

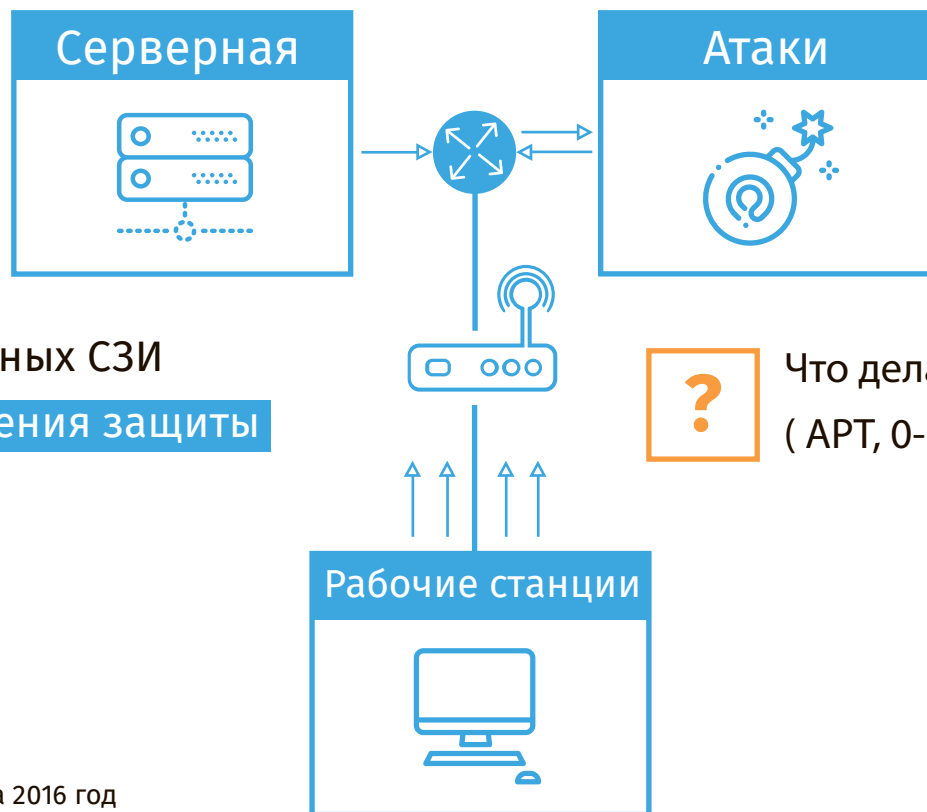
«Песочница» как сервис

www.itsoc.ru

www.infosec.ru

Проблематика. Worldwide

Схема ИТ-сети



При правильно настроенных СЗИ
можно добиться **обеспечения защиты**



Что делать с оставшимися? **5%**
(APT, 0-day)

* согласно отчетам компании Gartner за 2016 год

Практика «ИНФОРМЗАЩИТЫ»

Тестирование защищенности сети телеком оператора с использованием сетевых «Песочниц» (декабрь 2016 г.)

1. Тестирование с использованием синтетических образцов вредоносного кода.

	Веб	Почтовый трафик
На входе для анализа:	55 зловредов	15 зловредов
Обнаружено сигнатурными СЗИ	23 зловредов	1 зловред
Поступило в «Песочницу»	32 зловредов	14 зловредов

Обнаружено «Песочницей» (лучший результат)	29 из 32	9 из 14
Существующие СЗИ заказчика	0 из 32	0 из 14

2. Тестирование на реальном интернет-трафике пользователей Заказчика ИЗ.



На входе для анализа —
реальный трафик за 1 месяц.

72
угрозы

зафиксировано «Песочницей»-
суммарно за один месяц (не
заблокированные и не зафиксиро-
ванные существующими
сигнатурными средствами
антивирусной защиты)

Тестируемые решения:



Практика «ИНФОРМЗАЩИТЫ»

Анализ входящего трафика интегратора с включением сетевой «Песочницы» (август – сентябрь 2018 г.)

Тестируемые решения:



1. Тестирование с использованием синтетических образцов вредоносного кода.

2. Тестирование на реальном веб-трафике.

На входе для анализа	25 зловредов	реальный веб-трафик за 1 месяц от ~ 350 АРМ
Поступило на обработку в «Песочницу»	25 зловредов	9 637 файлов
Результат «Песочницы»	25 угроз (обнаружены все 25 зловредов)	10 угроз 0,1% Суммарно за один месяц «Песочницей» зафиксировано (не заблокированные и не зафиксированные существующими сигнатурными средствами антивирусной защиты компании) от общего числа обработанных файлов «Песочницей».

НЕ ВСЕ ГОТОВЫ
ПРИНИМАТЬ РИСКИ

ПРОПУСКА В СЕТЬ
НЕИЗВЕСТНЫХ ВИРУСОВ И АТАК

ЭФФЕКТИВНА ТЕХНОЛОГИЯ «ПЕСОЧНИЦЫ»

Внедрение «Песочницы»

Какие есть варианты



Внедрение собственной «песочницы»



Долгосрочное вложение в создание и развитие технологии
(модернизация, эксплуатация и поддержание компетенций).



Подключение к PUBLIC Services производителей



Доступ к услуге глобальных ЦОД **за территорией РФ.**



Подключение к сервису локальной «Песочницы» ИНФОРМЗАЩИТЫ



С применением MSSP программ **Check Point;**



Доступ к расширенной экспертизе и компетенциям ИЗ;



Индивидуальный подход к подключению;



Доступ к услуге на **территории РФ.**



Быстрое подключение/
отключение услуги



Четкое планирование
расходов



Не требуется специальных
знаний для управления
сервисом



Доп. услуги по требованию



Отсутствие эксплуатационных
издержек



Низкая стоимость владения

Сервис «Песочница» от ИНФОРМЗАЩИТЫ

Варианты подключения



Check Point
Security Gateway
ИСПОЛЬЗУЕТСЯ



CP SG

Для отправки файлов нужно:

- приобрести подписку NGTX;
- активировать модуль Threat Emulation;
- настроить отправку файлов для эмуляции в «песочницу» ИЗ (te.itsoc.ru).



Check Point
Security Gateway
НЕ ИСПОЛЬЗУЕТСЯ



Virtual Gateway

Для отправки файлов нужно:

- приобрести подписку NGTX (vSEC);
- развернуть виртуальный МЭ CP NGTX (vSEC);
- настроить отправку файлов для эмуляции в «песочницу» ИЗ (te.itsoc.ru).



APM

Для отправки файлов нужно:

- приобрести подписку на CP SandBlast Agent;
- развернуть агент на APM пользователя;
- настроить функцию отправки файлов для эмуляции в «песочницу» ИЗ (te.itsoc.ru).

Что предлагаем

1. **24x7x365
в облаке IZ**

Сервис эмуляции угроз

Услуги удаленной эмуляции и извлечения угроз.

Включает в себя:

- ✓ Удаленное подключение к изолированной среде IZ ThreatCloud Emulation
- ✓ Запуск до 25 000 файлов/месяц в изолированной среде
- ✓ Анализ и блокирование подозрительных файлов
- ✓ Предоставление безопасной копии подозрительного документа
- ✓ Оповещение администратора офицера ИБ Заказчика
- ✓ Предоставление базовых отчетов о количестве подозрительных файлов



2. **до 1000
правил**

Настройка политик МЭ

Услуги оптимизации политики Threat Prevention

Включает в себя:

- ✓ Анализ текущих правил МЭ
- ✓ Разработка рекомендаций на основе «best practice»
- ✓ Помощь в настройке правил МЭ согласно рекомендациям
- ✓ Документирование правил



3. **24x7x365
реакция 2 часа**

Первичный Forensic Analysis

Проведение базовой аналитики по инциденту.

Включает в себя:







- ✓ Автоматическое расследование угроз (инцидентов) средствами CP SandBlast Agent
- ✓ Предоставление отчета об инциденте администратору/офицеру ИБ Заказчика
- ✓ Предоставление базовых рекомендаций по реагированию на инцидент

Стоимость эмуляции файлов

Количество файлов в месяц:

Количество АРМ:

Стоимость в месяц:

	до 20 000 	до 100	от 25 800 ₺*
	до 25 000 	до 200	от 30 000 ₺*
	до 50 000 	до 350	от 56 000 ₺*

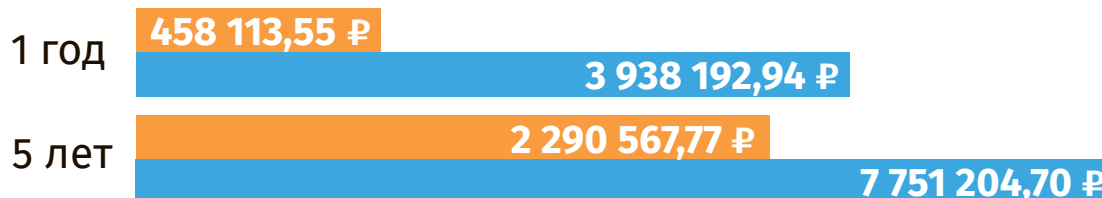
* Стоимость указана с НДС.
Предложение действительно до 31 декабря 2018 г.

Сравнение стоимости

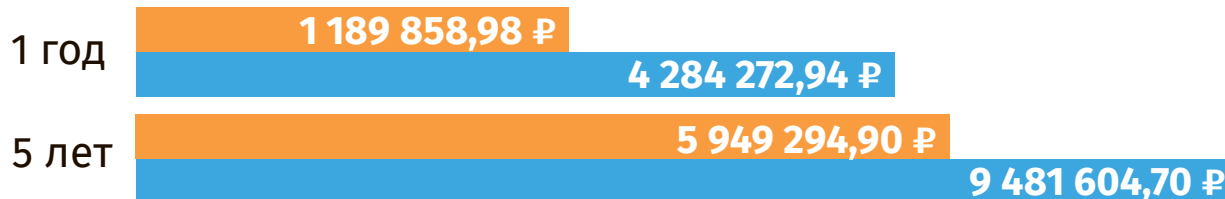
С локацией в РФ



до **20 000** файлов в месяц
(~ до **100** АРМ)



до **50 000** файлов в месяц
(~ до **350-400** АРМ)



Предполагается наличие CP Security Gateway
с подпиской NGTP

■ Подключение к облачному сервису «ИНФОРМЗАЩИТЫ»
■ Внедрение собственного решения

Стоимость включает расширение до NGTX и обработку файлов «песочницей». НДС включен.

тестирование

понимание отраслевых
потребностей

необходимые технические средства

опыт и экспертиза

compliance

стенды

СЕРВИСНЫЕ РЕШЕНИЯ ДЛЯ РЕАЛЬНОЙ БЕЗОПАСНОСТИ



+7 (495) 980-2345

высококвалифицированные
эксперты

проверка эффективности



info@itsoc.ru

комплексный анализ требований
и подбор сервисных решений

эксплуатация СЗИ