЧЕСКОГО SOC

JETCSIRT
Центр реагирования на инциденты информационной безопасности

- Фокус на мониторинг и реагирование
- SIEM Заказчика или SIEM из облака Jet CSIRT
- Мультивендорность HP, IBM, PT, Fortinet, Splunk
- Опции: администрирования СЗИ, пентесты и тд
- Гибкий подход под задачи Заказчика

Типовой коммерческий SOC

- Фокус на мониторинг
- SIEM из облака
- Одна платформа
- Опции помимо мониторинга на подрядах и дорогие
- Типовые массовые услуги

СРАВНЕНИЕ JET CSIRT И СОБСТВЕННОГО SOC

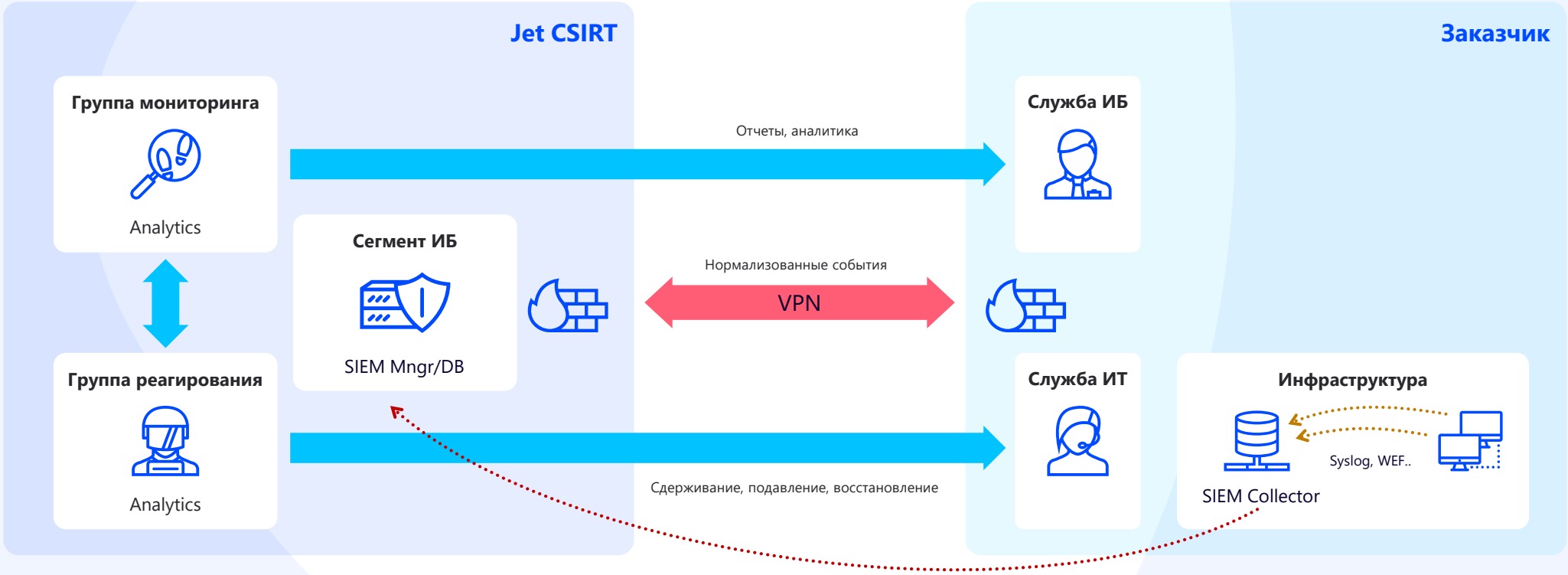
JET CSIRT
Центр реагирования на инциденты информационной безопасности

- Решение кадровой проблемы
- Умеренные OPEX затраты
- Снижение нагрузки на персонал
- Ответственность на уровне контракта и соблюдения SLA
- Глобальное виденье угроз и рисков ИБ

Собственный SOC

- Сложно найти, удержать и дорого содержать экспертов
- Высокие CAPEX и OPEX затраты
- Расфокусировка и избыточная нагрузка на персонал
- Ответственность в рамках должностных инструкций
- Виденье в рамках своей инфраструктуры

КАК ПОПРОБОВАТЬ JET CSIRT



- Срок пилота — 1 месяц (без оргподготовки)
- Согласуем методику проведения пилота
- Подключаем пилотный сегмент (живой) с несколькими источниками
- Опционально сканирование уязвимостей
- Опционально Sandbox
- Опционально реагирование на инциденты (Cont/Erad/Recov)

19/07/2018

СПАСИБО ЗА ВНИМАНИЕ!

Алексей Мальнев
Начальник отдела аутсорсинга ЦИБ АО «Инфосистемы Джет»
ay.malnev@msk.jet.su / +7 985 849-89-33