ПОДСЫПЬ ПЕСОЧКА

ВАРИАНТЫ ПЕСОЧНИЦ И ИХ ИСПОЛЬЗОВАНИЕ В СИСТЕМЕ ЗАЩИТЫ

Александр Тварадзе
IT Security Director
Axoft Azerbaijan

AXOFT

ПЕСОЧНИЦУ НАДО?

- Прежде чем попасть на анализ в «песочницу», файлы с зловредным кодом проходили анализ средствами защиты, с использованием сигнатурных и репутационных механизмов
- Архивация файла с использованием форматов RAR, ZIP, 7-ZIP, в том числе с защитой архива паролем
- Почтовые сообщения с веб-ссылками на вредоносный файл, в том числе с использованием «коротких» URL (URL shortening);
- Загрузка зловредного кода по частям
- Шифрование (AES) вредоносного кода (payload) макроса в документах Microsoft Word.

Электронная почта

Интернет

ПЕСОЧНИЦУ НАДО?

Стандарт	Найдено	Не найдено	Эффективность
Электронная почта	1	14	6%
Интернет	23	32	41%

Песочницы	Найдено	Не найдено	Эффективность
Электронная почта	29	3	90%
Интернет	9	5	64%

ВИДЫ ПЕСОЧНИЦ

- Расположение «облако»

- Расположение «хост»

- «Все в одном»

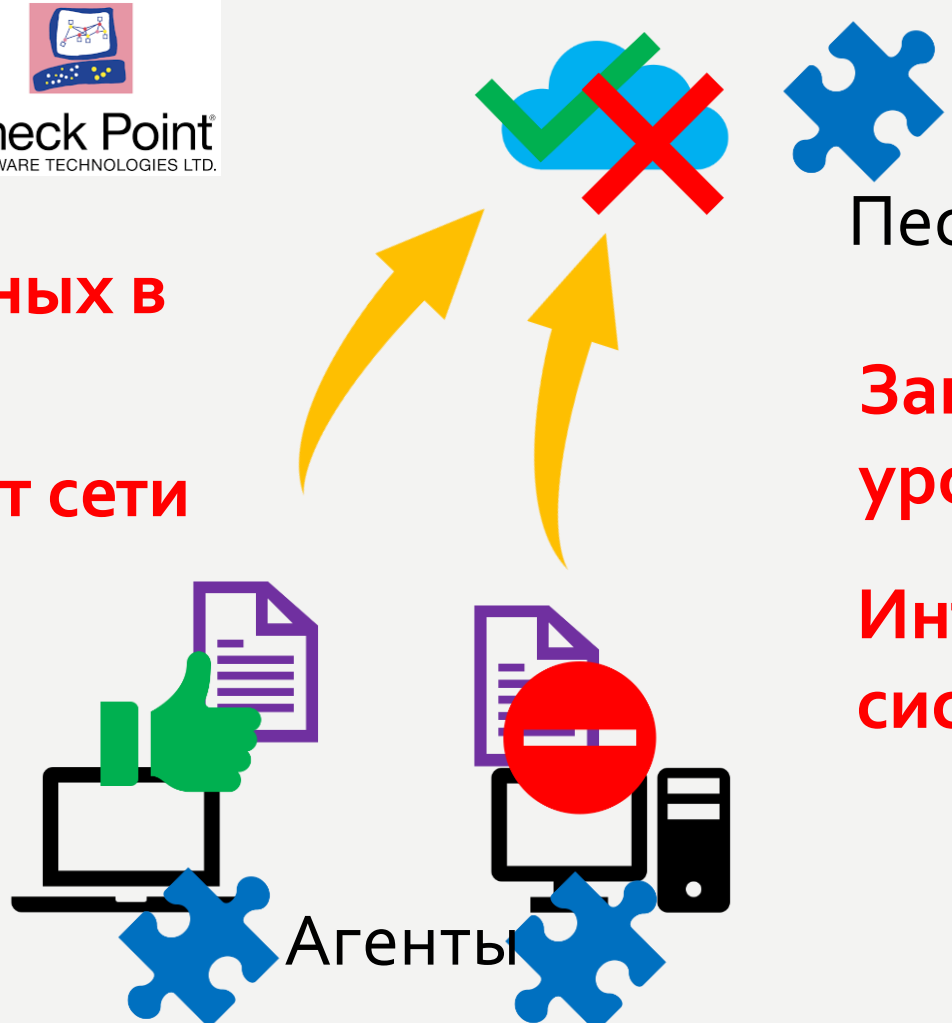
- Специализированные и универсальные

DDI– анализ трафика
DDEI – эл. почта
DDAN– универсальная

NX– анализ трафика
EX – эл. почта

ПЕСОЧНИЦЫ И АРХИТЕКТУРА ИТ БЕЗОПАСНОСТИ

- Облако и агенты



Передача данных в облако

Зависимость от сети Интернет

Защита только на уровне станции

Инъекция в ОС и системы

ПЕСОЧНИЦЫ И АРХИТЕКТУРА ИТ БЕЗОПАСНОСТИ

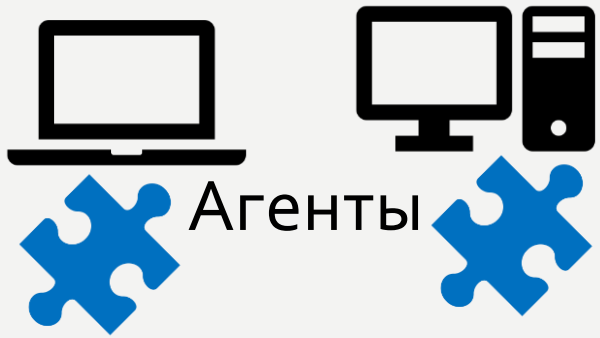
- UTM и агенты

Check Point
SOFTWARE TECHNOLOGIES LTD.

Единая точка отказа при атаке

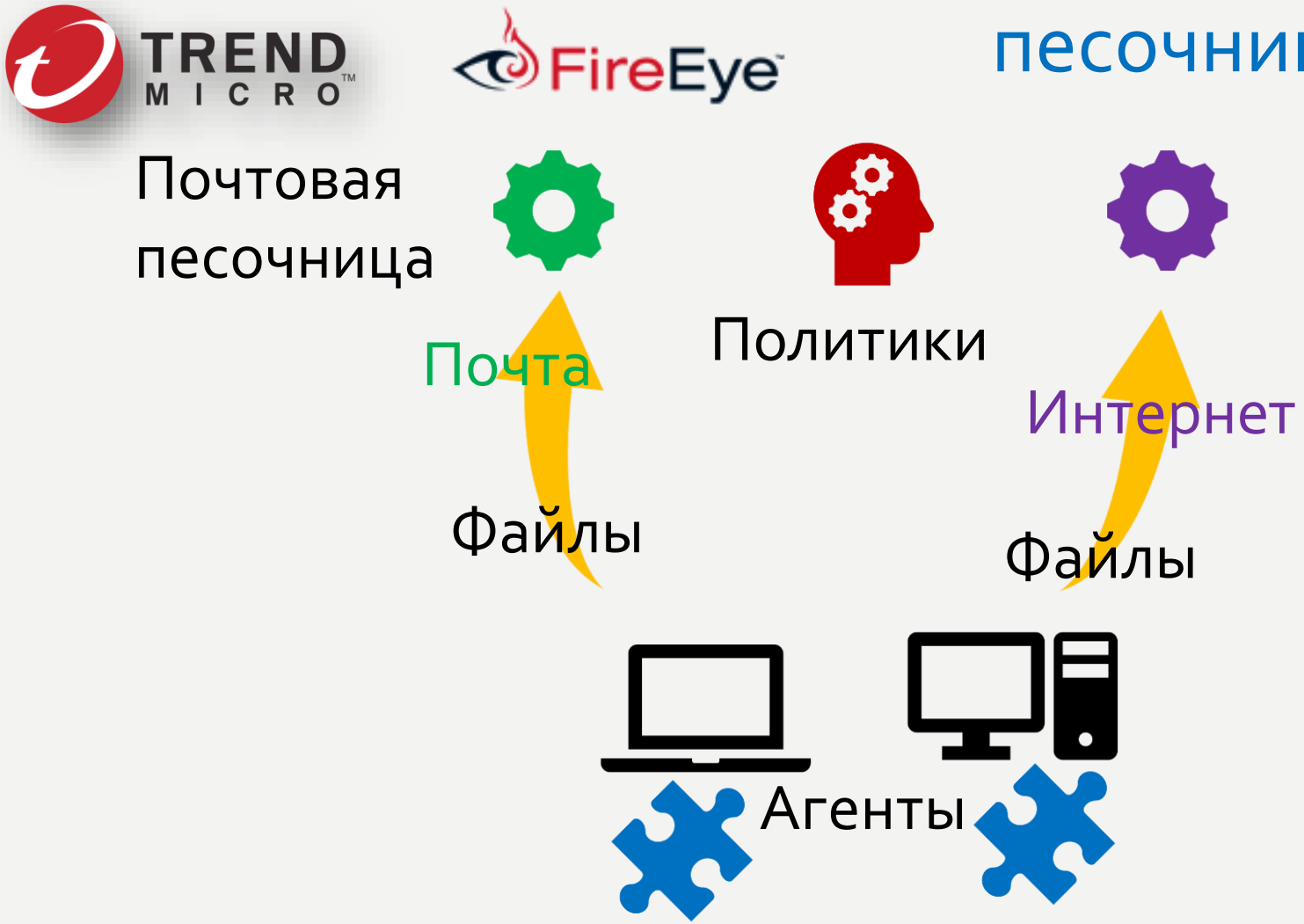
Избыточность

Неполная защита трафика



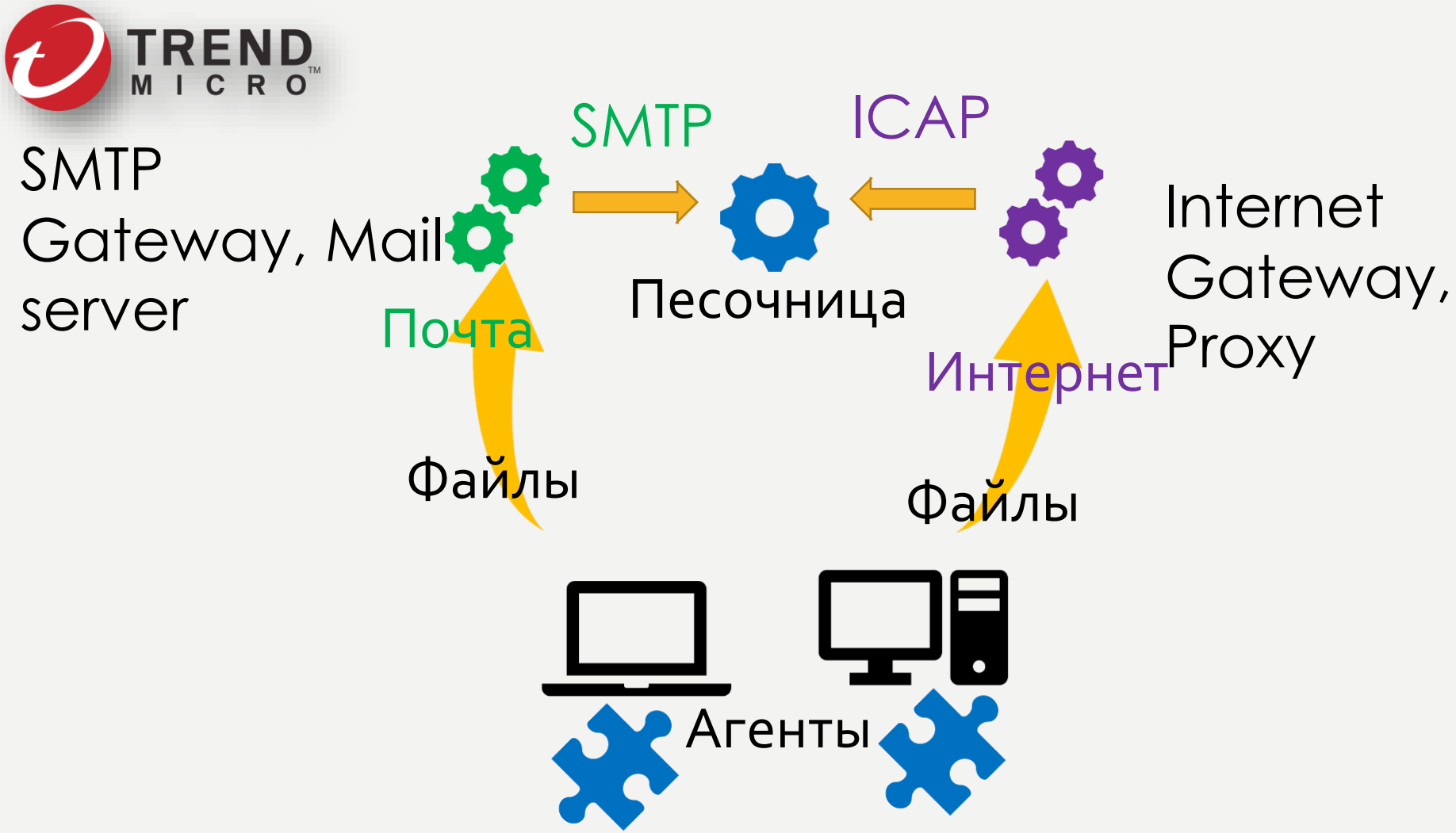
ПЕСОЧНИЦЫ И АРХИТЕКТУРА ИТ БЕЗОПАСНОСТИ

- Специализированные песочницы



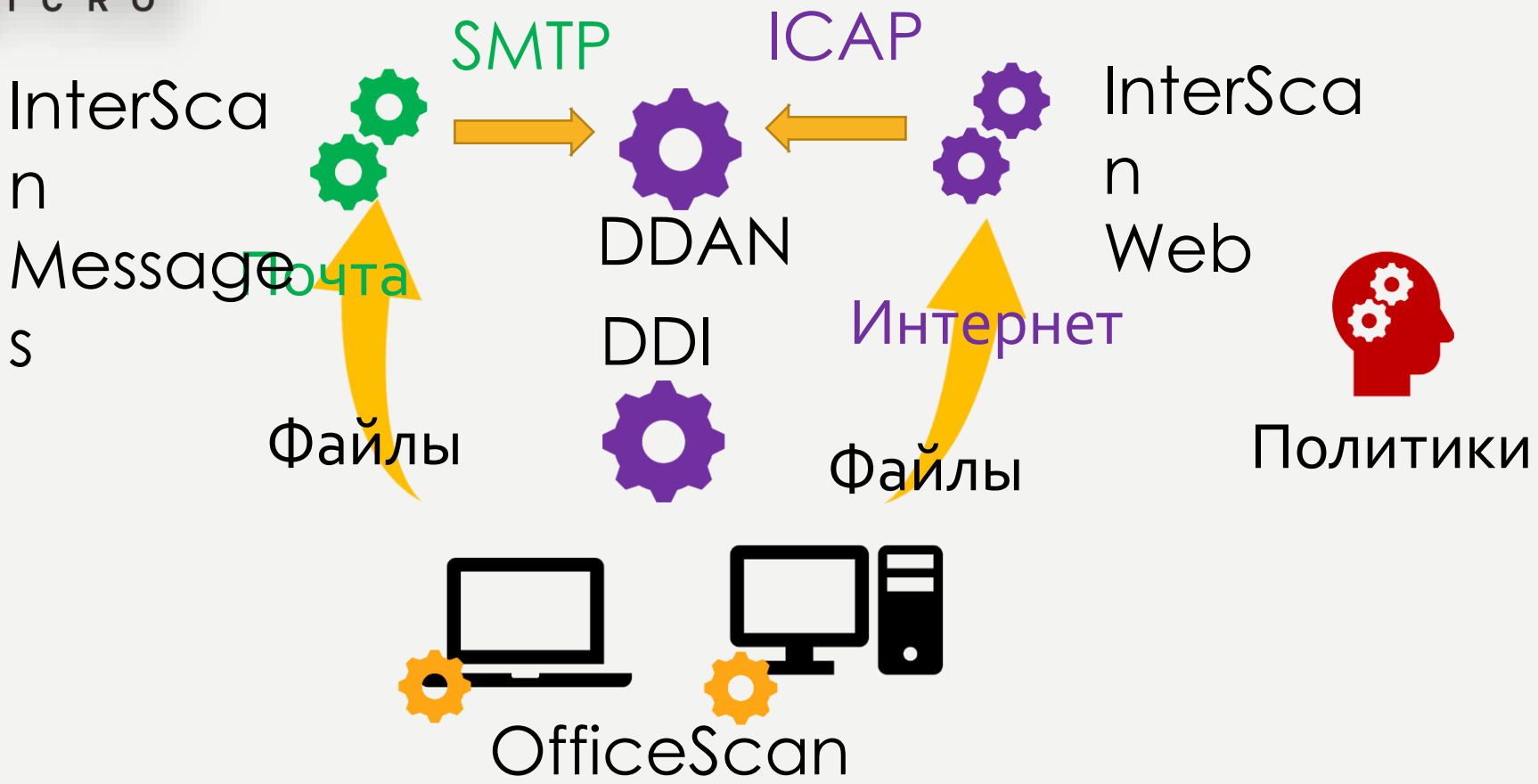
ПЕСОЧНИЦЫ И АРХИТЕКТУРА ИТ БЕЗОПАСНОСТИ

- Универсальная песочница



ПЕСОЧНИЦЫ И АРХИТЕКТУРА ИТ БЕЗОПАСНОСТИ

- Полное покрытие



ВНУТРЕННЯЯ АРХИТЕКТУРА

Преднастроенные образы

Произвольные образы

Обнаружение песочниц по серийным номерам образов

Приближенность к реальным станциям

Реальные рабочие серийные номера организаций

Реальные образы станций

ВНУТРЕННЯЯ АРХИТЕКТУРА

	FireEye	TREND MICRO	Check Point SOFTWARE TECHNOLOGIES LTD.
Произвольный образ	✗	✓	✗
MacOS	✓	✗	✗
Win Server	✗	✓	✗
Критерии файлов	✓	✓	✗
Ручной критерий	✓	✓	✗
Запароленные архивы	✓	✓	✓

СПАСИБО ЗА ВНИМАНИЕ

Александр Тварадзе
IT Security Director
Axoft Azerbaijan