Информзащита
Сервисный центр

Сервис удаленной эмуляции угроз

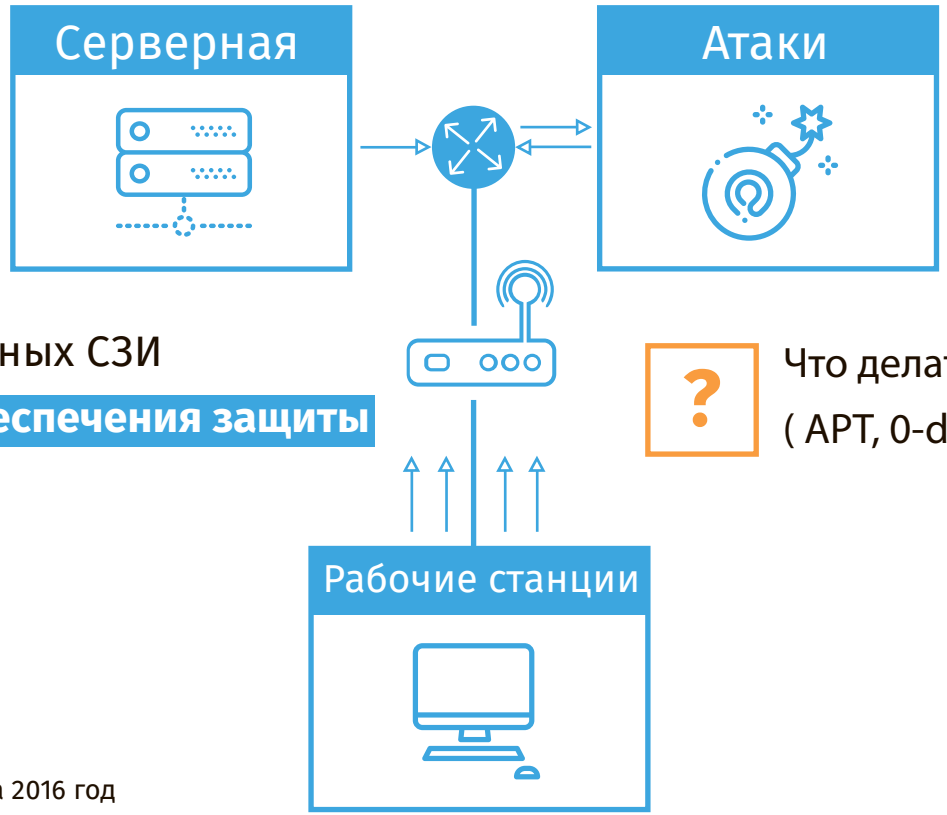
«песочница» как сервис

www.itsoc.ru

www.infosec.ru

Проблематика. Worldwide

Схема ИТ-сети



При правильно настроенных СЗИ
можно добиться **95%* обеспечения защиты**

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

* согласно отчетам компании Gartner за 2016 год

Информзащита
Сервисный центр

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 зафиксированные существующими сигнатурными средствами антивирусной защиты)

https://www.anti-malware.ru/compare/Test_protection_against_targeted_attacks_comparison_network_sandboxes#part5

Тестируемые решения:

Check Point SOFTWARE TECHNOLOGIES LTD

FireEye™

TREND MICRO™

Информзащита
Сервисный центр

Практика «ИНФОРМЗАЩИТЫ»

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

Тестируемые решения:

Check Point
SOFTWARE TECHNOLOGIES LTD

	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%** от общего числа обработанных файлов «песочницей»). Суммарно за один месяц «песочницей» зафиксировано (не заблокированные и не зафиксированные существующими сигнатурными средствами антивирусной защиты компании)

Информзащита
Сервисный центр

НЕ ВСЕ ГОТОВЫ ПРИНИМАТЬ РИСКИ ПРОПУСКА В СЕТЬ НЕИЗВЕСТНЫХ ВИРУСОВ И АТАК

ЭФФЕКТИВНА ТЕХНОЛОГИЯ «ПЕСОЧНИЦЫ»

**помогает предотвратить атаки,
направленные на корпоративную инфраструктуру
из недоверенных источников**

Информзащита
Сервисный центр

«Классические СЗИ» & «песочница»

Классическая защита
реализуется с использованием:
IPS, AntiVirus, AntiBot решений

+

Проверка входящего трафика «песочницей»

- **Работа только с известными сигнатурами**
- **Работа только с известными атаками**
- **НЕТ защиты от таргетированных, целенаправленных, 0-day атак**

- **Открытие (или запуск) подозрительного файла в изолированной среде и наблюдение за его поведением**
- **Вердикт о признании безопасности файлов (заблокировать или пропустить)**

Комплексный подход в решении вопросов информационной безопасности — верный путь к ЗАЩИТЕ ОТ ЦЕЛЕВЫХ АТАК и УГРОЗ «НУЛЕВОГО ДНЯ»

Информзащита
Сервисный центр

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

Информзащита
Сервисный центр

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 АРМ пользователя;**
- **настроить функцию отправки файлов для эмуляции в «песочницу» ИЗ (te.itsoc.ru).**

Информзащита
Сервисный центр

Что предлагаем

1. 24x7x365 в облаке ИЗ

Сервис эмуляции угроз

Услуги удаленной эмуляции и извлечения угроз

Включает в себя:

- Удаленное подключение к изолированной среде ИНФОРМЗАЩИТЫ
- Запуск до 50 000 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

Информзащита
Сервисный центр

тестирование

понимание отраслевых потребностей

необходимые технические средства

опыт и экспертиза

compliance

СЕРВИСНЫЕ РЕШЕНИЯ ДЛЯ РЕАЛЬНОЙ БЕЗОПАСНОСТИ

стенды

+7 (495) 980-2345

info@itsoc.ru

высококвалифицированные эксперты

проверка эффективности

комплексный анализ требований и подбор сервисных решений

эксплуатация СЗИ