



Jet

31/05/2018

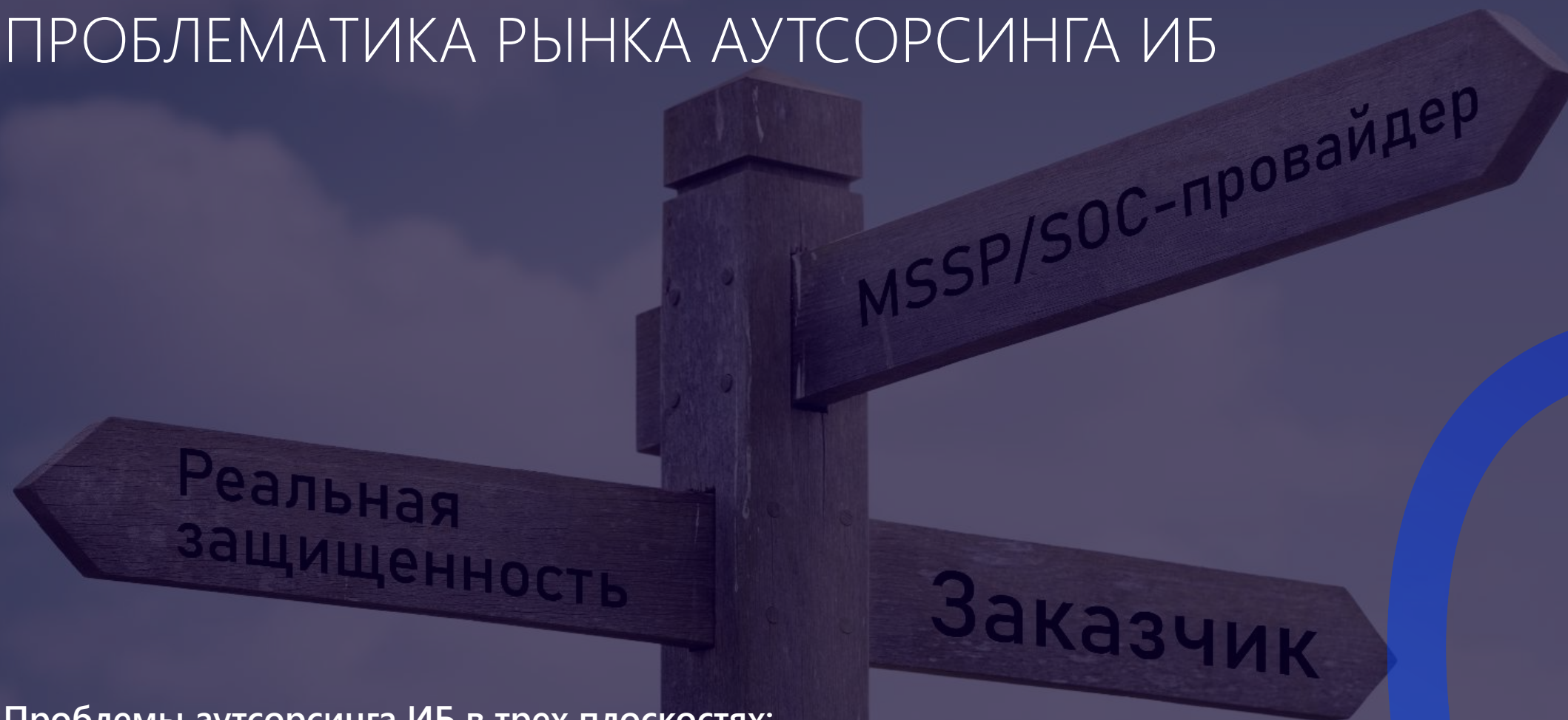
JET CSIRT: ЕСЛИ НУЖНО БОЛЬШЕ ЧЕМ SOC

**Алексей
Мальнев**

Начальник отдела аутсорсинга ЦИБ «Инфосистемы Джет»
au.malnev@jet.su / +7 985 849-89-33

- 1 | Проблематика рынка аутсорсинга ИБ
- 2 | Почему CSIRT, а не SOC?
- 3 | Сервис Jet CSIRT: подход и архитектура

ПРОБЛЕМАТИКА РЫНКА АУТСОРСИНГА ИБ



Проблемы аутсорсинга ИБ в трех плоскостях:

РЫНОК

ПРОЦЕССЫ

РЕАЛИЗАЦИЯ

МНОГО МАРКЕТИНГА В ИБ



MSSP

MDR

CERT



Threat
Intelligence

Security
Intelligence

CSIRT

SOC

МНОГО МАРКЕТИНГА В ИБ



CSIRT – Computer Security Incident Response Team

CERT – Computer Emergency Incident Response Team

SOC – Security Operation Center

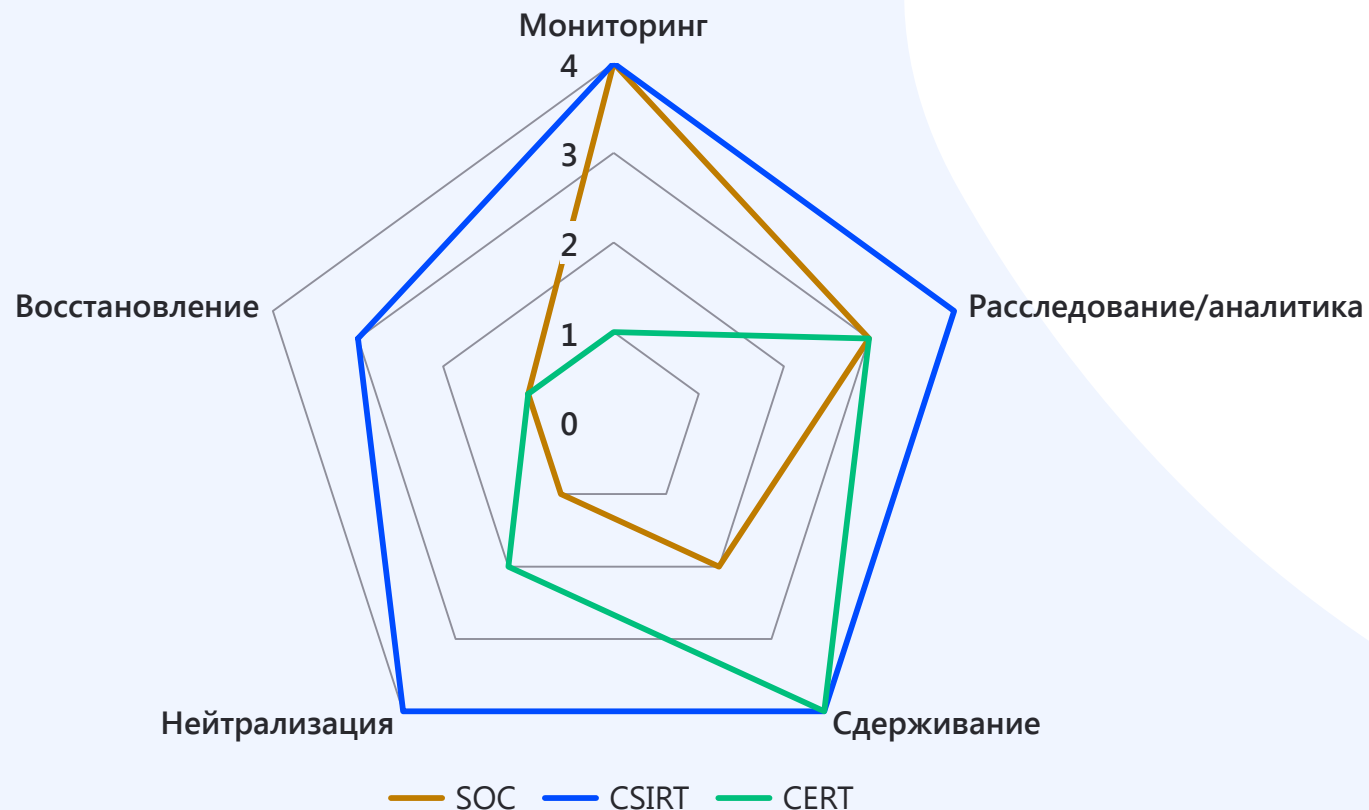
MDR – Managed Detection and Response Services

MSSP – Managed Security Service Provider

НЕСООТВЕТСТВИЕ ФОКУСА СЕРВИС-ПРОВАЙДЕРОВ И ОЖИДАНИЙ РЫНКА (1/2)



Сервис-провайдеры рынка экспертного аутсорсинга*



* Анализ усредненный, сделанный по опыту работы с десятками клиентов рынка аутсорсинга ИБ. В расчете уровней зрелости учитывалась статистика MicroFocus

НЕСООТВЕТСТВИЕ ФОКУСА СЕРВИС-ПРОВАЙДЕРОВ И ОЖИДАНИЙ РЫНКА (2/2)



* Анализ усредненный, сделанный по опыту работы с десятками клиентов рынка аутсорсинга ИБ. В расчете уровней зрелости учитывалась статистика MicroFocus

Проблемы конвейерного подхода:

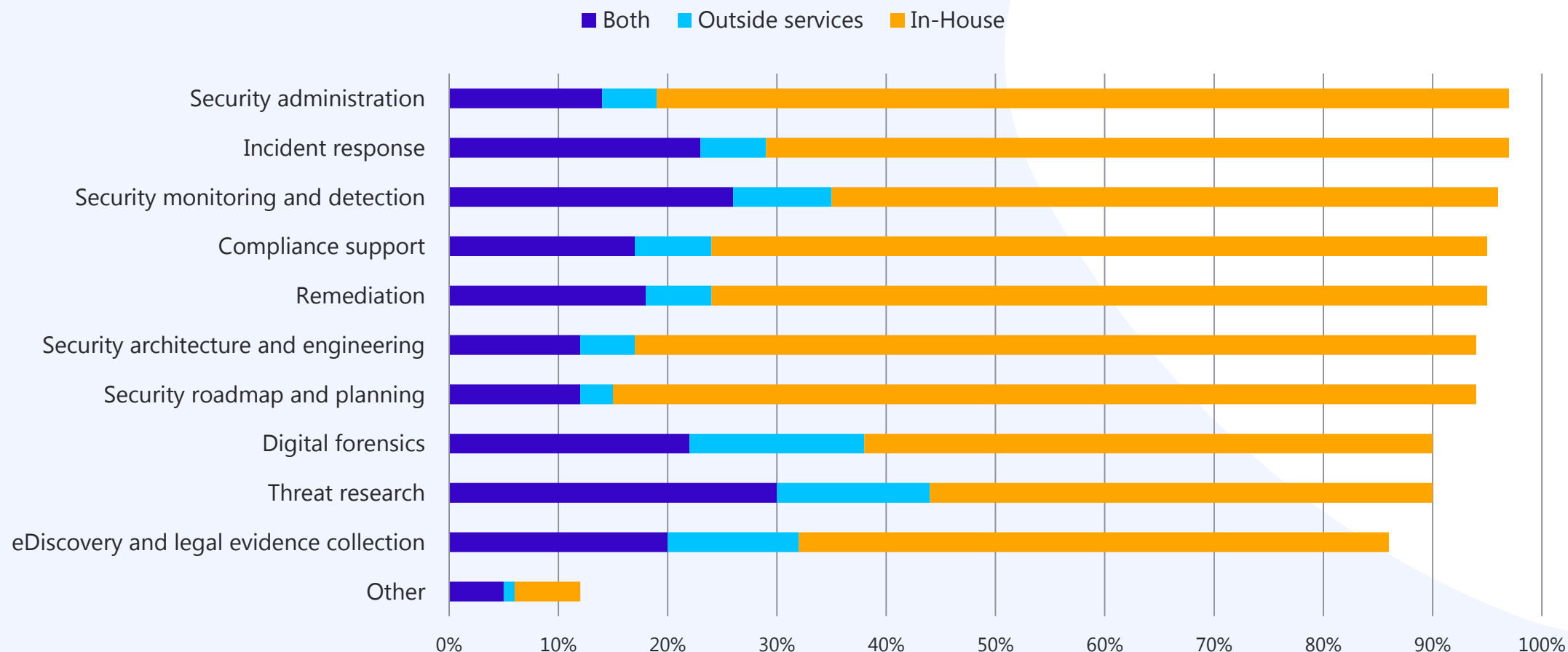
- SLA в ущерб процессам
- Типовые сценарии
- Облачный SIEM вместо SOC

Фундаментальные причины проблем:

- Минимизация трудозатрат
- Лояльность клиента не в приоритете

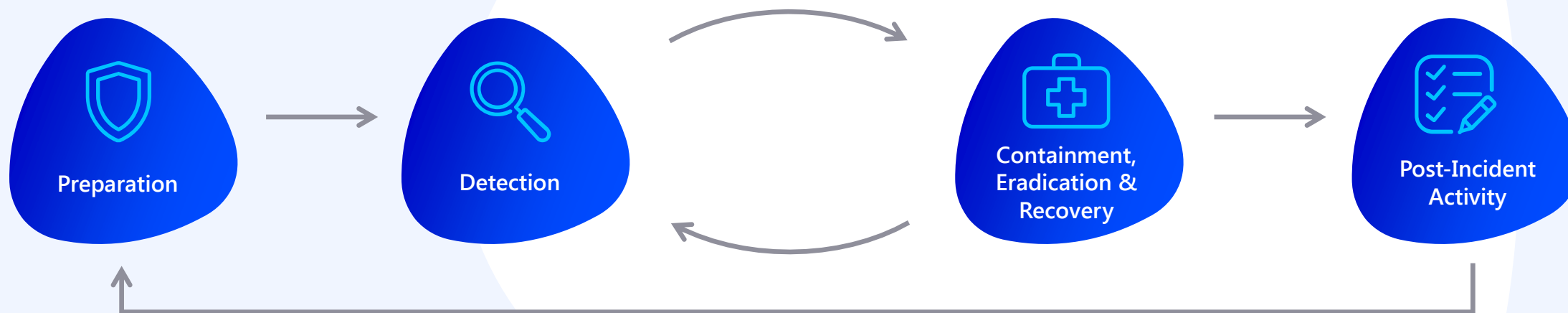
КОНВЕЙЕРНЫЙ
ПОДХОД

КАК НА ЭТО РЕАГИРУЕТ РЫНОК



Future SOC: SANS 2017 Security Operations Center Survey — <https://www.sans.org/reading-room/whitepapers/analyst/future-soc-2017-security-operations-center-survey-37785>

РЕАГИРОВАНИЕ БЫВАЕТ ОЧЕНЬ РАЗНЫМ

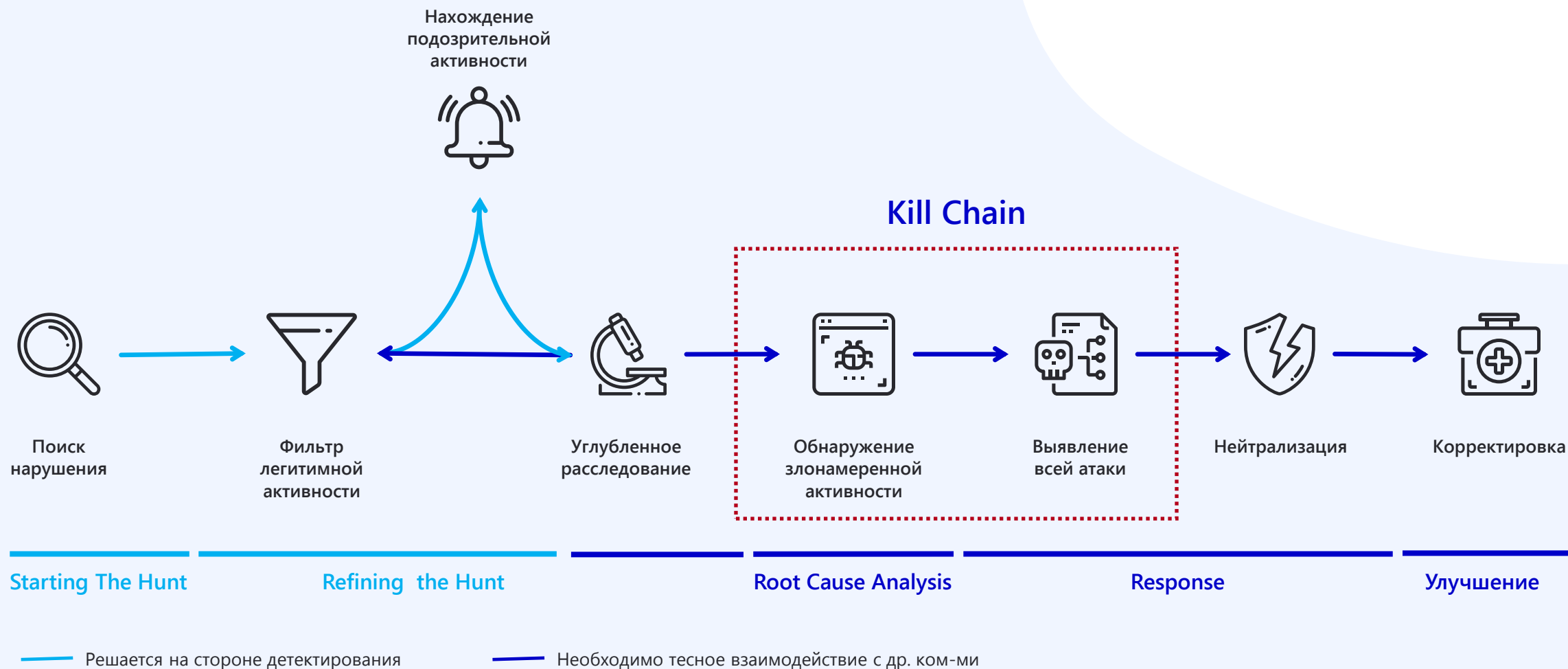


- **Preparation:** аудит-проектирование-настройка, war rooms, методики, playbooks
- **Detection:** обнаружение, **аналитика, расследование, уведомление**
- **Containment, Eradication & Recovery:** **сдерживание, нейтрализация, подавление, восстановление**
- **Post-Incident Activity:** **документирование, улучшение процессов, закрытие**

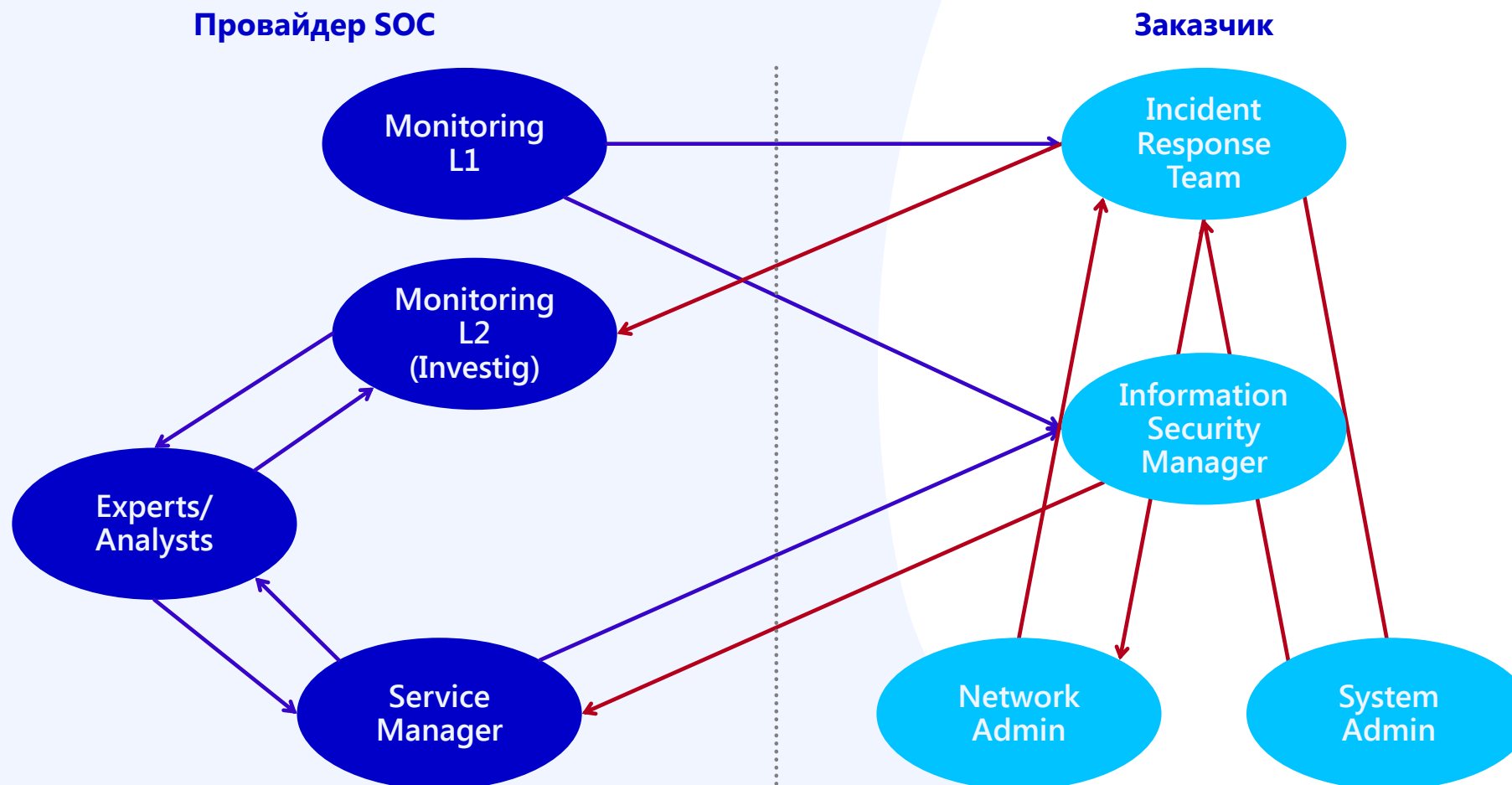
РЕАГИРОВАНИЕ

SP 800-61 Rev. 2 Computer Security Incident Handling —
<https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>, ISO/IEC 27035:2016

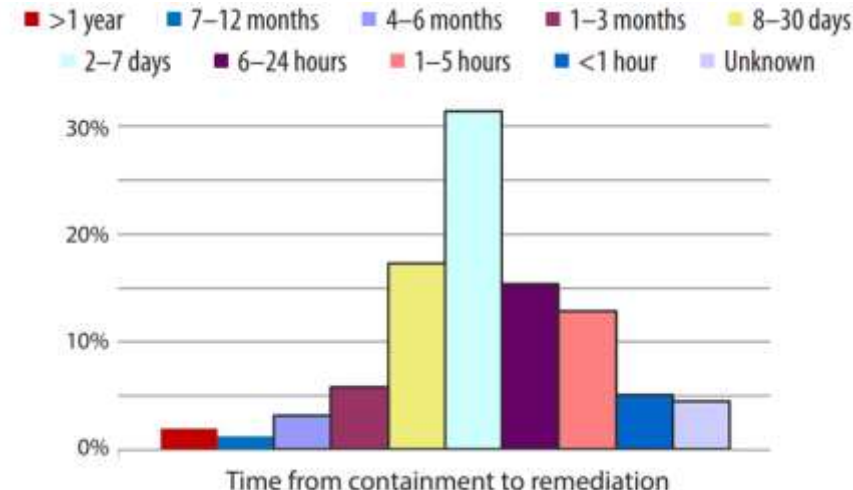
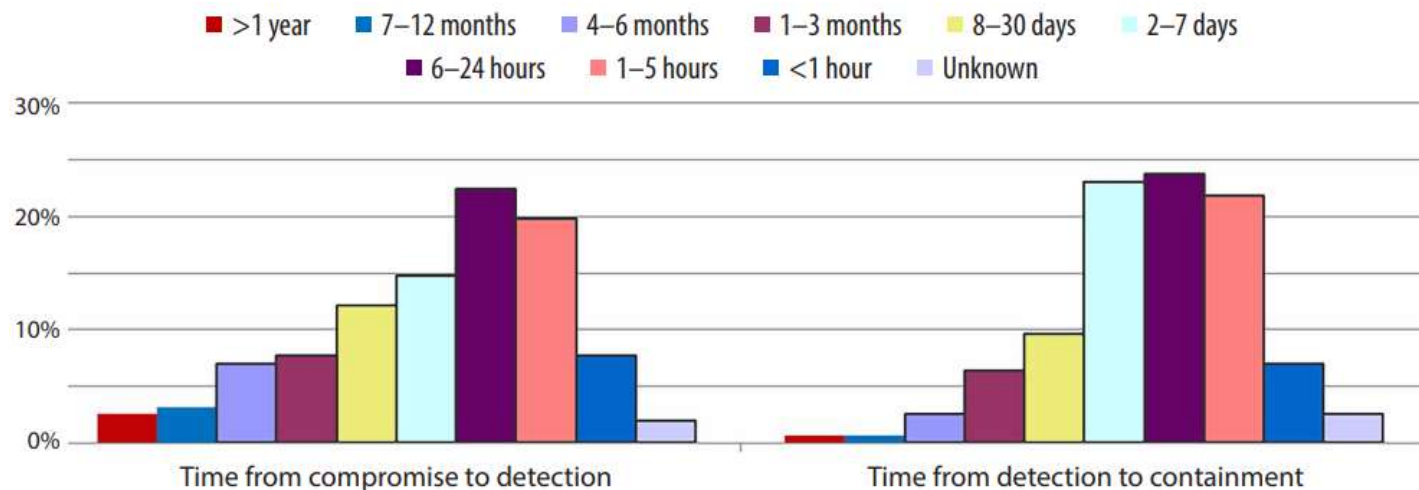
THREAT HUNTING — ПРОАКТИВНЫЙ ПОИСК И ОБНАРУЖЕНИЕ УГРОЗ



НЕСОГЛАСОВАННОСТЬ IR-ВЗАИМОДЕЙСТВИЯ НА ПРАКТИКЕ



К ЧЕМУ ПРИВОДИТ НЕСОГЛАСОВАННОСТЬ IR-ВЗАИМОДЕЙСТВИЯ



- От компрометации до обнаружения ~30% от месяца и более, ~15% от двух дней до недели
- От обнаружения до сдерживания ~20% от месяца и более, ~23% от двух дней до недели
- От сдерживания до восстановления ~30% от месяца и более, ~30% от двух дней до недели

Future SOC: SANS 2017 Security Operations Center Survey —

<https://www.sans.org/reading-room/whitepapers/analyst/future-soc-2017-security-operations-center-survey-37785>

ВЫВОДЫ



- Клиентам нужен сервис по многим процессам Incident Response
- Реагирование имеет много специализаций
- Мониторинг без реагирования теряет смысл
- Желательно минимизировать кол-во сторон в процессах

The background is a dark, textured surface with a blue curved line and a white curved line. The blue line starts from the top right and curves down towards the bottom right. The white line starts from the bottom right and curves up towards the bottom left. The overall color scheme is dark blue and black with some lighter blue and white accents.

JET CSIRT

JET COMPUTER SECURITY INCIDENT RESPONSE TEAM



ПОЧЕМУ CSIRT?

- Фактор фокуса на реагирование
- Фактор ширины покрытия разных процессов
- Сервисная ориентированность концепции CSIRT
- Потому что Jet moJet
(крупнейшие в стране и регионе ресурсы ИБ,
сервисная ориентированность компании)



НАШ ОПЫТ В АУТСОРСИНГЕ

- Более **170 специалистов** в команде и **400 специалистов** сервисного центра
- Более **200 заказчиков** техподдержки ИБ
- Около **50 заказчиков** аутсорсинга ИБ
- Более **20 лет** на рынке аутсорсинга ИБ
- Средняя длительность контракта **более 5 лет**
- Исполнимость SLA **99% кейсов**
- В **95% случаев** клиенты продлевают контракт

JET CSIRT. ЧЕМ ЕЩЕ РУКОВОДСТВУЕМСЯ ПОМИМО ОПЫТА



Выстраивание процессов



Команда и роли в ней



РС БР ИББС-2.5-2014

Технологии и архитектура



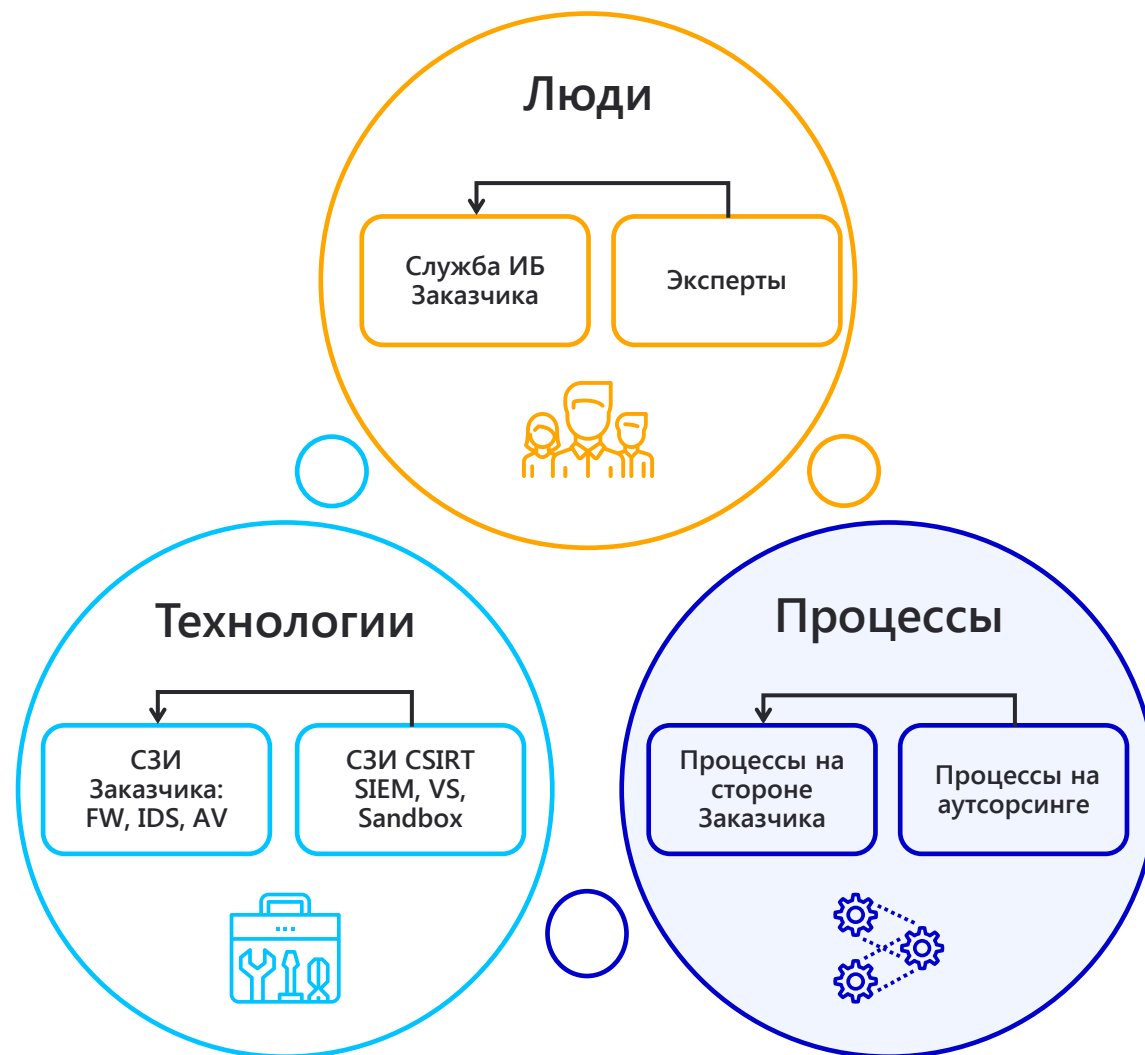
Метрики и оценка зрелости



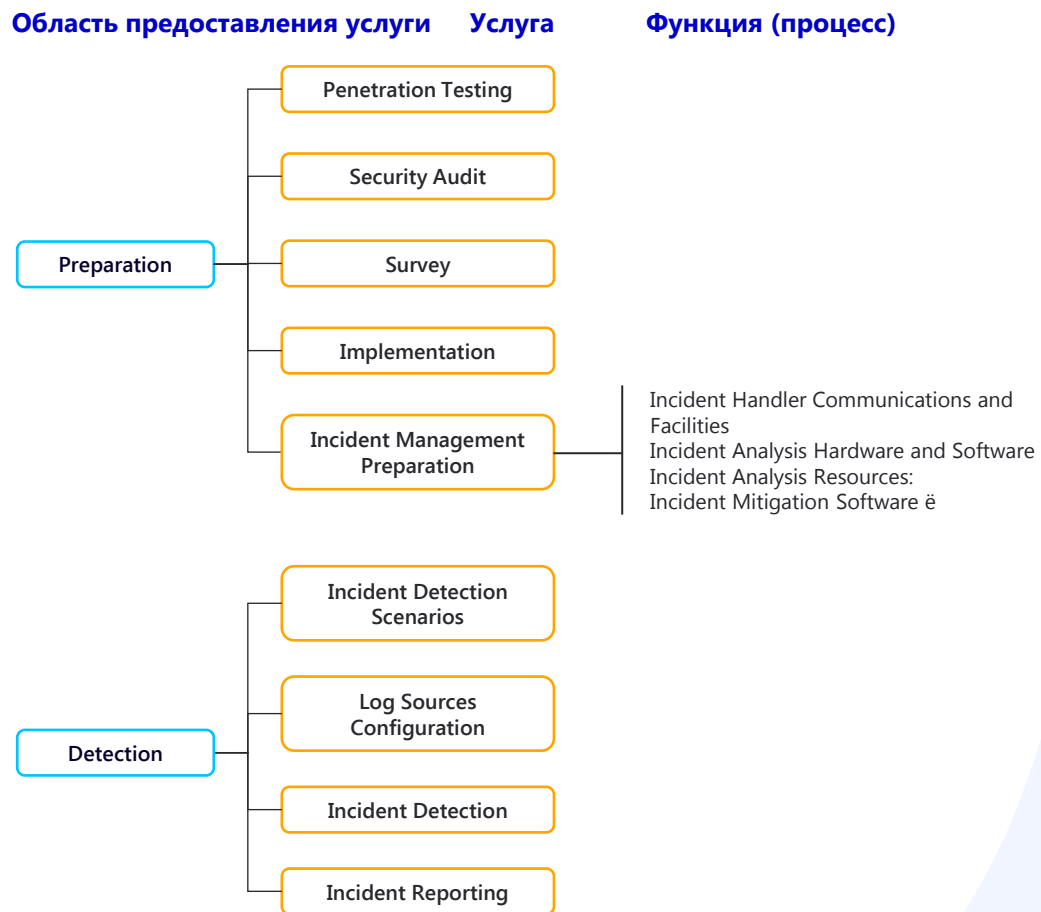
Соответствие

№99-ФЗ, №187-ФЗ, ПП-79, ПП-541, СТО БР ИББС-1.0-2014

ОБЩАЯ АРХИТЕКТУРА JET CSIRT



ПРОЦЕССЫ CSIRT В ТЕОРИИ

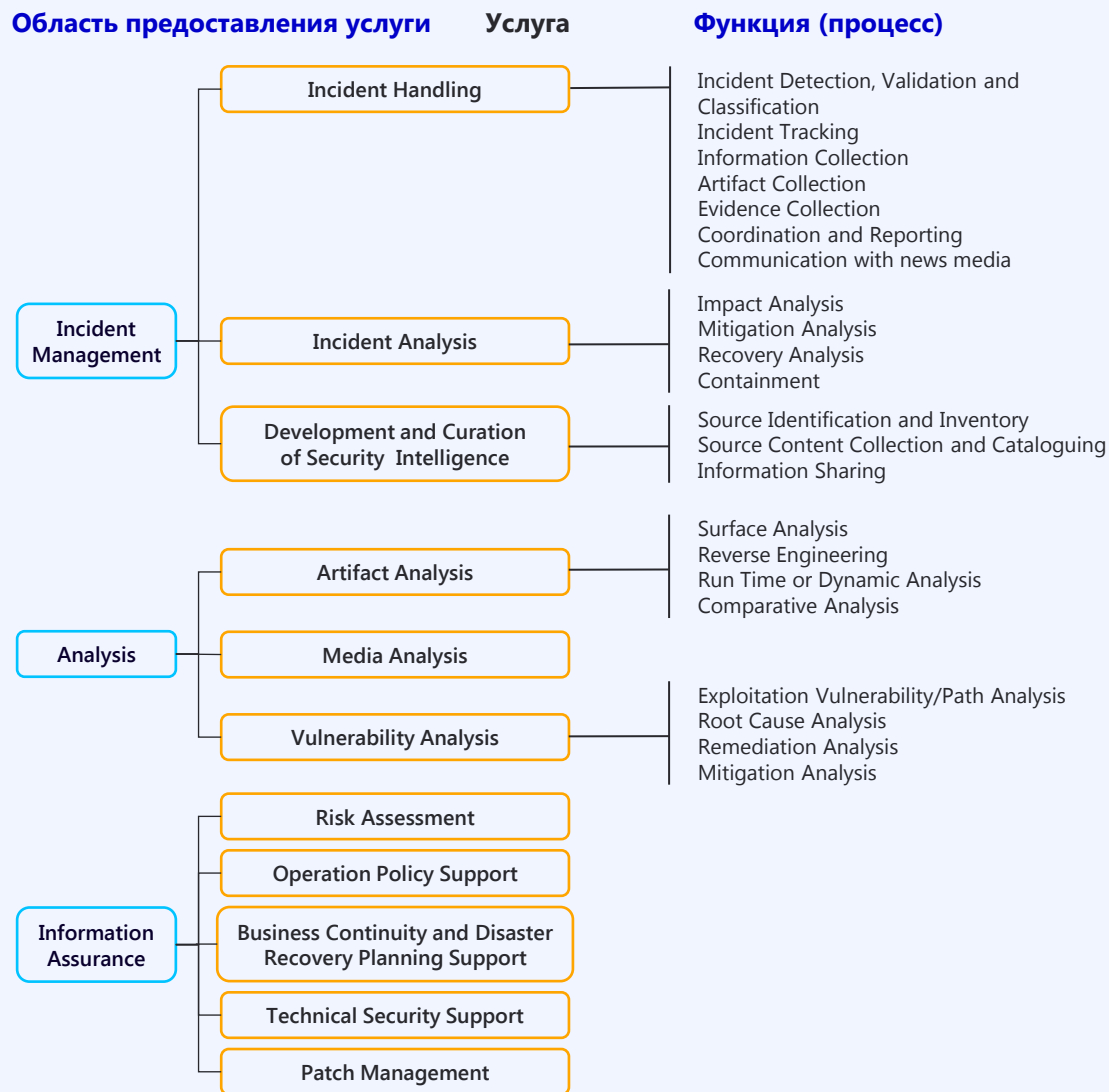


FIRST CSIRT Framework

https://www.first.org/education/csirt_service-framework_v1.1

SP 800-61 Rev. 2 Computer Security Incident Handling

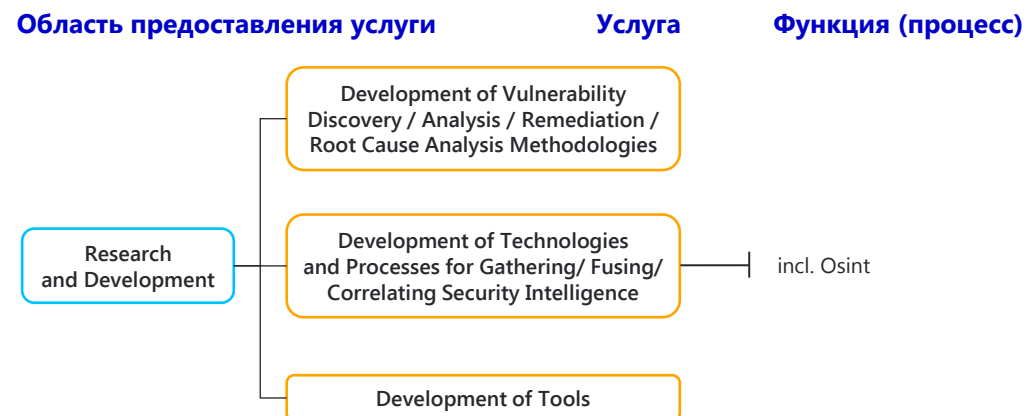
<https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>



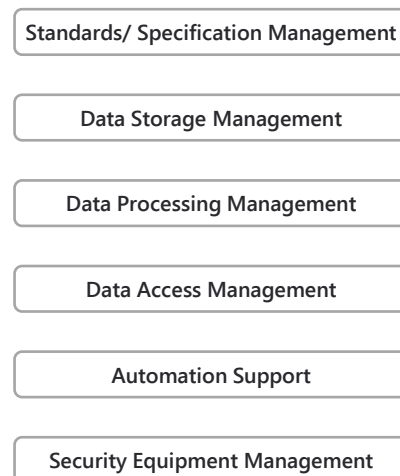
ПРОЦЕССЫ CSIRT В ТЕОРИИ



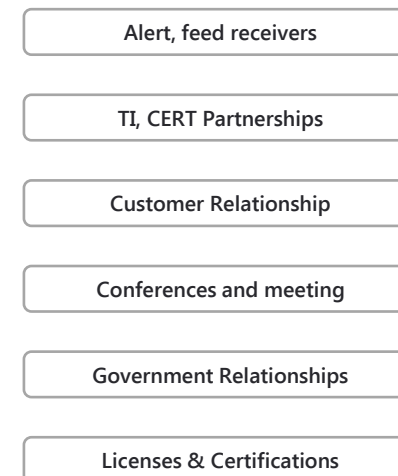
FIRST CSIRT Framework
https://www.first.org/education/csirt_service-framework_v1.1
 SP 800-61 Rev. 2 Computer Security Incident Handling
<https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>



Management



Relationship Management



JET CSIRT В СОСТАВЕ УСЛУГ ЦИБ



ОПЦИИ JET CSIRT



Стандарт

Мониторинг событий ИБ

Подключение
источников событий

Расследование инцидентов ИБ

Кибераналитика
по внешним угрозам

Техническое реагирование
Сдерживание и нейтрализация

Управление жизненным циклом
инцидента (IRP Jet Signal)

Расширенный

Управление уязвимостями

Разработка уникальных сценариев
выявления инцидентов

Техническое реагирование
Восстановление

Проактивный поиск
и обнаружение угроз

Администрирование СЗИ

Предоставление
СЗИ по подписке

Премиум

Изучение вредоносного кода

Аналитика по открытым
данным (OSINT)

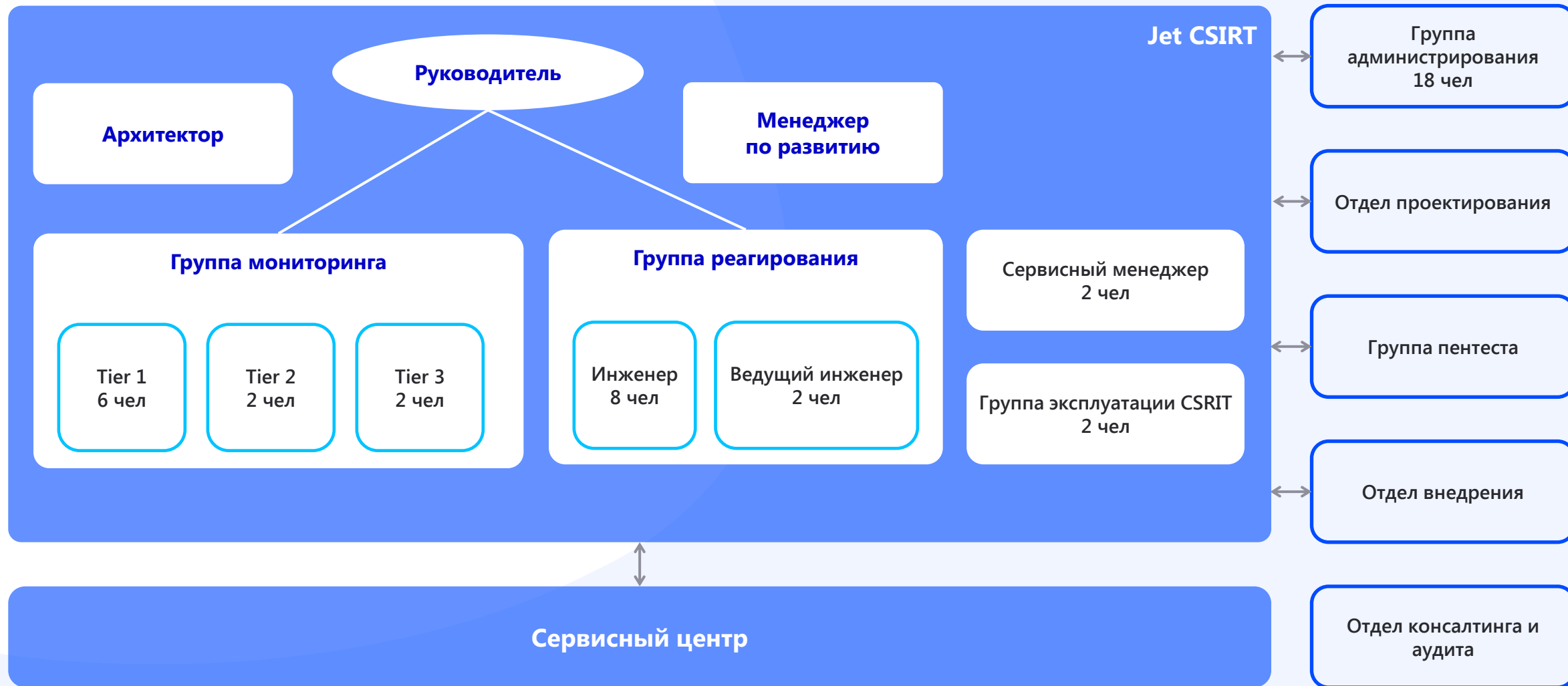
Бизнес-ориентированная
аналитика

Комплексное ИБ
консультирование

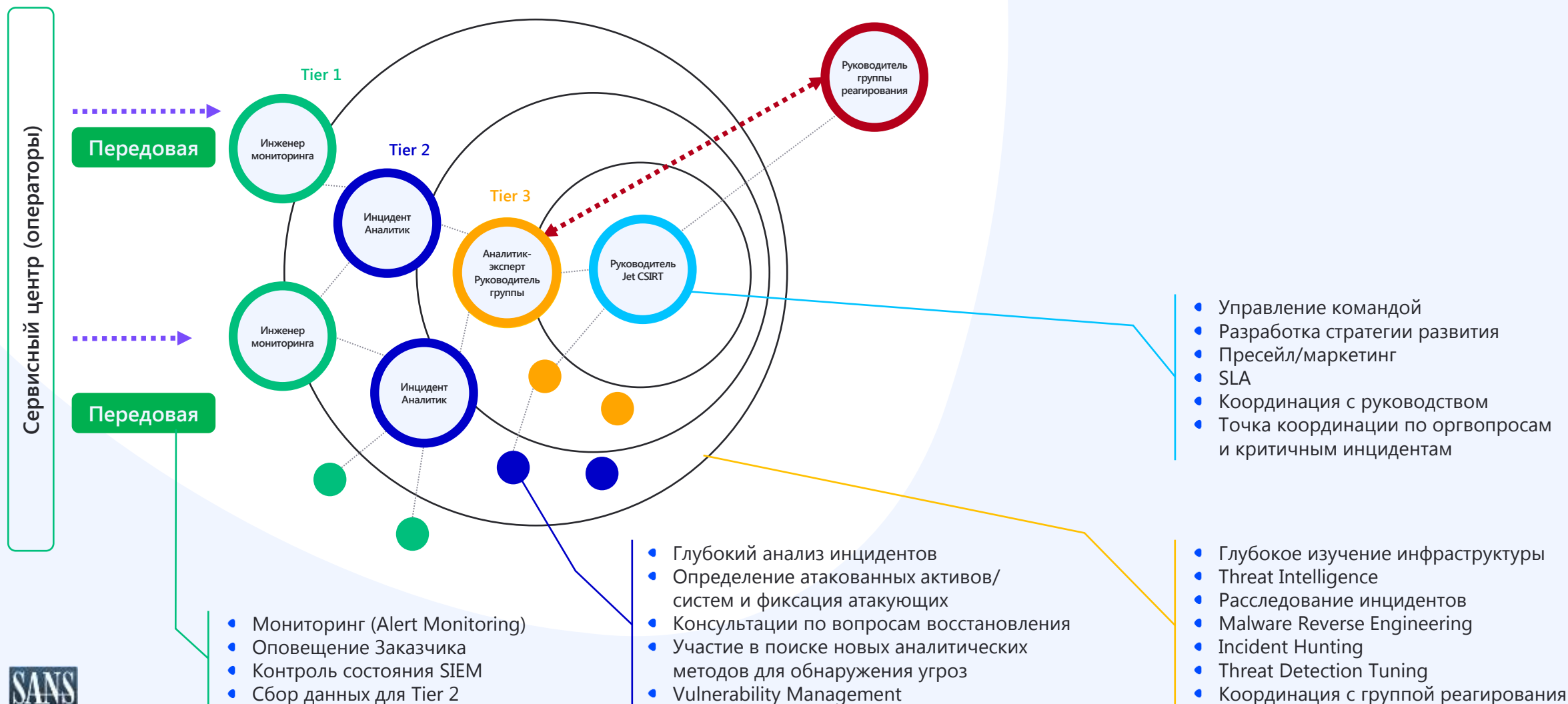
Аудит и анализ защищенности

Форензика

КОМАНДА JET CSIRT. ОРГСТРУКТУРА



КОМАНДА JET CSIRT. ГРУППА МОНИТОРИНГА



КОМАНДА JET CSIRT. ГРУППА РЕАГИРОВАНИЯ

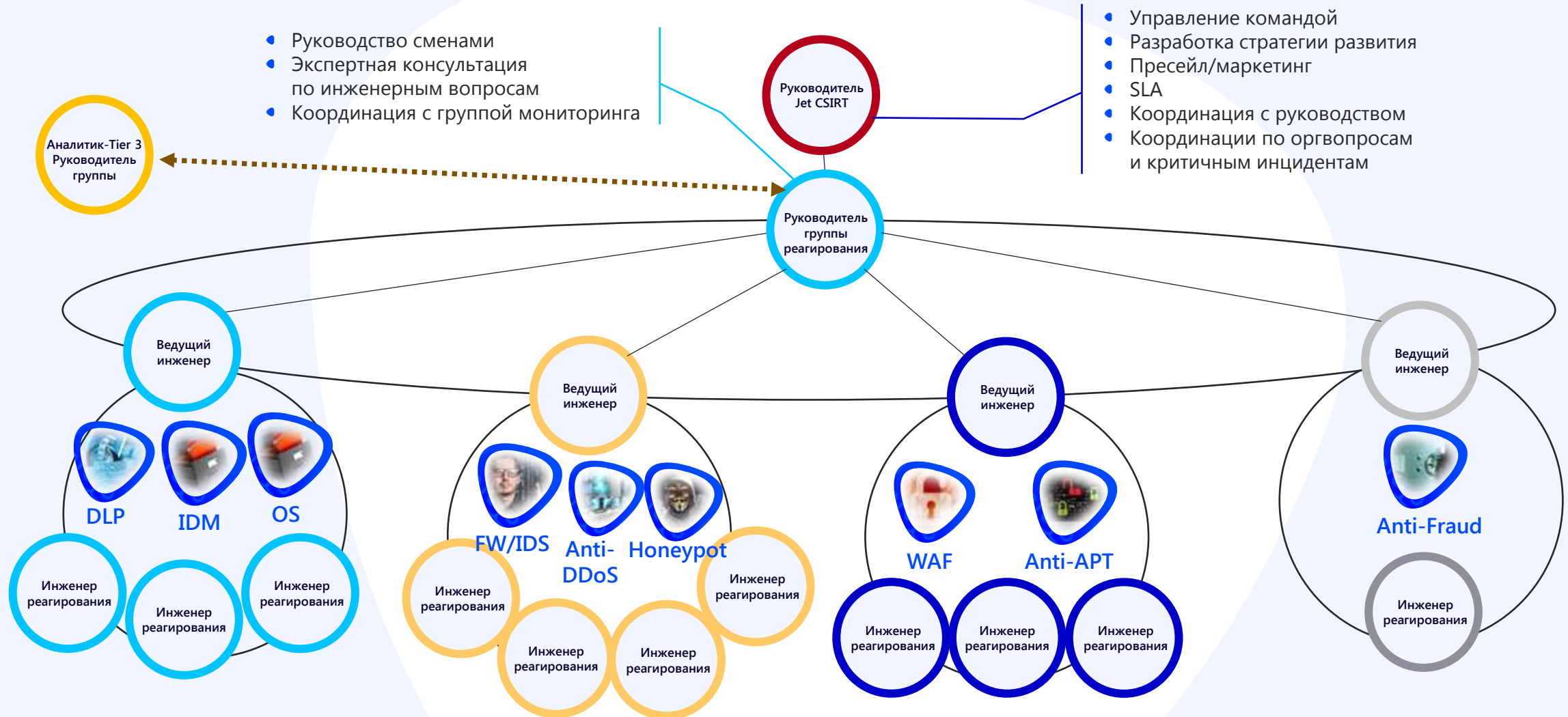


СХЕМА ПОДКЛЮЧЕНИЯ JET CSIRT. ВАРИАНТ 1

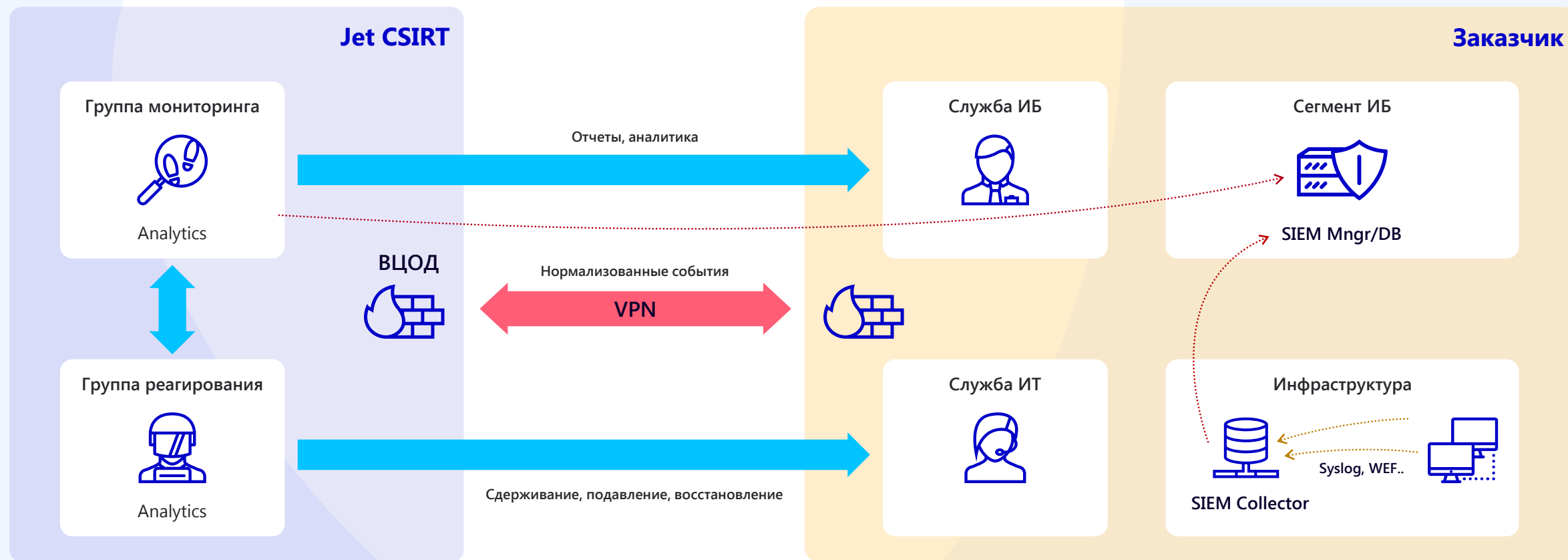
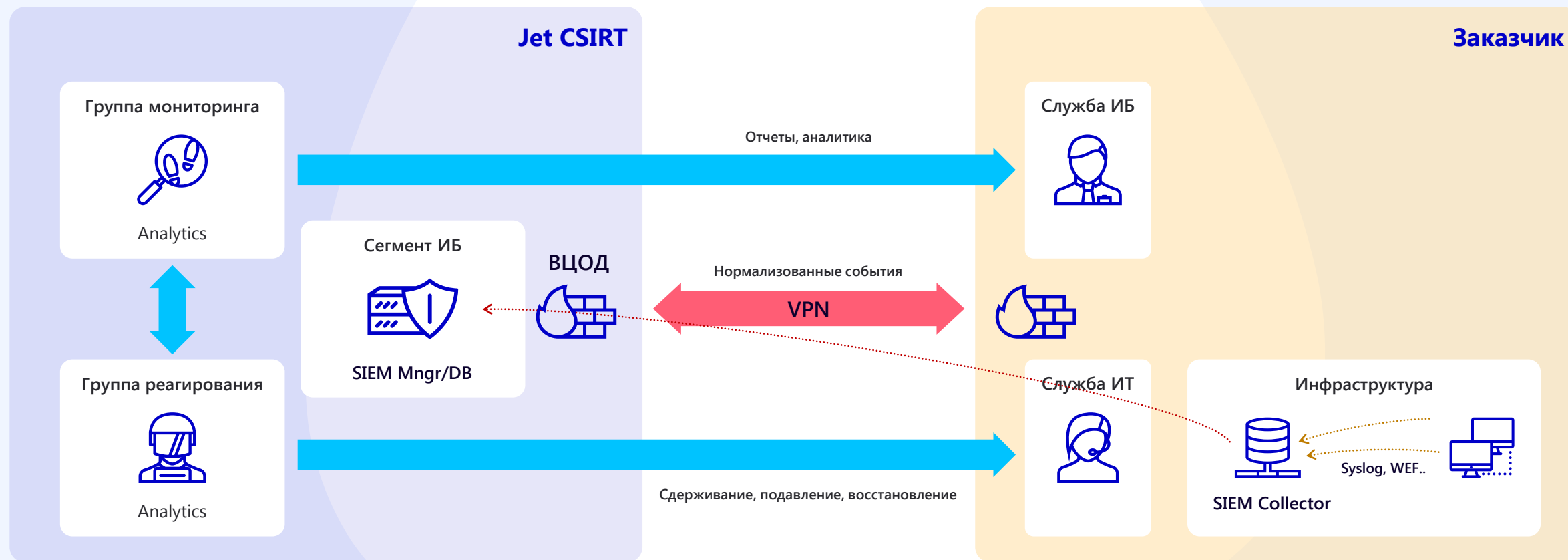


СХЕМА ПОДКЛЮЧЕНИЯ JET CSIRT. ВАРИАНТ 2



ИНСТРУМЕНТЫ JET CSIRT



Источники данных (телеметрия)

Сетевая инфраструктура

Сервера

Рабочие станции

Приложения

Средства защиты информации

Базы Данных

Мониторинг

FORTINET

POSITIVE
TECHNOLOGIES

MICRO
FOCUS

Radar

splunk

Управление жизненным циклом инцидента



bmc Remedy

Средства реагирования

cisco

paloalto
NETWORKS



Check Point
SOFTWARE INTEGRATION

McAfee

POSITIVE
TECHNOLOGIES

FORTINET

IMPERVA



radware

INFOWATCH

ARBOR
NETWORKS

SKYBOX
SECURITY

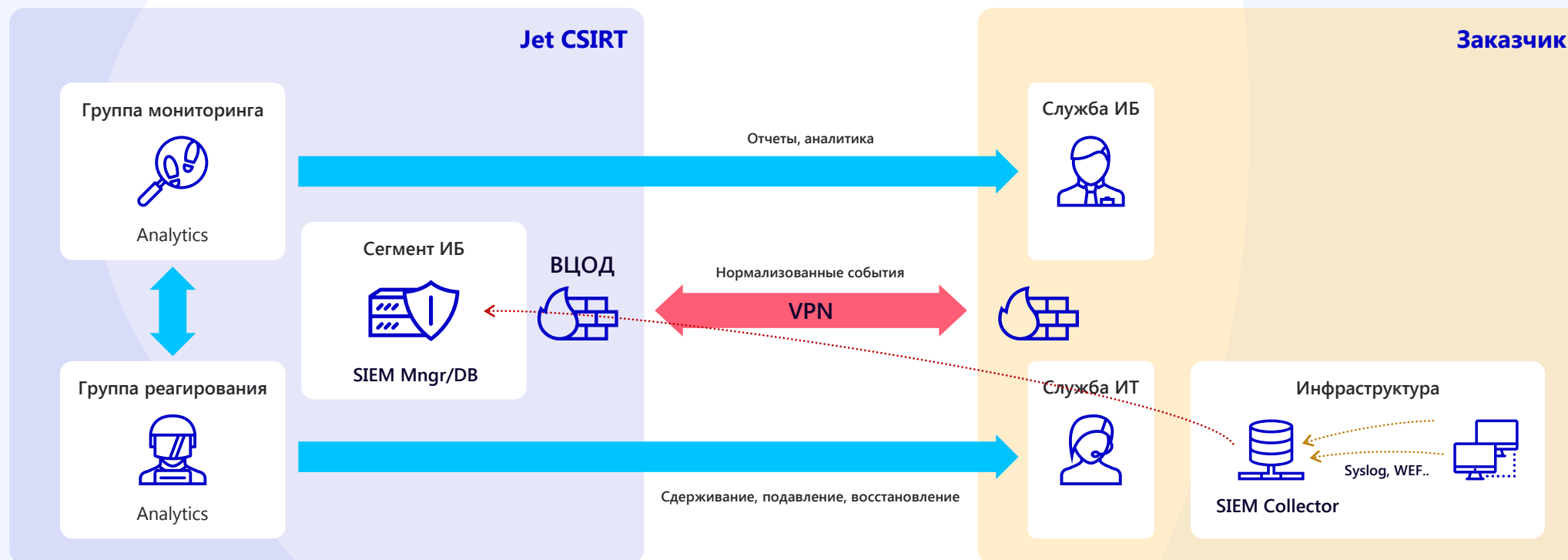
KASPERSKY

Средства визуализации



Qlik Sense

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)



31/05/2018

СПАСИБО ЗА ВНИМАНИЕ!

**Алексей
Мальнев**

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