Безопасность сети
Ловля на живца

Вячеслав Синьков
30.03.2018

IT.Integrator

TrapX DeceptionGrid – основоположник новой продуктовой категории Gartner

The current information security market has many categories of services and software. In 2014 worldwide information security spending reached almost $71.1 billion per Gartner Group.[2] This includes worldwide security software revenue which in 2013 totaled $19.9 billion.[3] Many of these existing services and technologies are integrated into your operations today. A new category, Deception Technology has emerged with the launch of new products such as TrapX Security's Deception Grid™.

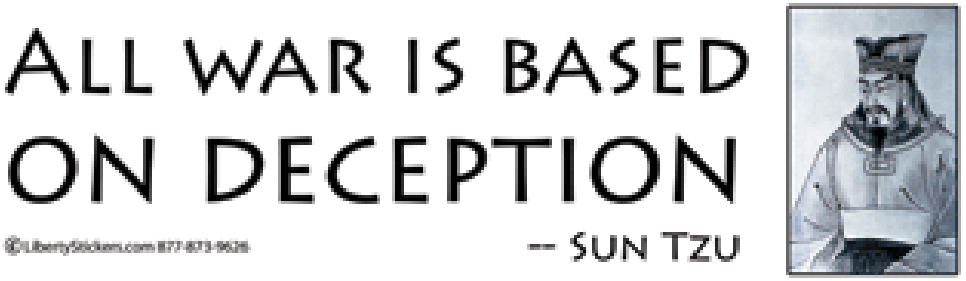
Deception Technology allows your cyber defense team to detect the most sophisticated attacks to include advanced persistent threats (APTs) and zero day events in real-time. In July, 2015 Gartner Group noted that by 2018, 10% of enterprises will use deception tools and related tactics, and actively participate in deception operations against attackers. They further noted that deception as a defense strategy against attackers has merit and it can be an attractive new capability for larger organizations desiring advanced threat detection and defense solutions.[4]

Deception - #3 в Top Technologies for Security в 2017 (http://www.gartner.com/newsroom/id/3744917)

Война – это путь обмана

“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



Основные факты о компании TrapX

- 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.
- Более 250 заказчиков по всему миру
- В 2017 вышла уже ver.6 продукта
- Основные инвесторы – Intel Capital и BRM (инвесторы CheckPoint)

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 CoolVendor

CYBERSECURITY HOT LEADER 2016

CYBERSECURITY Excellence Awards Innovative product of the Year Threat Detection WINNER 2017

Современное состояние ИБ

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?»***

Традиционный подход

- Фокусировка на **защитных** инструментах
- Реагирование **после** инцидента
- Большой поток информации и ложных срабатываний

Проактивный подход

- Принятие факта, что успешные атаки **неизбежны**
- Построение системы ИБ исходя из этого
- Фокусировка на максимально **быстром** обнаружении атак

Риск успешной APT атаки есть всегда

TrapX DeceptionGrid

Решение для тех заказчиков, кто **не хочет/не имеет права принимать на себя риски** связанные с использованием 0-day уязвимостей и направленных атак:

Уже используют:

- Министерство обороны Израиля
- Национальная полиция Израиля
- Национальный Банк Израиля
- Фондовая биржа Тель-Авива
- Центр ядерных исследований Нахаль-Сорек (Израиль)
- Телеком-сектор: Bezeq (крупнейший ISP Израиля), Telemax (Мексика), American Mobile (США), NTT (Япония)
- А так же: BBC, Motorolla, RenaissanceRe, Unilever

TrapX DeceptionGrid

Сенсорная сеть для раннего обнаружения APT и 0-day угроз, на базе «условно уязвимых» сенсоров (ПК, серверы, сетевые устройства, приложения, SCADA /POS /ATM /IoT-устройства), которая позволяет:

- **Быстро обнаруживать** успешные атаки **независимо** от того, какие уязвимости/инструменты используются
- **Замедлять** ход атаки с помощью техник активной дезинформации атакующей стороны
- **Автоматически подавлять** атаки на этапе распространения за счет интеграции с другими ИБ-решениями (NAC/SIEM/AV)

Анатомия целенаправленной атаки

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

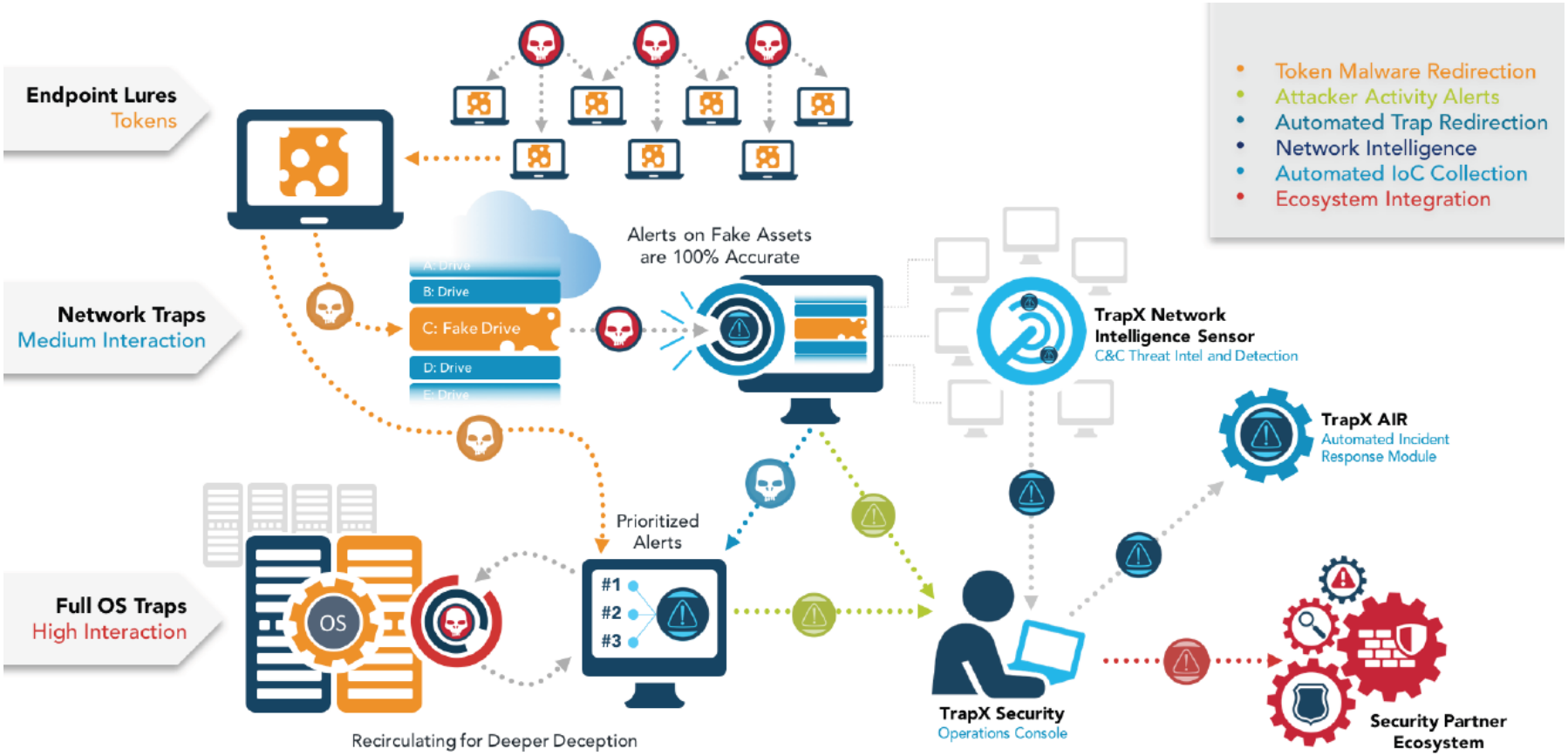
РАСПРОСТРАНЕНИЕ

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

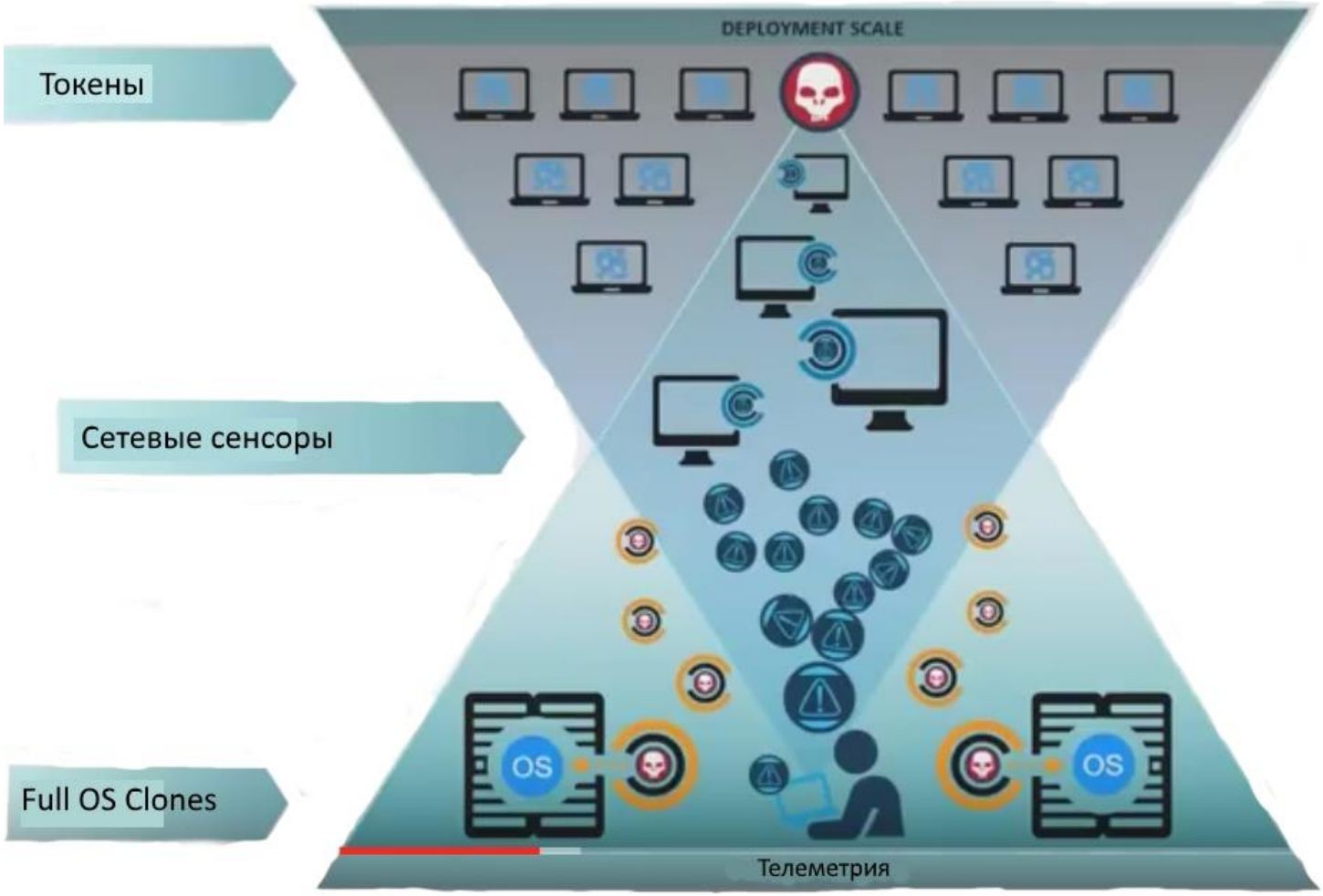
ПРОНИКНОВЕНИЕ

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

Архитектура решения



Архитектура решения



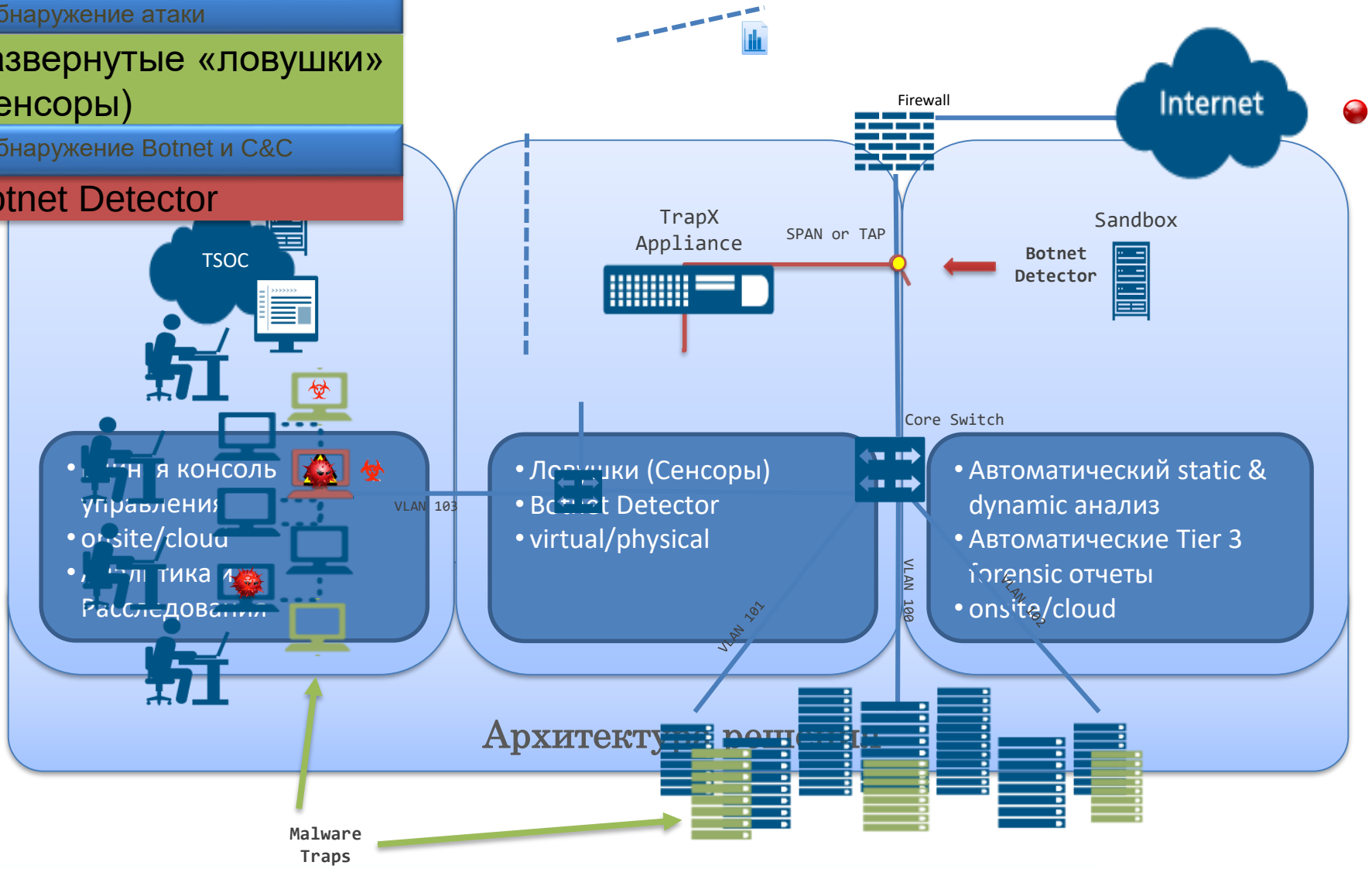
Принцип работы

Обнаружение атаки

Развернутые «ловушки» (сенсоры)

Обнаружение Botnet и C&C

Botnet Detector



Функционал и возможности ловушек

Приманки

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

Ловушки

Эмуляции

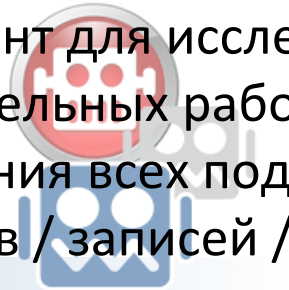
Windows
Voip
Router
Linux
Swift
Med
Macintosh
Scada
IOT

Протоколы и сервисы

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

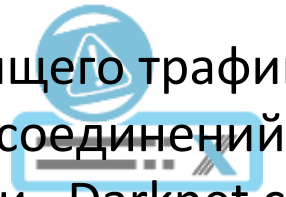
Дополнительные возможности

Botnet Detector



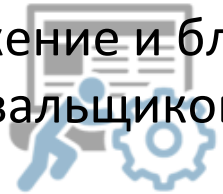
Инструмент для исследования подозрительных рабочих станций и выявления всех подозрительных процессов / записей / настроек / ключей и т.п.

Automatic Incident Response



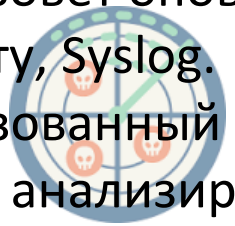
Анализ исходящего трафика и обнаружение соединений с C&C серверами, Darknet соединений

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

NAC

Интеграция с NAC позволяет изолировать ПК или блокировать трафик

Response & Sandbox

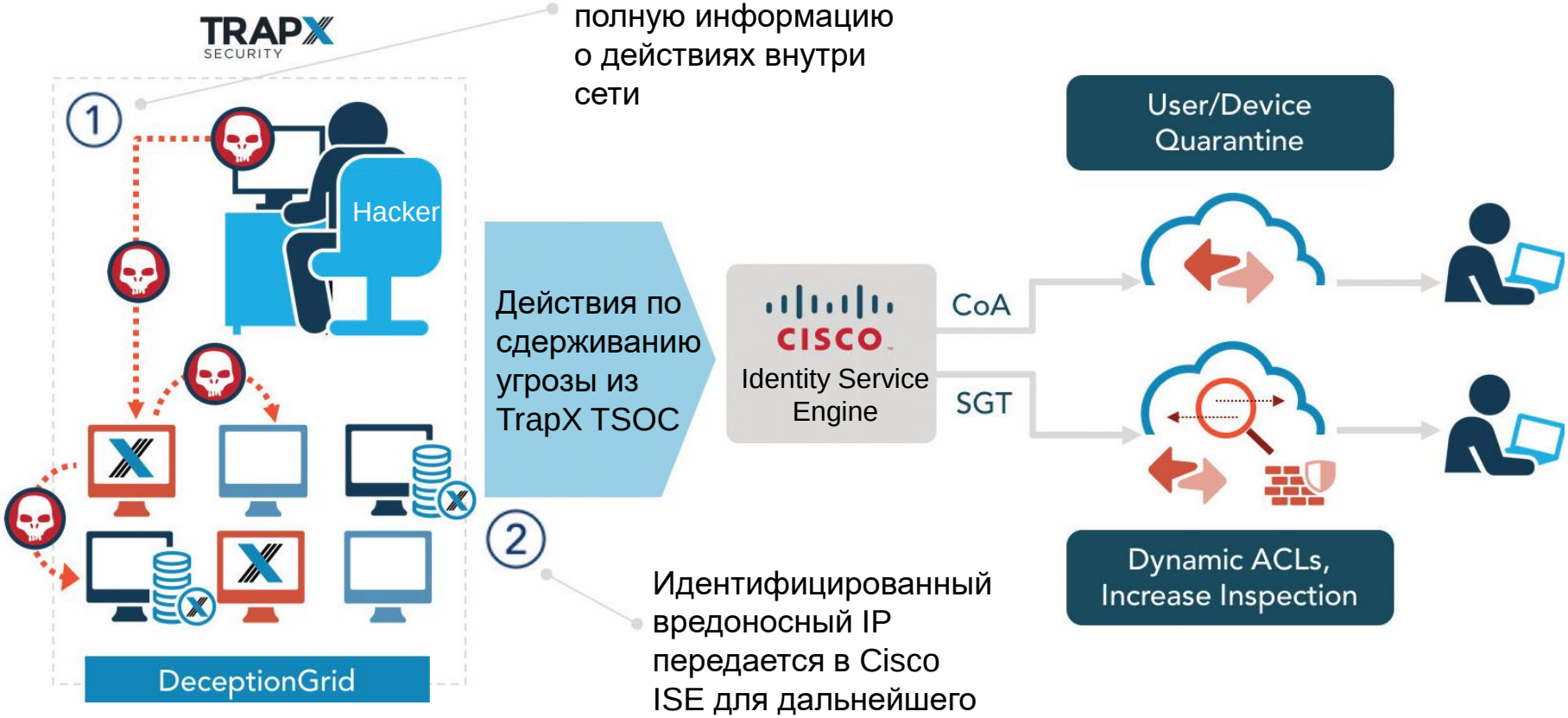
Интеграция с MacAfee EPO позволяет блокировать атаки на конечных точках. Интеграция с Sandbox позволяет проводить динамический анализ угроз

Служит источником высококачественной информации для SIEM

SIEM

Адаптивная защита с Cisco ISE

Ловушки и маркеры предоставляют полную информацию о действиях внутри сети

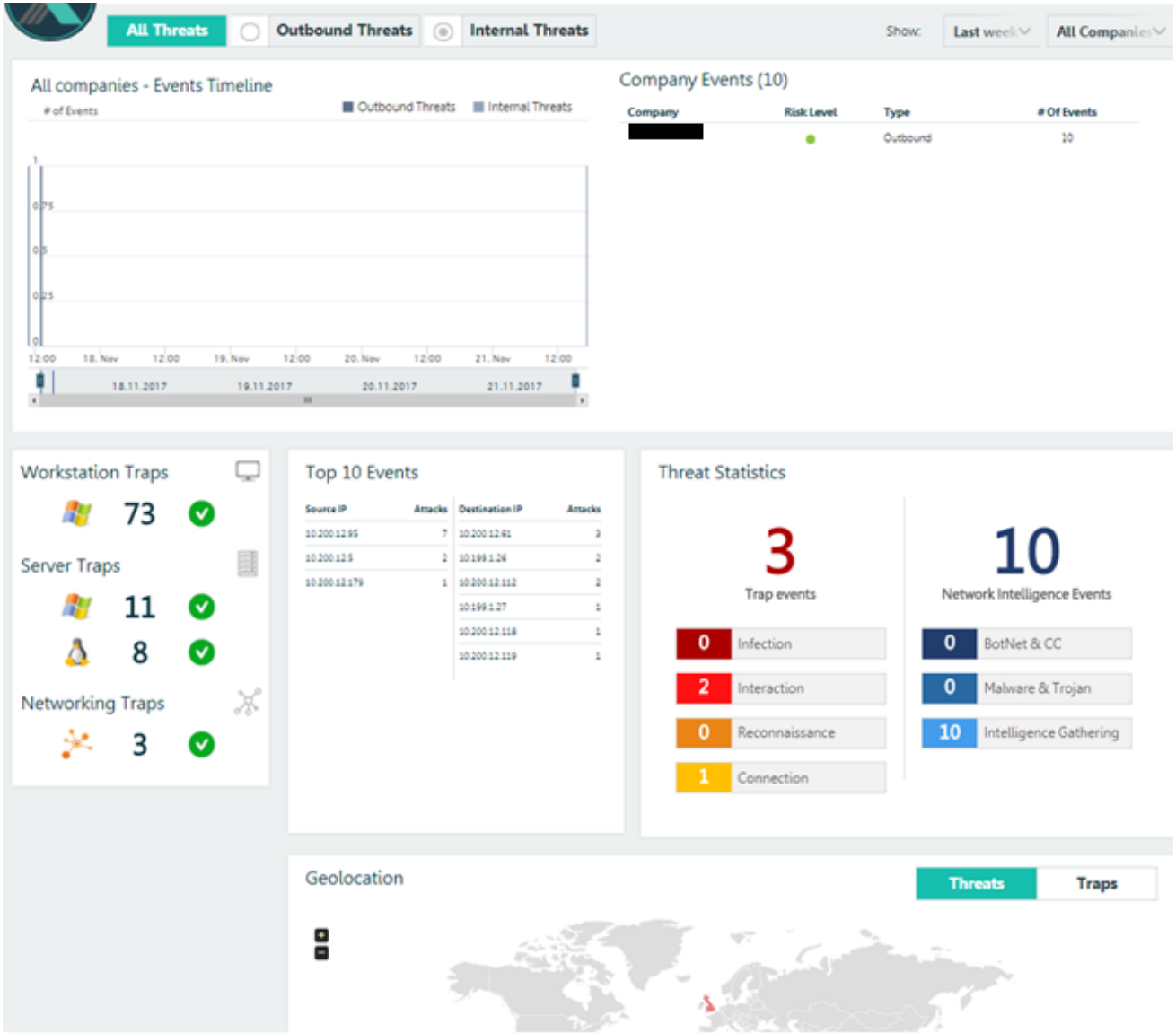


Идентифицированный вредоносный IP передается в Cisco ISE для дальнейшего реагирования

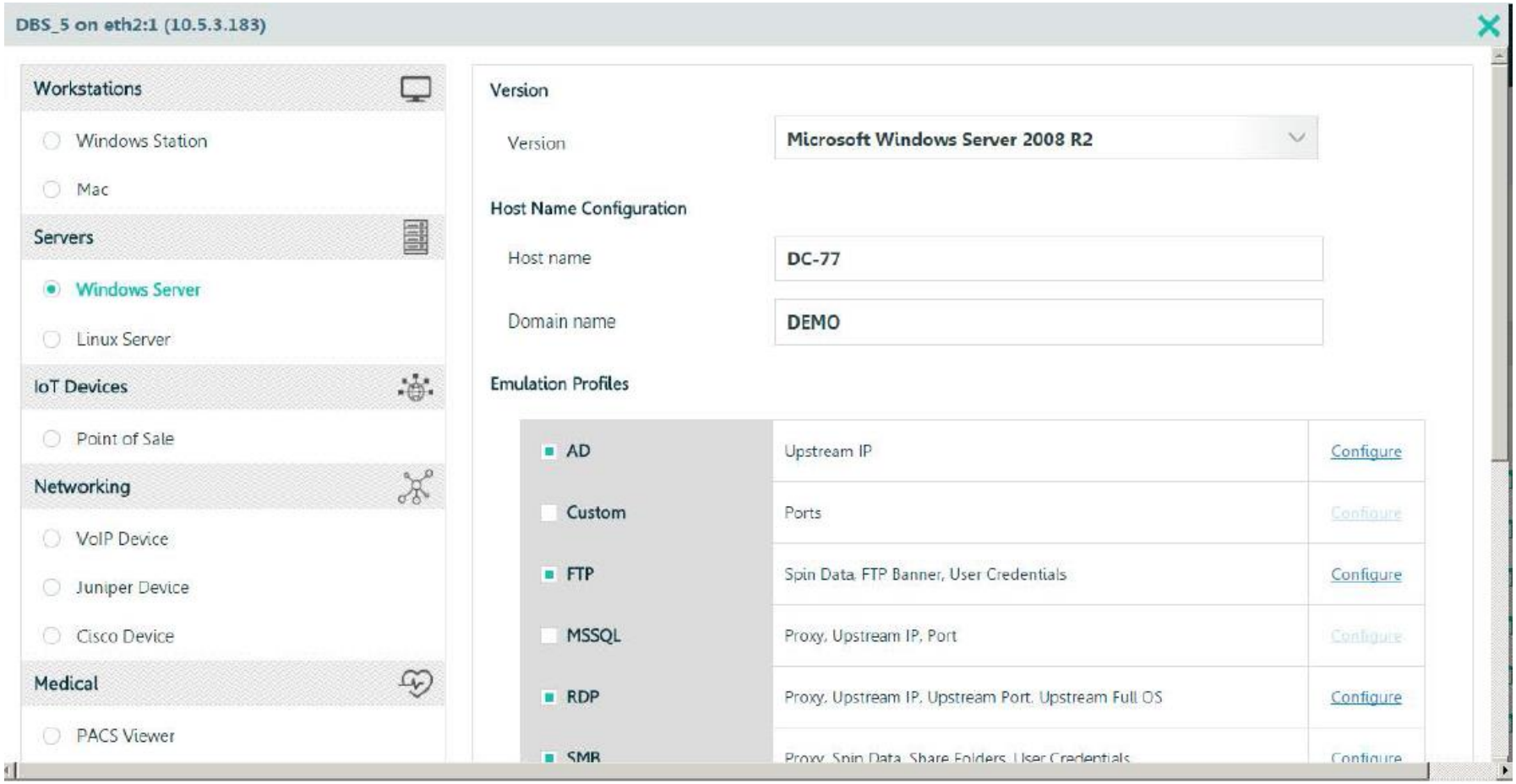
Преимущества решения

- 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
- 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
- Возможность интеграции с существующими решениями ИБ от McAfee, Palo Alto, Cisco и других производителей

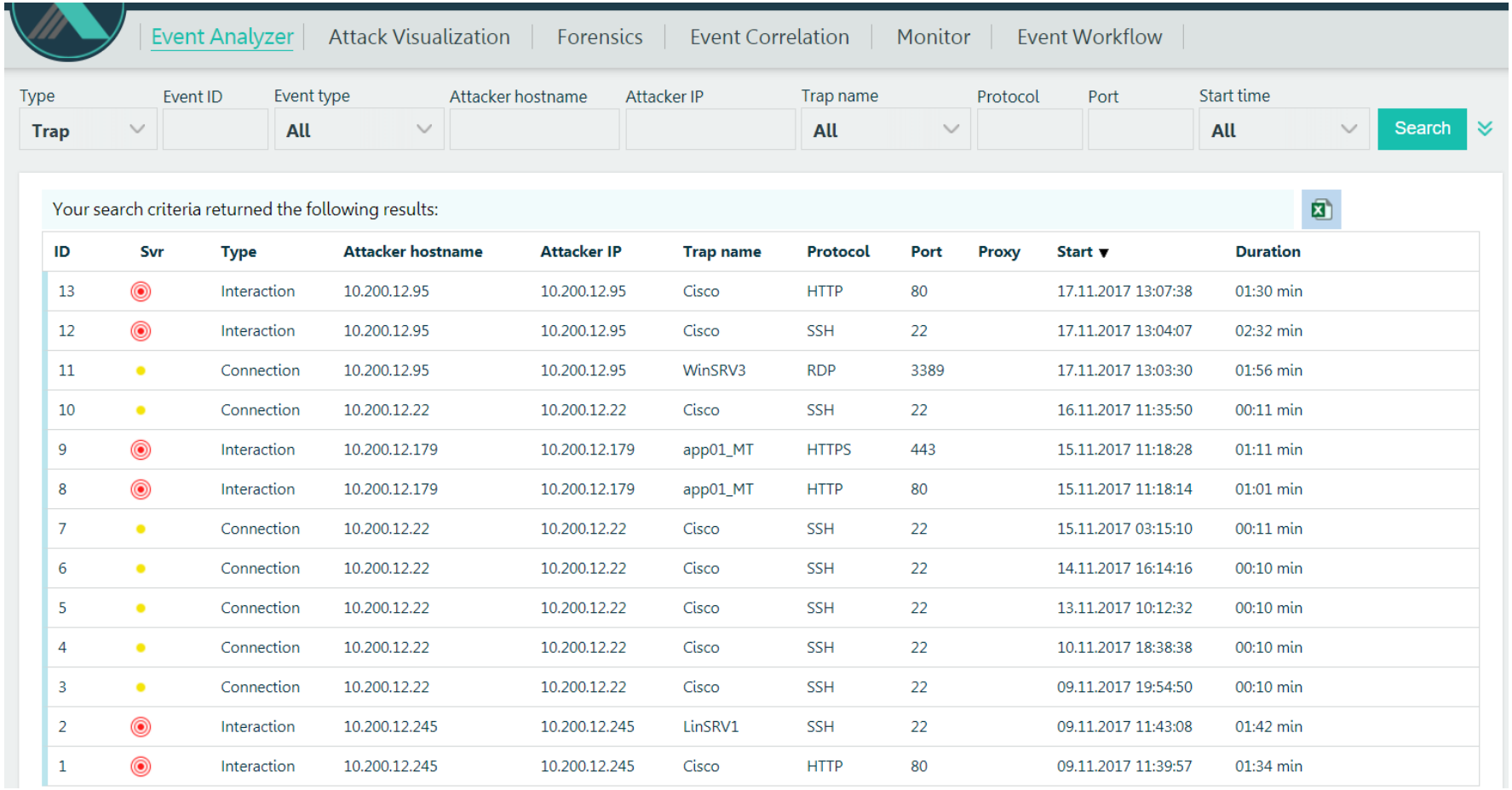
Веб-консоль


All Threats
Outbound Threats
Internal Threats
Show:
Last week
All Companies
All companies - Events Timeline
# of Events
Outbound Threats
Internal Threats
Company Events (10)
Company
Risk Level
Type
Of Events
Outbound
10
Workstation Traps
73
Server Traps
11
8
Networking Traps
3
Top 10 Events
Source IP
Attacks
Destination IP
Attacks
Threat Statistics
3
Trap events
0 Infection
2 Interaction
0 Reconnaissance
1 Connection
10
Network Intelligence Events
0 BotNet & CC
0 Malware & Trojan
10 Intelligence Gathering
Geolocation
Threats
Traps

Создание ловушки

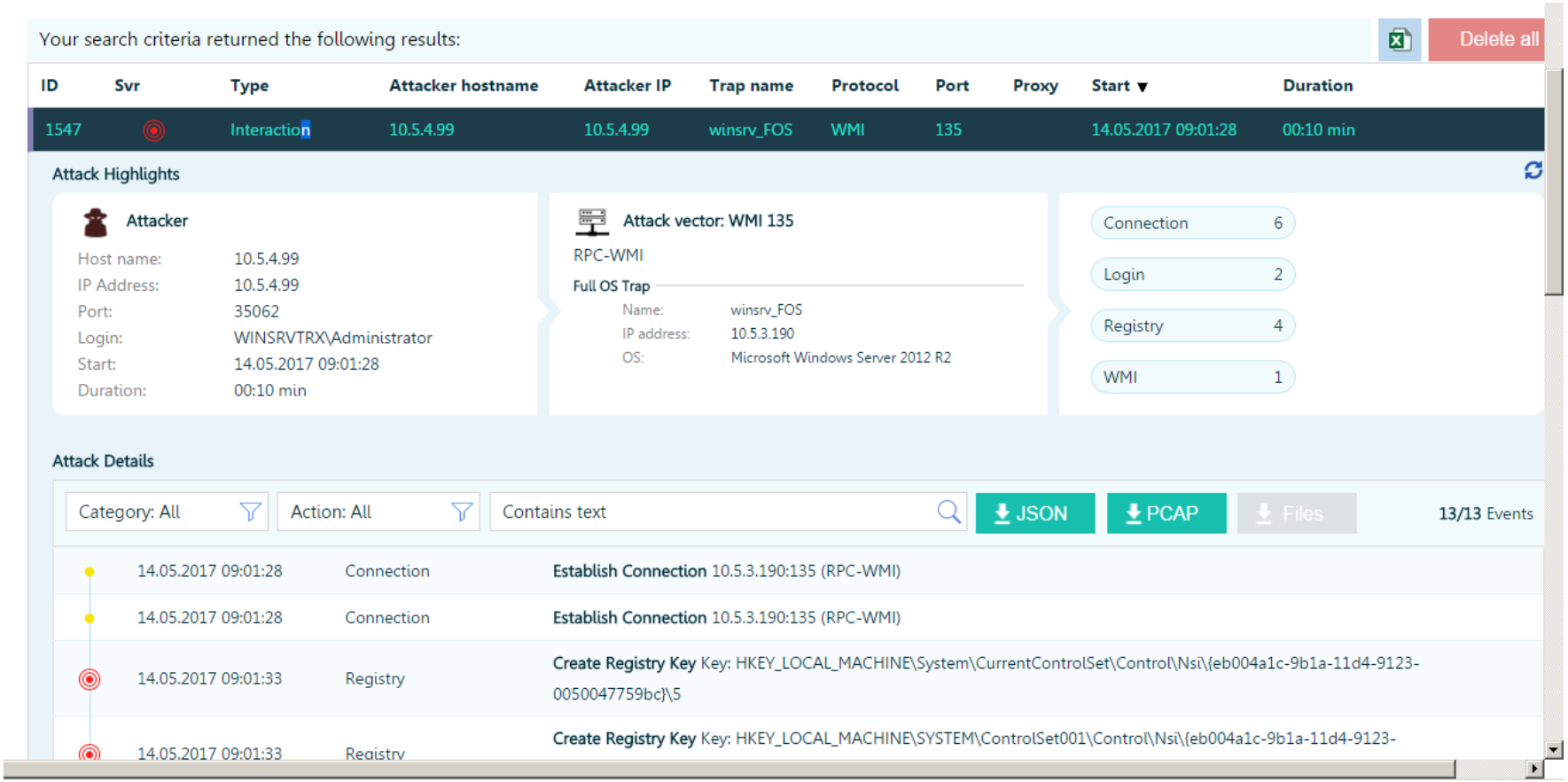


Анализатор событий

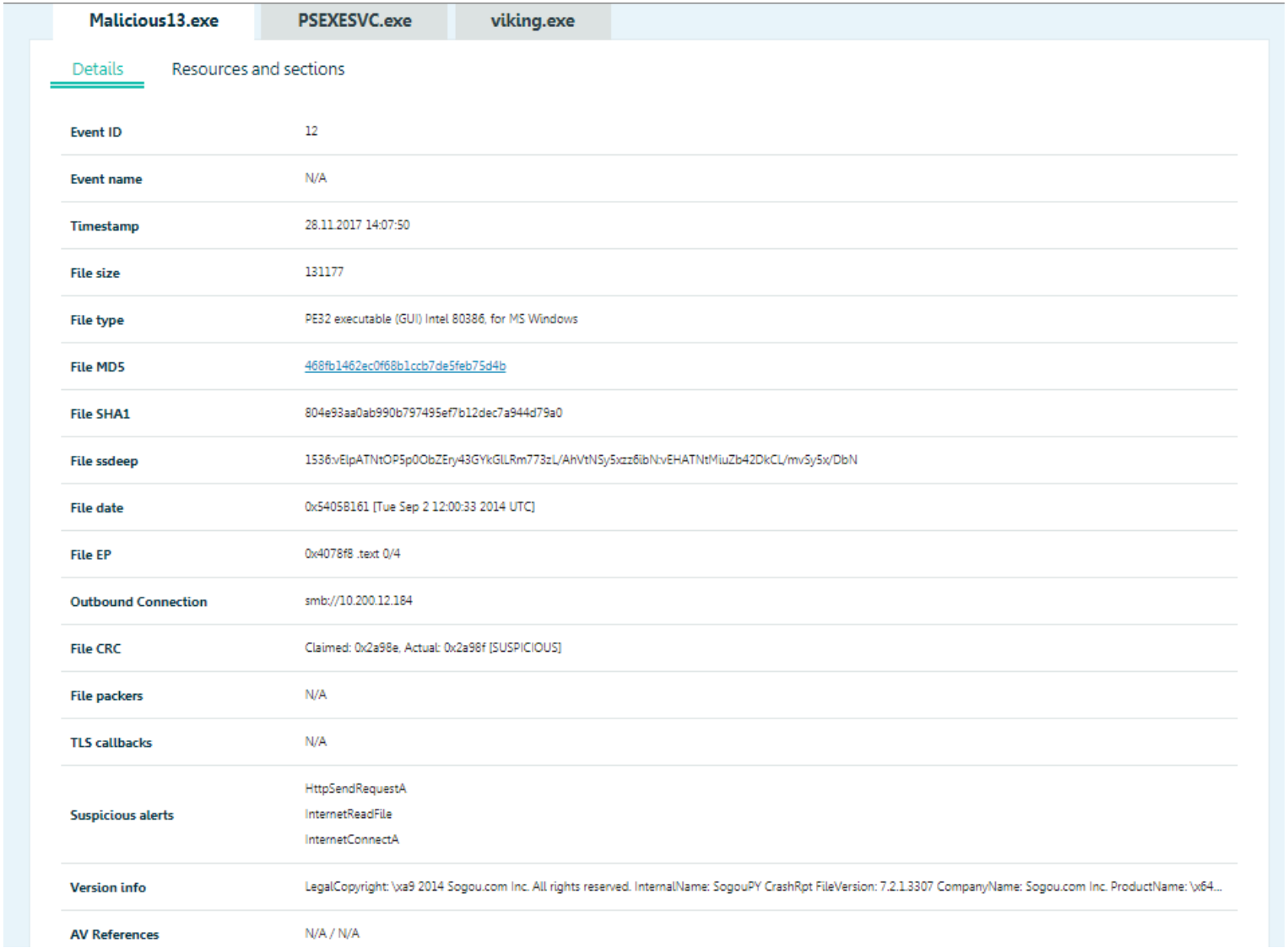


ID	Svr	Type	Attacker hostname	Attacker IP	Trap name	Protocol	Port	Proxy	Start ▼	Duration
13		Interaction	10.200.12.95	10.200.12.95	Cisco	HTTP	80		17.11.2017 13:07:38	01:30 min
12		Interaction	10.200.12.95	10.200.12.95	Cisco	SSH	22		17.11.2017 13:04:07	02:32 min
11		Connection	10.200.12.95	10.200.12.95	WinSRV3	RDP	3389		17.11.2017 13:03:30	01:56 min
10		Connection	10.200.12.22	10.200.12.22	Cisco	SSH	22		16.11.2017 11:35:50	00:11 min
9		Interaction	10.200.12.179	10.200.12.179	app01_MT	HTTPS	443		15.11.2017 11:18:28	01:11 min
8		Interaction	10.200.12.179	10.200.12.179	app01_MT	HTTP	80		15.11.2017 11:18:14	01:01 min
7		Connection	10.200.12.22	10.200.12.22	Cisco	SSH	22		15.11.2017 03:15:10	00:11 min
6		Connection	10.200.12.22	10.200.12.22	Cisco	SSH	22		14.11.2017 16:14:16	00:10 min
5		Connection	10.200.12.22	10.200.12.22	Cisco	SSH	22		13.11.2017 10:12:32	00:10 min
4		Connection	10.200.12.22	10.200.12.22	Cisco	SSH	22		10.11.2017 18:38:38	00:10 min
3		Connection	10.200.12.22	10.200.12.22	Cisco	SSH	22		09.11.2017 19:54:50	00:10 min
2		Interaction	10.200.12.245	10.200.12.245	LinSRV1	SSH	22		09.11.2017 11:43:08	01:42 min
1		Interaction	10.200.12.245	10.200.12.245	Cisco	HTTP	80		09.11.2017 11:39:57	01:34 min

Детальная информация



Анализ Malware

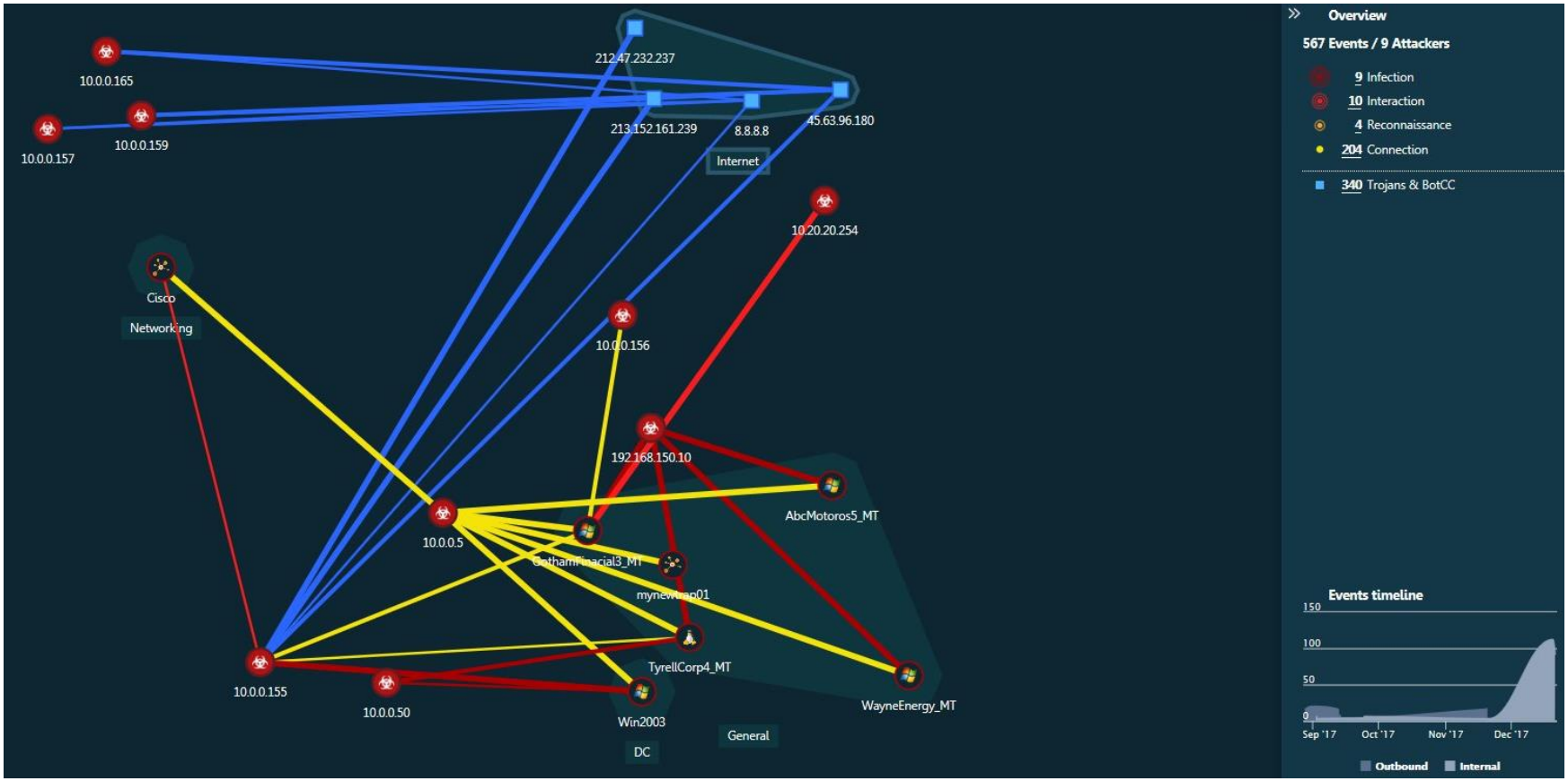


Malicious13.exe | PSEXESVC.exe | viking.exe

Details | Resources and sections

Event ID	12
Event name	N/A
Timestamp	28.11.2017 14:07:50
File size	131177
File type	PE32 executable (GUI) Intel 80386, for MS Windows
File MD5	468fb1462ec0f68b1ccb7de5feb75d4b
File SHA1	804e93aa0ab990b797495ef7b12dec7a944d79a0
File ssdeep	1536:vElpATNtOP5p0ObZEry43GYkGlLRm773zL/AhVtNSy5xzz6ibN:vEHATNtMiuZb42DkCL/mv5y5x/DbN
File date	0x5405B161 [Tue Sep 2 12:00:33 2014 UTC]
File EP	0x4078f8 .text 0/4
Outbound Connection	smb://10.200.12.184
File CRC	Claimed: 0x2a98e, Actual: 0x2a98f [SUSPICIOUS]
File packers	N/A
TLS callbacks	N/A
Suspicious alerts	HttpSendRequestA InternetReadFile InternetConnectA
Version info	LegalCopyright: \xa9 2014 Sogou.com Inc. All rights reserved. InternalName: SogouPY CrashRpt FileVersion: 7.2.1.3307 CompanyName: Sogou.com Inc. ProductName: \x64...
AV References	N/A / N/A

Визуализация атаки



Выводы

- Анализ горизонтального трафика внутри VLAN-ов
- Практически мгновенное обнаружение действий злоумышленников
- Анализ инцидентов и используемой стратегии злоумышленника
- Система проста во внедрении
- Нет необходимости в каких то глобальных перестройках или реконфигурации сети.

Спасибо
за внимание!