11.01.2017

TRAPX SECURITY

Система быстрого обнаружения направленных атак и 0-day угроз

Лозиков Алексей
TrapX BDM

SOFTPROM

Современное состояние ИБ

TRAPX SECURITY

- Правильный вопрос НЕ ***«Могут ли взломать мою сеть?»***, а ***«Кто и как ее взломал? Как долго он/они в моей сети и что они уже успели сделать?»***

Основные факты о компании TrapX Security

TRAPX SECURITY

- TrapX (trapx.com) – один из мировых лидеров в области систем активной кибер-защиты на базе сетевых ловушек (псевдоуязвимые сервисы/устройства)
- Основана в 2011 году в Израиле. Офисы в Израиле, США, Великобритании, Гонконге
- Более 200 заказчиков по всему миру
- Темп роста выручки – более 100% ежегодно

Best 2015 in Biz AWARDS 5th annual WINNER

Best 2016 in Biz AWARDS 6th annual WINNER

THE GOLDEN BRIDGE AWARDS GOLD BEST 2016 BUSINESS WORLD

CYBERSECURITY Excellence Awards The most innovative product WINNER 2016

Gartner 2015 Cool Vendor

CYBERSECURITY [H]M LEADER 2016

Война – это путь обмана

TRAPX SECURITY

“Война — это путь обмана. Поэтому, даже если ты способен, показывай противнику свою неспособность. Когда должен ввести в бой свои силы, притворись бездеятельным. Когда цель близко, показывай, будто она далеко; когда же она действительно далеко, создавай впечатление, что она близко.”

Сунь Цзы, Искусство войны

Анатомия направленной атаки 1/2

TRAPX SECURITY

ДОСТИЖЕНИЕ ЦЕЛЕЙ

- Хищение ключевой информации
- Изменение данных
- Манипуляции с бизнес процессами
- Сокрытие следов
- Точка возврата

ПОДГОТОВКА

- Выявление цели
- Сбор информации
- Разработка стратегии
- Создание стенда
- Разработка инструментов

РАСПРОСТРАНЕНИЕ

- Закрепление
- Распространение
- Обновление
- Поиск ключевой информации и методов достижения целей

ПРОНИКНОВЕНИЕ

- Техники обхода стандартных средств защиты
- Эксплуатация уязвимостей
- Социальная инженерия
- Комбинированные техники
- Инвентаризация сети

TrapX Deception Grid

TRAPX SECURITY

- Система централизованного развертывания специализированной «сигнальной сети» для раннего обнаружения APT и 0-day угроз, на базе «условно уязвимых» ИТ-сервисов (конечные точки, сетевые устройства, серверы, приложения, SCADA /POS /ATM /IoT-устройства)

Которая позволяет:

- Обнаруживать в режиме реального времени скрытые направленные атаки, не видимые традиционными средствами
- Защищать реальные ИТ-активы компании за счет переключения активности атакующих на «ловушки»
- Получать полную информацию о тактике атакующих, используемых ими инструментах и оперативно применять адекватные меры противодействия

Стратегия Deception

TRAPX SECURITY

1. Разведка

Изучение окружения
Активное/пассивное сканирование
Сбор учетных данных

Разнообразные «Приманки» на реальных ПК уводят атакера в «ловушки»
Маскировка реальной ИТ-инфраструктуры

---

2. Скрытое распространение/поиск целей

Поиск и построение вектора атаки к основной цели

Тысячи «Ловушек» замедляют и обеспечивают быстрое обнаружение атаки

---

3. Хищение/изменение/уничтожение информации

Клоны OS/ приложений обеспечивают:
- **быстрое обнаружение и замедление атаки**
- **сбор данных о тактике и инструментарии атакера**

Преимущества решения TrapX Deception Grid

TRAPX SECURITY

- Эффективно обнаруживает атаки, независимо от их типа
- Обнаружение скрытой активности атакующих за счет анализа не только «вертикального», но и «east-west» трафика внутри и между vlan-ами
- Высочайший уровень достоверности эмулируемых ИТ-активов
- Уровень false positive – близок к 0
- Автоматический статический и динамический анализ используемого злоумышленниками ПО
- Не использует агентов и не оказывает влияния на работу пользователей и ИТ-сервисов
- Не требует изменений в сетевой топологии или радикальной перенастройки оборудования
- Быстрый цикл внедрения – решение может быть развернуто за несколько часов
- Возможность интеграции с существующими решениями ИБ от McAfee, Palo Alto, Cisco
- Невысокие требования к аппаратным ресурсам, не нужны дополнительные лицензии на ПО (ОС, БД)

Клиенты

TRAPX SECURITY

Финансы/инвестиции

RenaissanceRe

IBI בית השקעות

שירותי בנק אוטומטיים בע"מ

בנק אגוד

בנק ישראל Bank of Israel

הבינלאומי

DEXIA

הבורסה לניירות ערך

Deloitte.

SAFECHARGE

Гос.органы

שורק

המרכז למחקר גרעיני - שורק

תל אביב יפו TEL AVIV YAFO

Производство

orbotech

Unilever

כיל ICL

MOBILEYE

MOTOROLA

Транспорт

ZIM

ИТ/Медиа

בזק

BBC

Медицина

בית חולים אסותא סטנדרט של בריאות

HCA Va Health System

Mede/Analytics

JOHN MUIR HEALTH

Строительство

שיכון ובינוי מקבוצת אריסון

TrapX DeceptionGrid™

Техническая часть

SOFTPROM

DeceptionGrid™

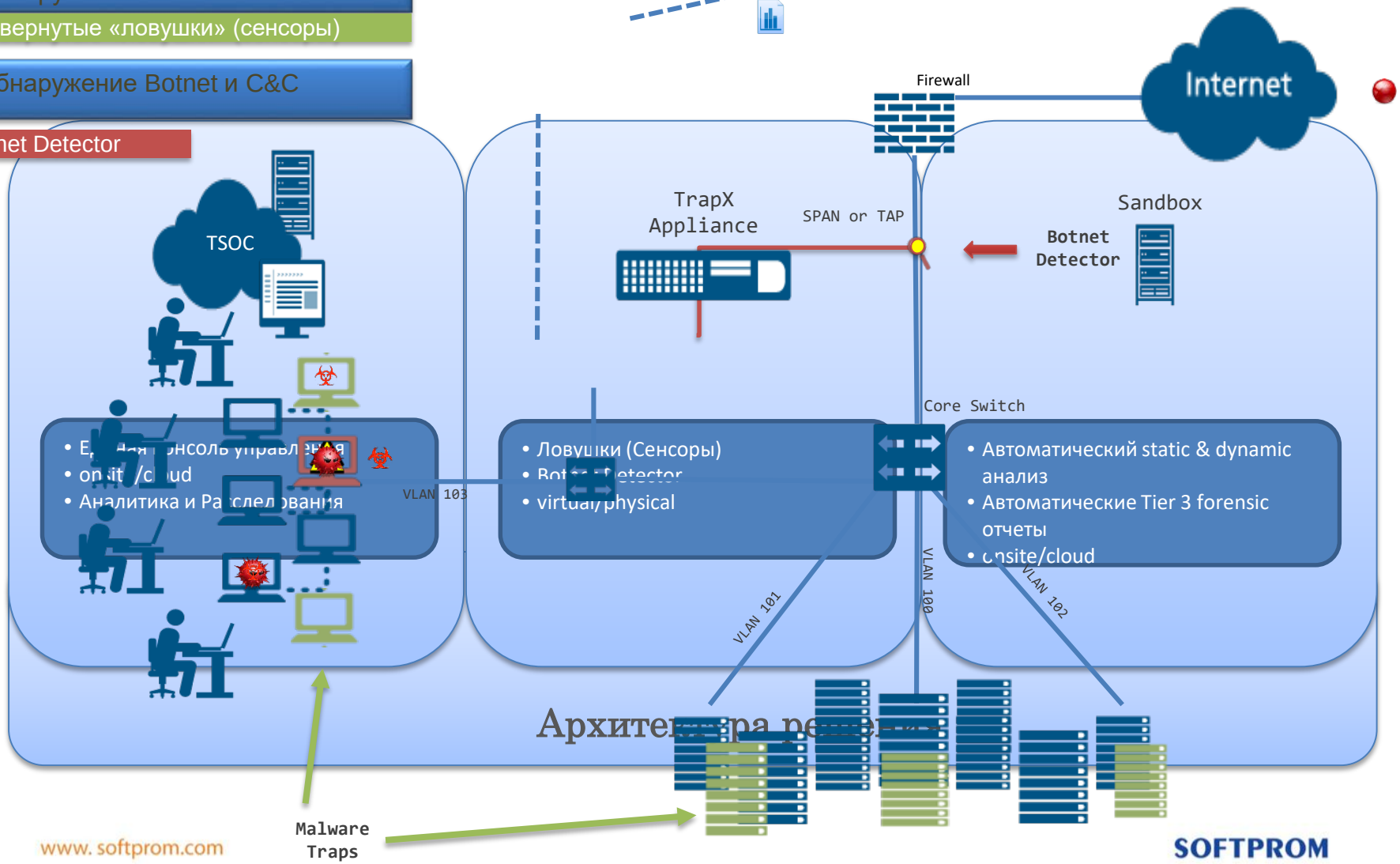
TRAPX SECURITY

Обнаружение атаки

Развернутые «ловушки» (сенсоры)

Обнаружение Botnet и C&C

Botnet Detector



TrapX – функционал и возможности ловушек

TRAPX SECURITY

Приманки

Drive Mapping
Browser History
Browser Credentials
Browser Bookmark
Hosts
ODBC
Putty
AD
Ложный трафик
Реакция на сканирование

Ловушки

Эмуляции

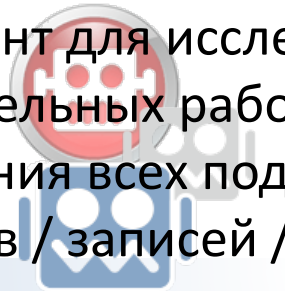
Windows
Voip
Router
Linux
Swift
Med
Macintosh
Scada
IOT

Протоколы и сервисы

SMB	FTP	AD	Web	DNS	RDP
WMI	SSH	Mysql	Mssql	Telnet	SNMP
TFTP	SIP	POS	Modbus	DNP3	Bonjur

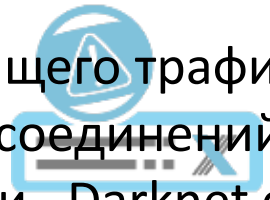
Дополнительные возможности

Botnet Detector



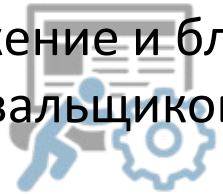
Инструмент для исследования подозрительных рабочих станций и выявления всех подозрительных процессов / записей / настроек / ключей и т.п.

Automatic Incident Response



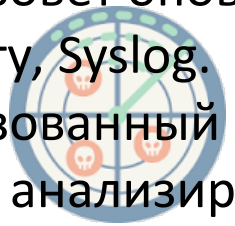
Анализ исходящего трафика и обнаружение соединений с C&C серверами, Darknet соединений

Automatic Forensics Reports



Обнаружение и блокирование «шифровальщиков»

CryptoTrap



Любое взаимодействие с ловушкой (сенсором) вызовет оповещение в консоль, почту, Syslog.
Любой использованный код, malware автоматически анализируется в «песочнице»

Экосистема TrapX

TRAPX SECURITY

Интеграция с NAC по зволяет изолировать ПК или блокировать трафик

NAC

ForeScout

cisco

portnox™ boundlessly smart

Response & Sandbox

Интеграция с MacAfee EPO позво ляет блокировать атаки на конечных точках.
Интеграция с Sand box позволяет про водить динамичес кий анализ угроз

Служит источником высококачественной информации для SIEM

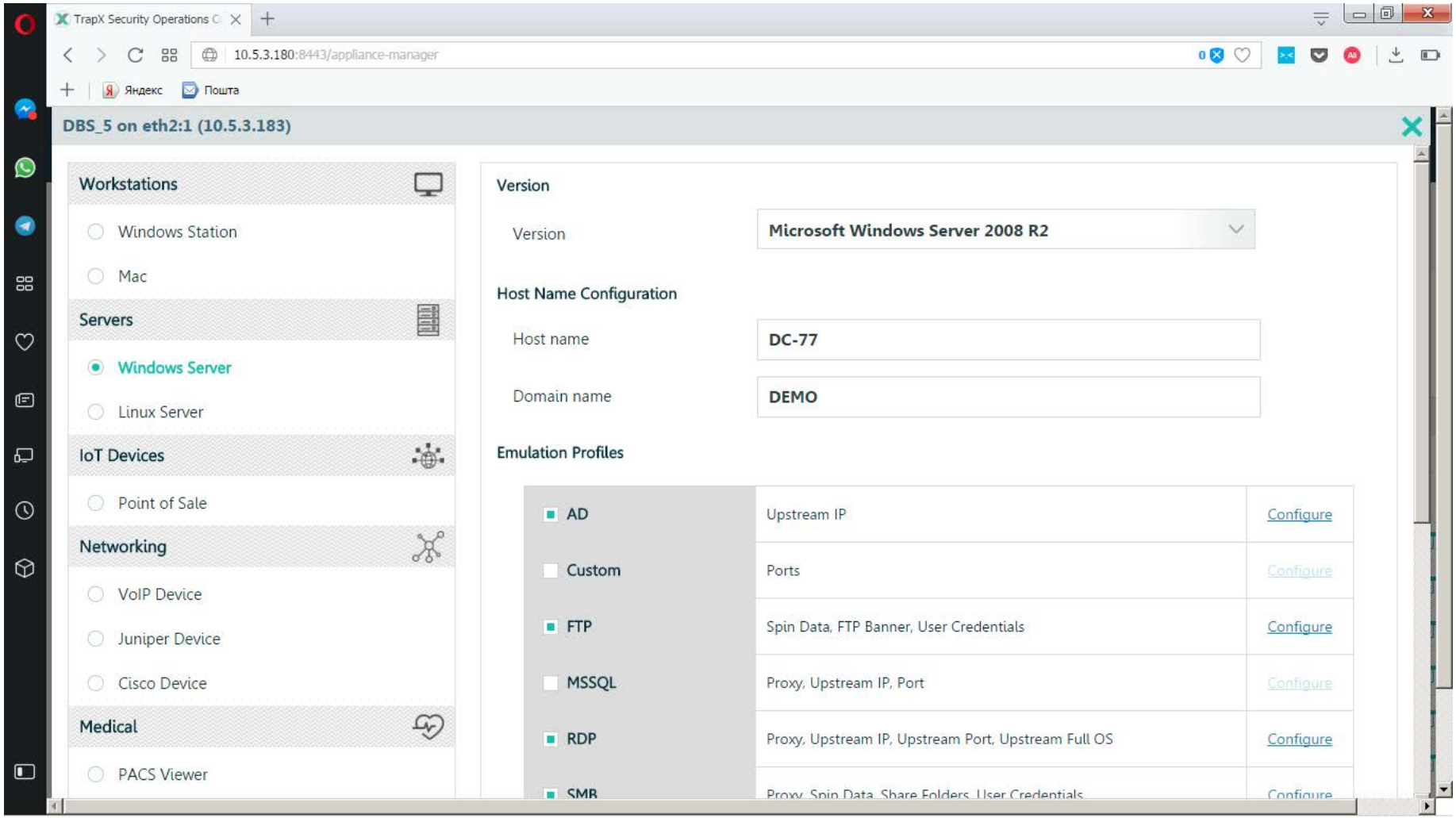
SIEM

ArcSight An HP Company

splunk>

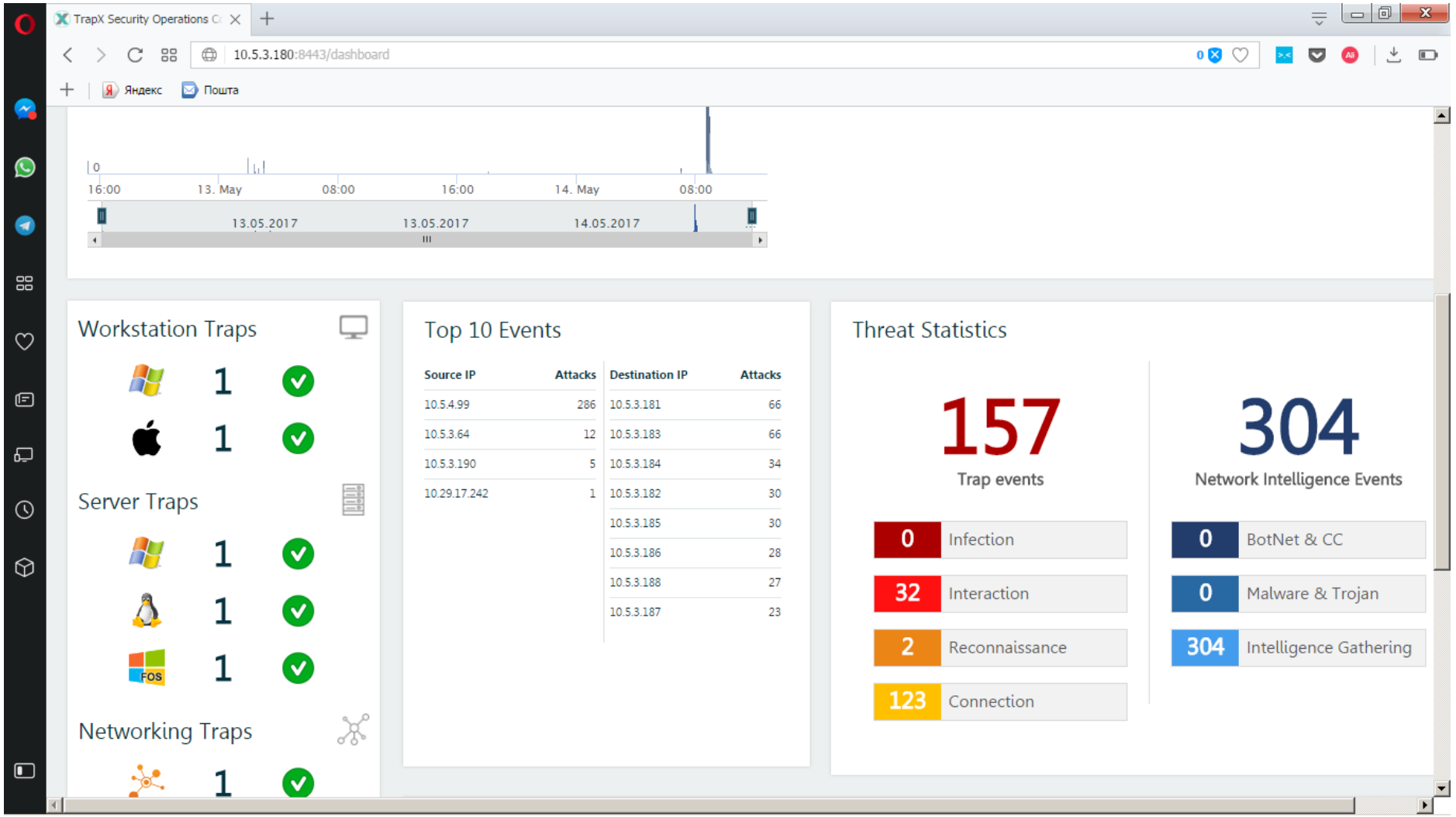
Radar

Настройка ловушки

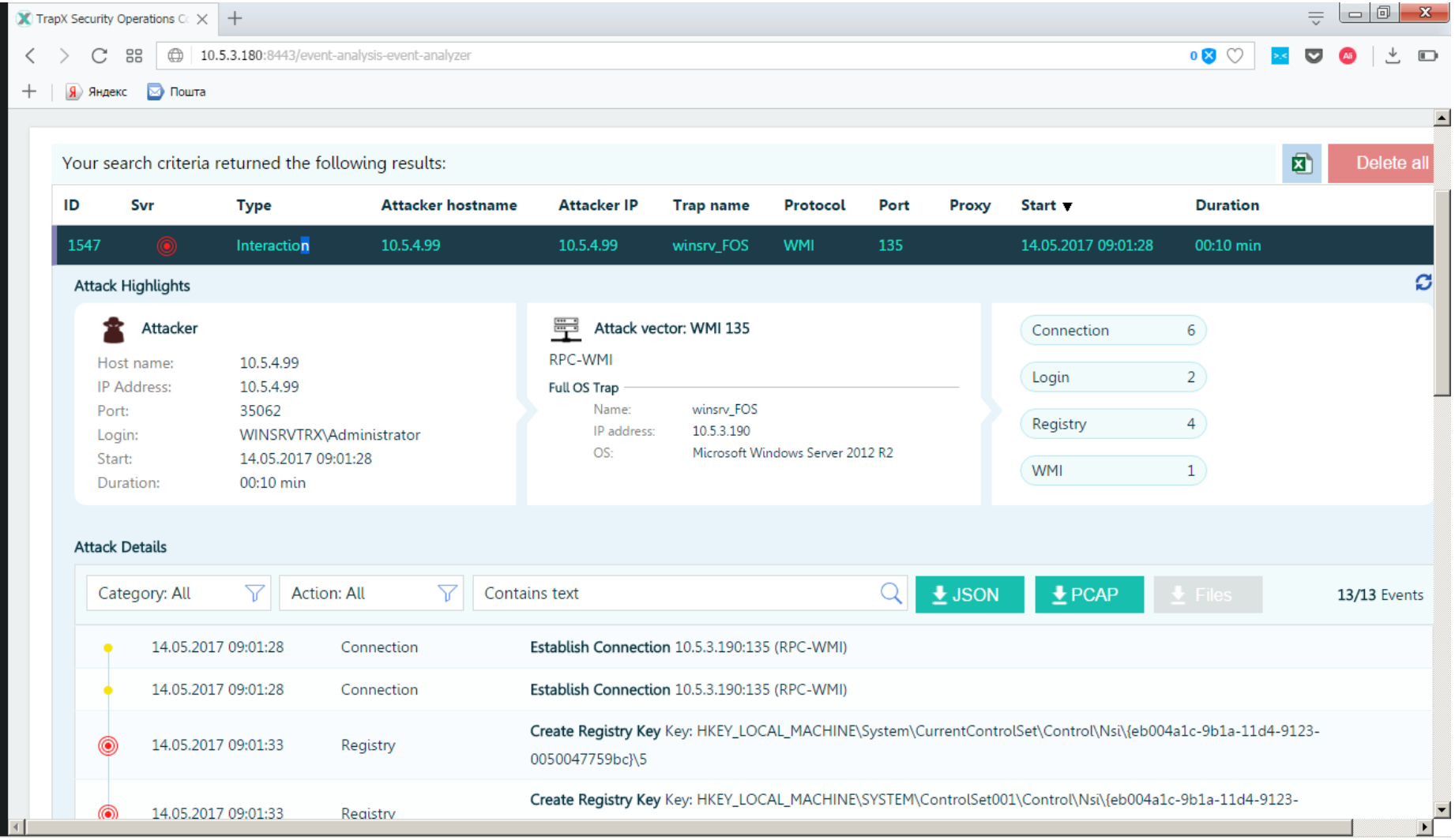


Консоль

TRAPX SECURITY



Информация о событии



Визуализация атаки

Преимущества TrapX Deception Grid

TRAPX SECURITY

Эффективно!

- Эффективно обнаруживает успешные атаки, независимо от их типа

Надежно!

- Уровень false positive – близок к 0

Быстро!

- Быстрый цикл внедрения – решение может быть развернуто за несколько часов

Минимум затрат!

- Не использует агентов и не оказывает влияния на работу пользователей и ИТ-сервисов
- Не требует изменений в сетевой топологии или радикальной перенастройки оборудования

СПАСИБО!

Лозиков Алексей

TrapX BDM

t.: +38 (044) 594 52 52 ext. 3155

m.: +38 050 58-58-58-9

lozikov@softprom.com

www.softprom.com