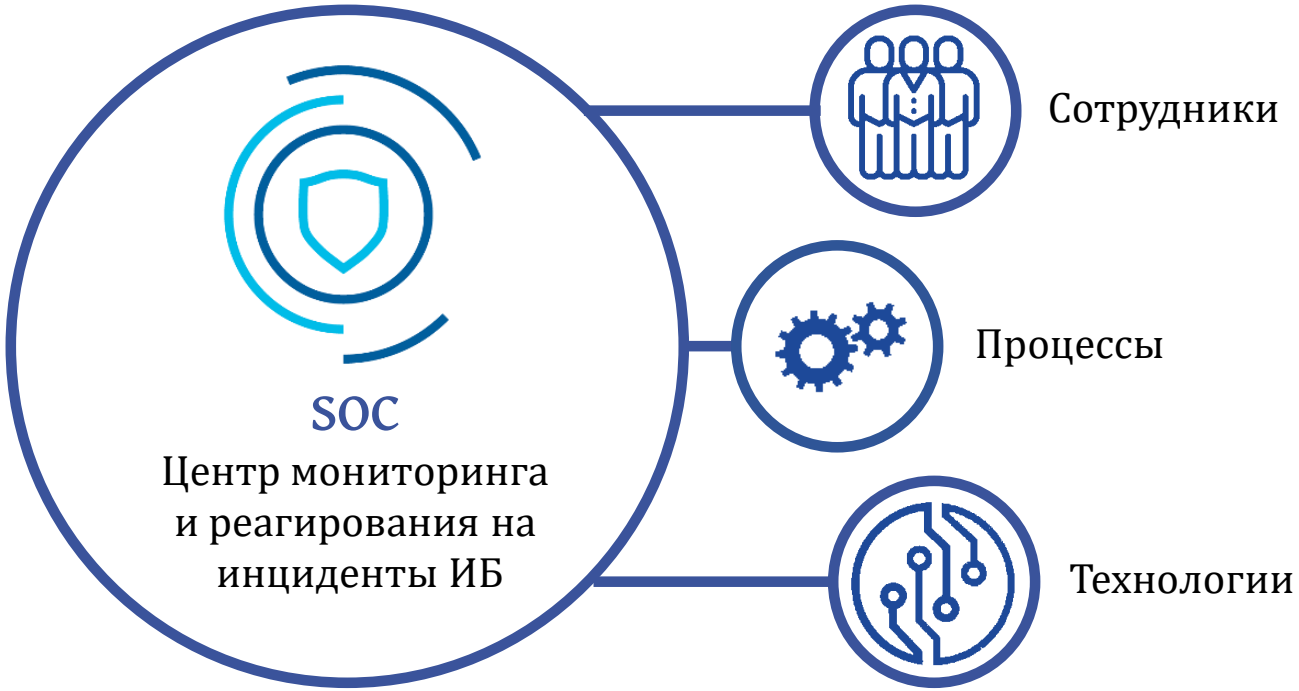
ISOC: МОНИТОРИНГ И РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИБ НА БАЗЕ PT MAXPATROL SIEM

ЗАЧЕМ НУЖЕН SOC



ЦЕЛИ

Снижение рисков хищения данных и денежных средств

Обеспечение непрерывности бизнеса

Снижение тяжести последствий инцидентов

РЕЗУЛЬТАТ

Выявление кибератак на ранних стадиях

Максимально быстрый разбор инцидентов в большом количестве информационных систем

ВАРИАНТЫ ПОСТРОЕНИЯ SOC

ВНУТРЕННИЙ SOC

Компания сама или с помощью консультантов строит процессы, обучает специалистов, создает и поддерживает SOC

PT MaxPatrol SIEM + Консалтинг

SOC AS SERVICE

Компания заключает договор с провайдером на сервис SOC с установленным SLA (Service Level Agreement)

ISOC

ГИБРИДНЫЙ SOC

Компания делегирует часть функций SOC сервис-провайдеру, остальные функции поддерживает самостоятельно

ISOC + PT MaxPatrol SIEM

ВАРИАНТЫ ПОСТРОЕНИЯ SOC. В ЧЕМ РАЗНИЦА

ВНУТРЕННИЙ SOC	SOC AS SERVICE	ГИБРИДНЫЙ SOC
Стоимость		
$$$ SIEM (Лицензия) $$$ Инфраструктура $$$ Внедрение системы $$$ Сервис 24/7	$ SIEM (Лицензия) $ Инфраструктура $$ Внедрение системы $$ Сервис 24/7	$$$ SIEM (Лицензия) $$$ Инфраструктура $$ Внедрение системы $$ Сервис 24/7
Скорость внедрения		
От 12 месяцев	3-4 месяца	6-12 месяцев
Преимущества		
Обработка и хранение событий на своей стороне	Гибкость в предоставлении сервиса	Обработка и хранение событий на своей стороне Гибкость в предоставлении сервиса

ПРЕИМУЩЕСТВА СЕРВИС-ПРОВАЙДЕРА

ЭКОНОМИЯ РЕСУРСОВ

Снижаются затраты (оборудование, персонал) на инфраструктуру для управления инцидентами*

РЕШЕНИЕ ПРОБЛЕМЫ КАДРОВ

Не нужно искать дорогих специалистов и обучать своих: сервис сопровождают профильные эксперты

ОЖИДАЕМЫЙ РЕЗУЛЬТАТ

Затраты и сроки внедрения сервиса заранее определены договором с провайдером

ФИКСИРОВАННЫЕ SLA

Клиент понимает, как быстро будет обработан инцидент или решен определенный вопрос

ОПЕРАТИВНАЯ РЕАКЦИЯ

Сервис предоставляется в режиме 24/7, поэтому вся информация об угрозах и уязвимостях поступает своевременно

ДОПОЛНИТЕЛЬНЫЕ СЕРВИСЫ

Сервис-провайдер может взять на сопровождение СЗИ и IT-инфраструктуру клиента

* В гибридном варианте на стороне клиента остается SIEM-система.
Для сбора и корреляции событий используется MaxPatrol SIEM (Positive Technologies)

ТЕХНОЛОГИЧЕСКАЯ ПЛАТФОРМА

MAXPATROL SIEM

Система мониторинга событий ИБ и выявления инцидентов
в реальном времени, разработанная компанией Positive Technologies

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА:

1. Полностью российская разработка, имеются сертификаты ФСТЭК РФ и Минобороны РФ, входит в реестр отечественного ПО
2. Своевременно детектирует новые типы угроз, получая обновления от экспертного центра безопасности Positive Technologies (PT ESC)
3. Лицензирование по количеству активов — а не по потоку событий — позволяет менять источники для мониторинга, выбирать наиболее важные и подключать новые без дополнительных затрат
4. Автоматически строит топологию сети, что помогает лучше понимать защищаемую инфраструктуру, упрощает расследование инцидентов
5. Большое количество дашбордов позволяет получать самую разнообразную информацию о работе системы

Positive Technologies

25% российского рынка SIEM

занял MaxPatrol SIEM
в 2017 году (исследование IDC)

100 проектов внедрения

MaxPatrol SIEM и SIEM LE
реализовано с 2015 года

230 преднастроенных источников

Бесплатное подключение других бизнес-систем, в том числе специфических и самописных

ТРЕБОВАНИЯ

ТРЕБОВАНИЯ К PT MAXPATROL SIEM

ВЕРСИЯ

Поддерживается версия 21 и выше

ЛИЦЕНЗИИ

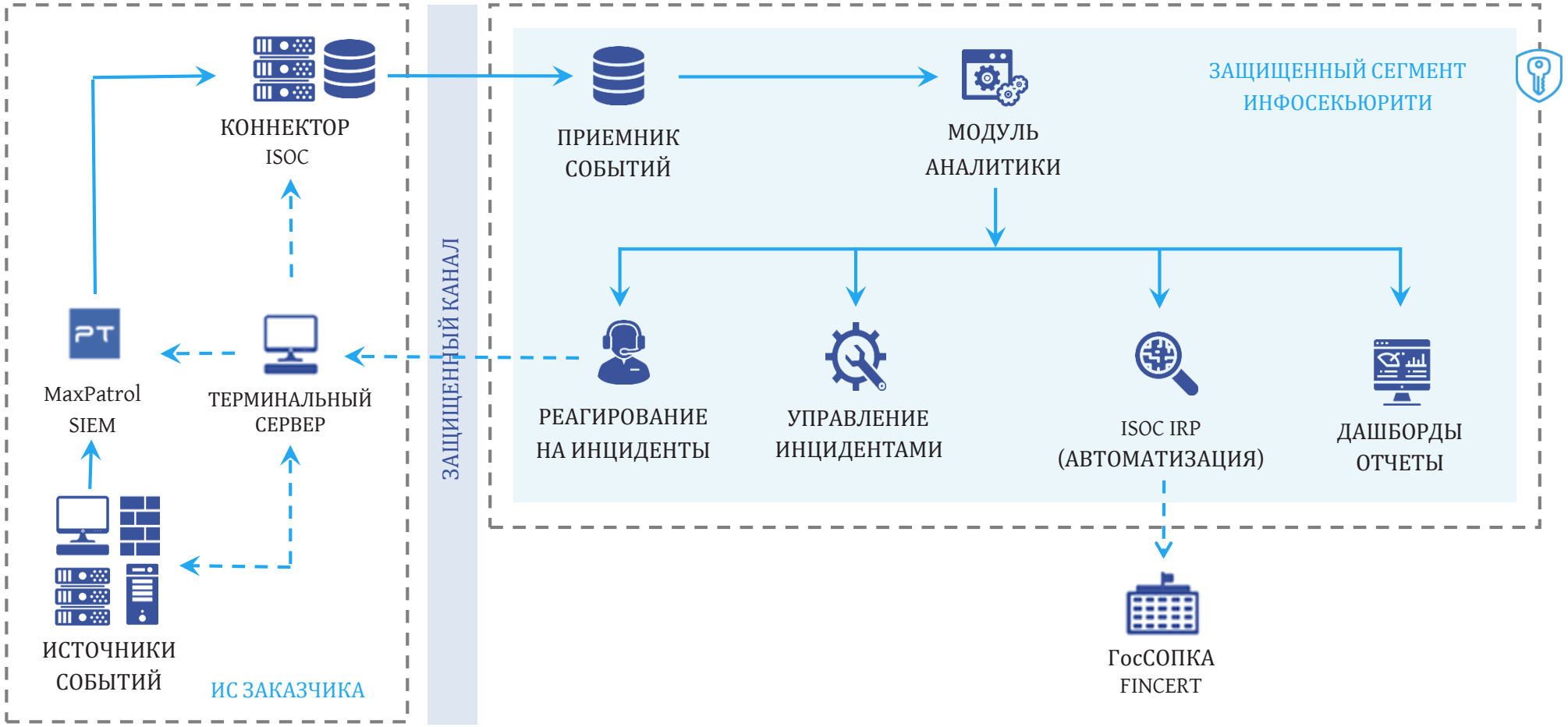
Необходимы лицензии:

- MP SIEM Server
- MP SIEM Log Collector

ПОДДЕРЖКА

Необходима вендорская поддержка PT MaxPatrol SIEM: коннекторы должны обновляться

АРХИТЕКТУРА ВЗАИМОДЕЙСТВИЯ



ПОДКЛЮЧЕНИЕ К ГОССОПКА

СОГЛАШЕНИЕ МЕЖДУ НКЦКИ И «ИНФОСЕКЬЮРИТИ» ПОЗВОЛЯЕТ НАМ ВЫСТУПАТЬ В РОЛИ КОРПОРАТИВНОГО ЦЕНТРА ГОССОПКА КЛАССА «А»

ФУНКЦИИ ЦЕНТРА ГОССОПКА	СООТВЕТСТВУЮЩИЕ УСЛУГИ
Разработка регламентирующих документов	Консалтинг
Взаимодействие с НКЦКИ	ISOC: передача информации через коннектор
Анализ событий Прием сообщений о возможных инцидентах Регистрация инцидентов Составление перечня инцидентов Эксплуатация средств обнаружения и реагирования Ликвидация последствий Анализ результатов ликвидации последствий Установление причин инцидентов (расследование)	ISOC: сервисы мониторинга, расследования, реагирования на инциденты
Подготовка предложений по повышению уровня защищенности	
Инвентаризация Выявление уязвимостей Анализ угроз Составление и актуализация перечня угроз	Сервис управления уязвимостями

INFOSECURITY
a Softline company

КАК РАБОТАЕТ СЕРВИС ISOC

МОЖНО ВЫБРАТЬ НЕОБХОДИМЫЙ НАБОР УСЛУГ В ЗАВИСИМОСТИ ОТ СВОИХ ПОТРЕБНОСТЕЙ

ЭКСПЕРТИЗА И ПРОЦЕССЫ ISOC

ЭФФЕКТИВНОСТЬ РАБОТЫ SOC ОБУСЛАВЛИВАЕТСЯ РЯДОМ УНИКАЛЬНЫХ ХАРАКТЕРИСТИК КОМПАНИИ «ИНФОСЕКЬЮРИТИ»

8 лет управления инцидентами ИБ

Участник FIRST, статус CERT

Соглашение НЦКИ позволяющее выступать в роли корпоративного центра ГосСОПКА класса «А»

База знаний и use case по обработке инцидентов

Использование актуальных данных Threat Intelligence

Опыт предоставления сервиса компании с количеством сотрудников более 30.000

Более 30 сотрудников, участвующих в мониторинге и реагировании, и более 60 профильных экспертов

INFOSECURITY
a Softline company

КОМАНДА ISOC

В команде **более 30 экспертов**, занимающихся непосредственно мониторингом и расследованиями инцидентов.

Кроме того, с ними в непрерывном режиме взаимодействуют **более 60 профильных инженеров** по различным направлениям информационной безопасности.

ПЕРВАЯ ЛИНИЯ

Мониторинг и оповещение 24/7

ВТОРАЯ ЛИНИЯ

Анализ инцидентов 24/7

ТРЕТЬЯ ЛИНИЯ

Расследования 8/5

СЕРВИСЫ ИБ

Реагирование на инциденты 24/7

АНАЛИТИКА

Правила реагирования

РАЗРАБОТКА

Платформа и автоматизация

ЭКСПЛУАТАЦИЯ ISOC

Сопровождение инфраструктуры ISOC

ЭТАПЫ ПОДКЛЮЧЕНИЯ*

1 АНАЛИТИКА И КОНСАЛТИНГ

- Анализ подключенных источников (ОС, СУБД, ПО, СЗИ, сетевое оборудование)
- Оптимизация правил корреляции PT MaxPatrol SIEM для соответствия нашим политикам реагирования

2 ОРГАНИЗАЦИЯ КАНАЛОВ СВЯЗИ

- Получение доступов
- Настройка защищенного сетевого канала
- Настройка защищенного почтового канала

3 ПОДГОТОВКА ИНФРАСТРУКТУРЫ

- Настройка коннектора к PT MaxPatrol SIEM в инфраструктуре заказчика
- Подключение дополнительных источников
- Настройка оповещений и доступа к дашбордам

4 СОГЛАСОВАНИЕ ВЗАИМОДЕЙСТВИЯ

- Определение схемы подключения новых источников
- Определение схем оповещения об инцидентах и эскалации

5 СОГЛАСОВАНИЕ SLA

- Установление режима работы
- Определение приоритета и скорости реагирования на инциденты
- Определение параметров и сроков отчетности

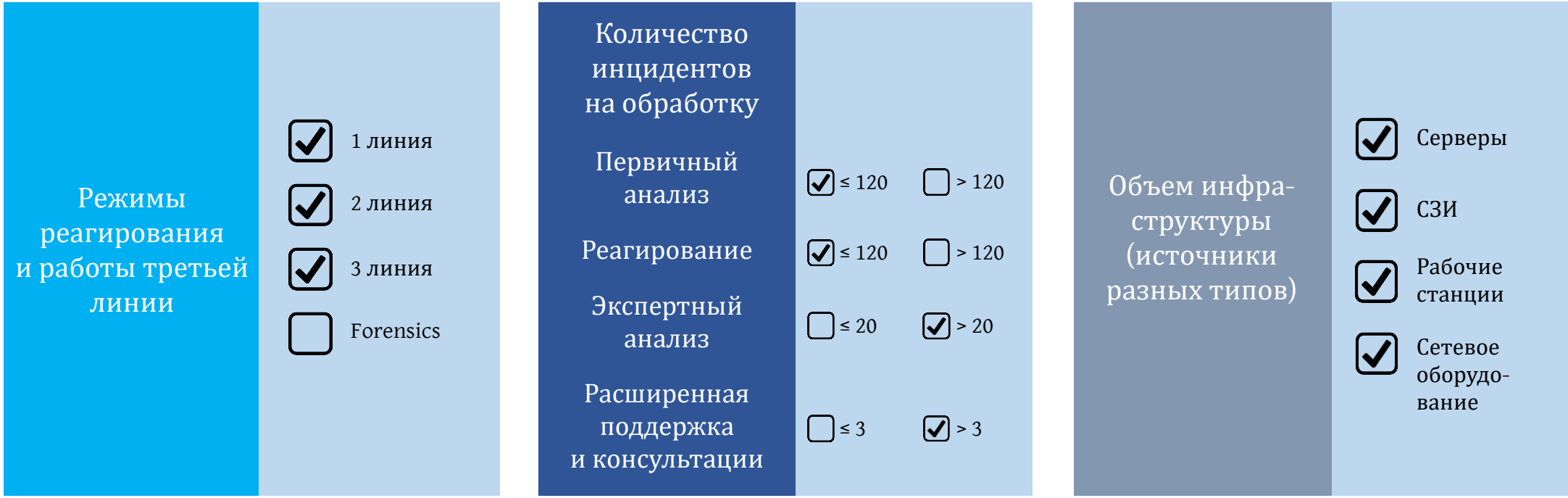
6 ВВЕДЕНИЕ В ЭКСПЛУАТАЦИЮ

- Тестирование
- Запуск мониторинга событий и реагирования на инциденты

* При условии наличия внедренной MaxPatrol SIEM у клиента. Мы также можем оказать услуги по развертыванию MaxPatrol SIEM в рамках отдельного проекта.

ЦЕНООБРАЗОВАНИЕ

СТОИМОСТЬ СЕРВИСА ISOC РАССЧИТЫВАЕТСЯ ИСХОДЯ ИЗ НЕСКОЛЬКИХ ПАРАМЕТРОВ



РЕЖИМ **ОБРАБОТКА** **МАСШТАБ**

INFOSECURITY
a Softline company

in4security.com