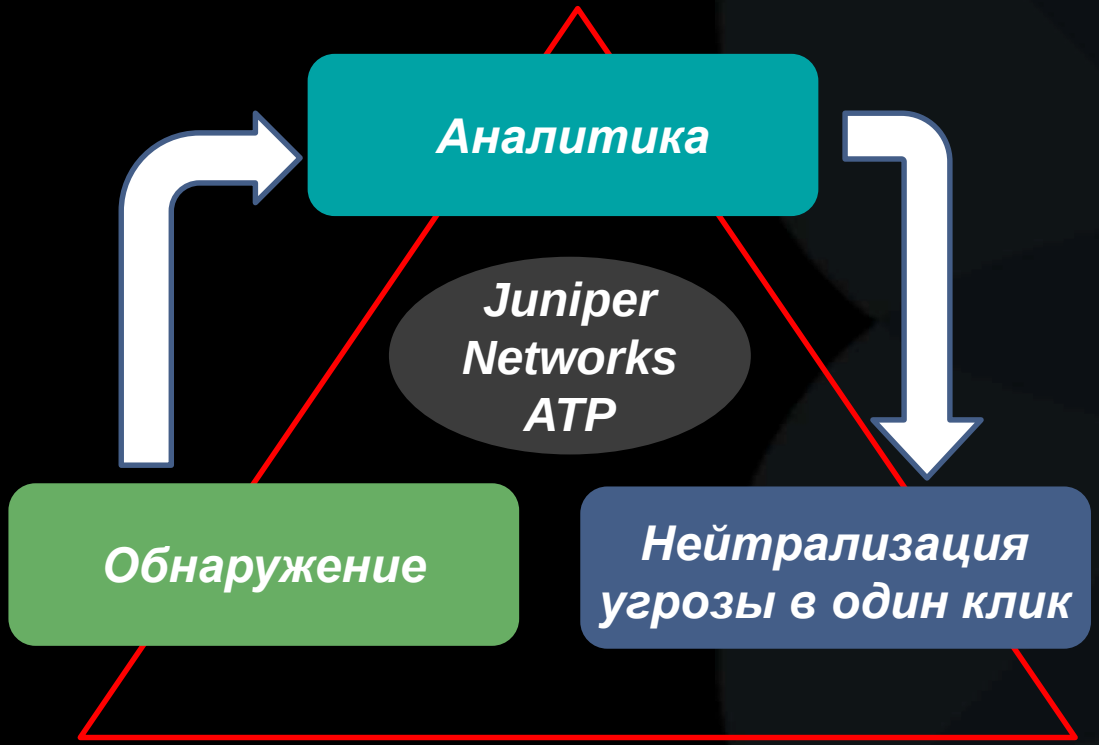
НАЙТИ ИГОЛКУ В СТОГЕ СЕНА. JUNIPER ADVANCED THREAT PREVENTION

Павел Живов

системный инженер, pzhivov@juniper.net

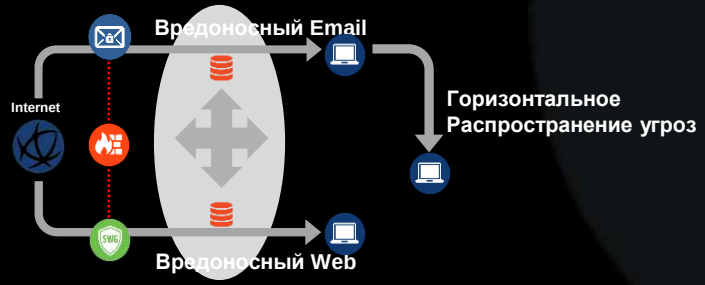
JUNIPER NETWORKS | Summit

3 ключевых функции решения Juniper ATP



- **Обнаружение** – Использованием алгоритмов машинного обучения и поведенческого анализа непрерывно собирают данные и обнаруживают угрозы в почтовом-, веб- и горизонтальном трафике
- **Аналитика** – модуль аналитики коррелируется и консолидирует данные о ВПО с учетом контекста и событий от других средств безопасности, ранжирует угрозы по результатам корреляции
- **Нейтрализация** – создание политик безопасности, сигнатур и правил для других имеющихся систем безопасности разных производителей для предотвращения заражения

Трудности, с которыми сталкиваются команды обеспечения информационной безопасности



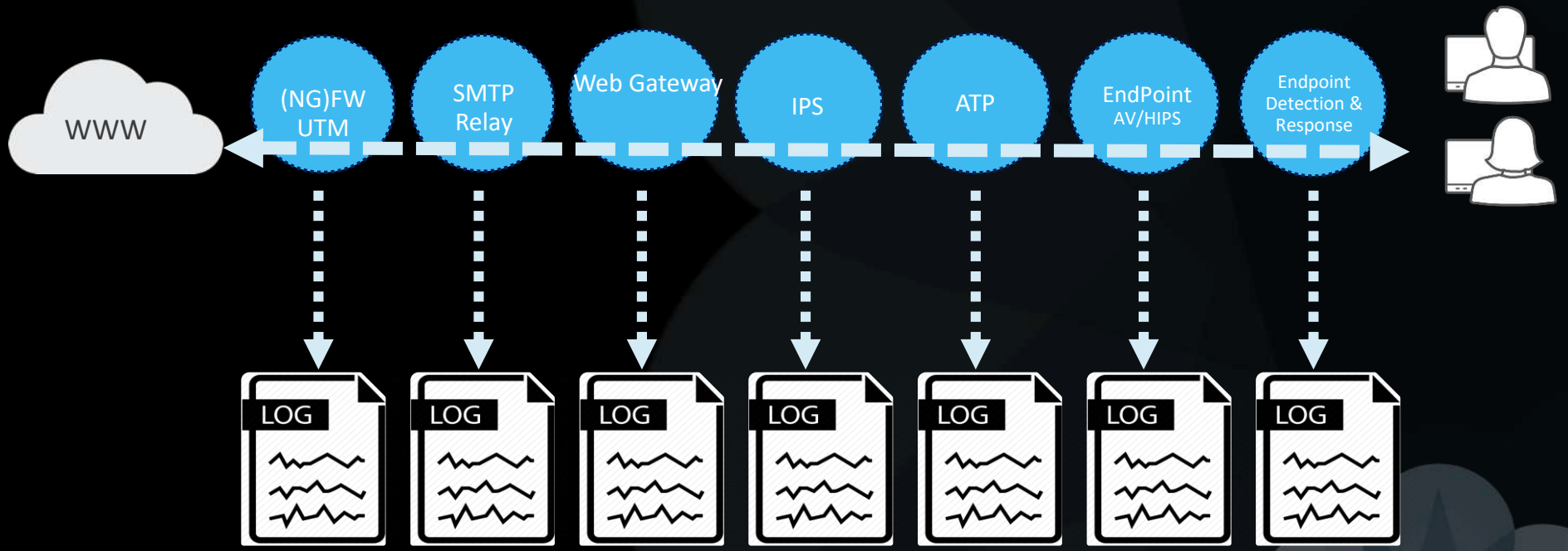
- ~ 200 млн. новых образцов ВПО в 2019 году
- ВПО нулевого дня обходят In-line защиту
- Почта и Веб продолжают быть основными векторами атаки
- Горизонтальное распространение угроз внутри сети

- 96% предупреждений в SOC игнорируется
- 69% требуется больше персонала для обработки задача IR
- 71% требуется больше автоматизации для решения задач IR

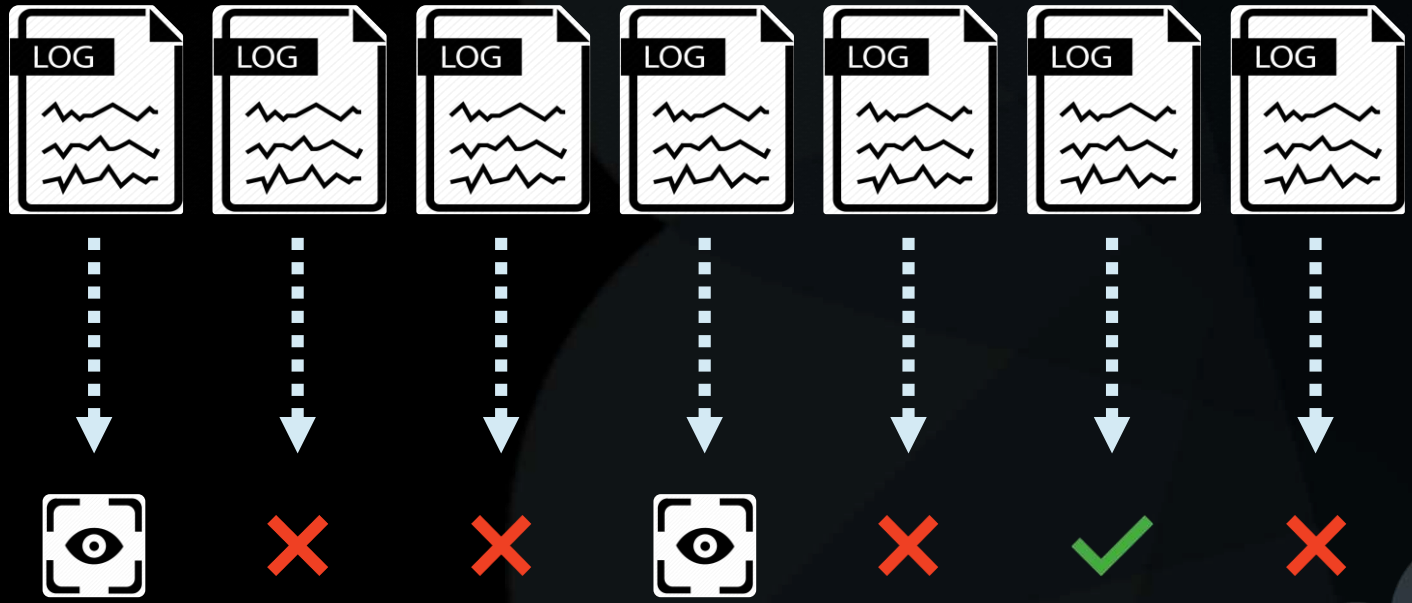
Источник: Symantec, IBM, Ponemon Institute, Osterman Research, McAfee


Реакция на
инциденты и
расследование

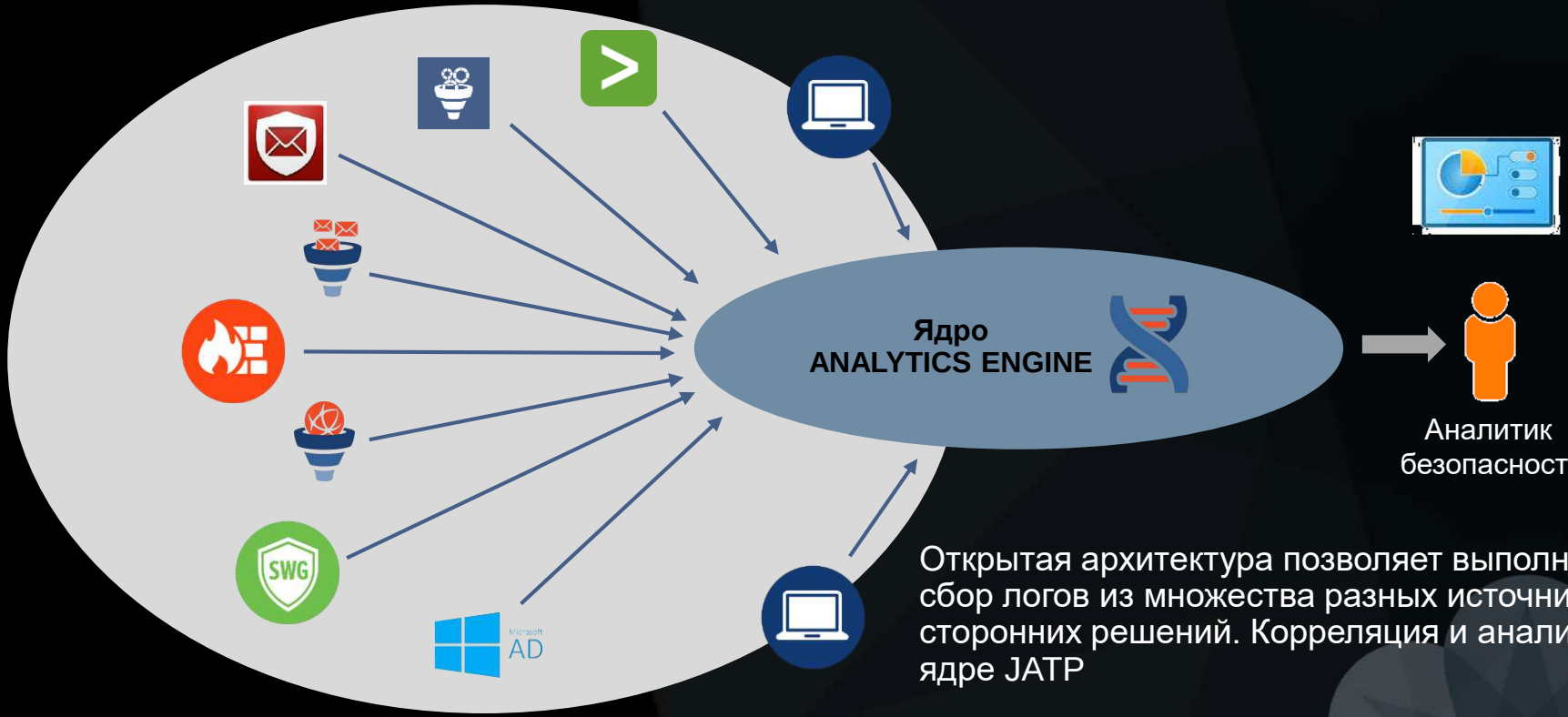
Модель безопасности с несколькими уровнями контроля



Модель безопасности с несколькими уровнями контроля

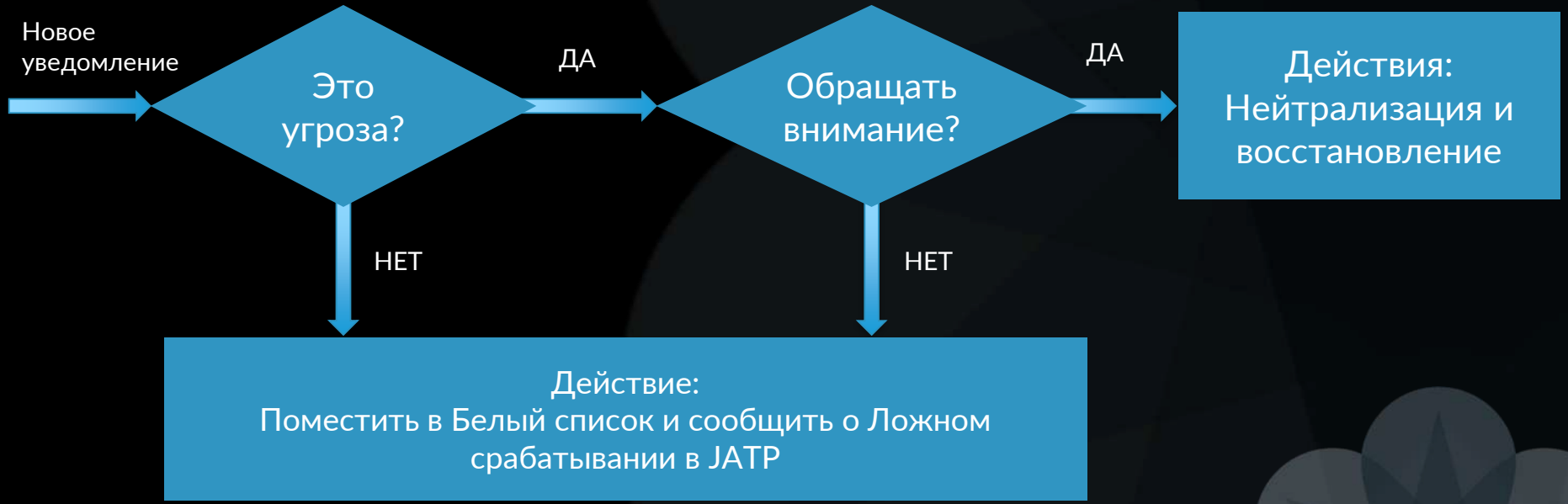


Продвинутая аналитика: консолидация и корреляция событий



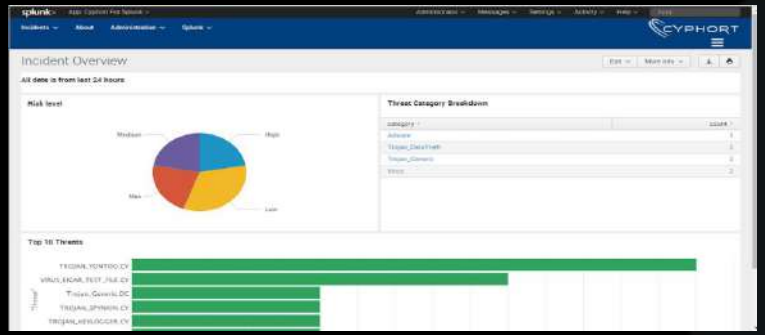
Открытая архитектура позволяет выполнять сбор логов из множества разных источников, сторонних решений. Корреляция и анализ в ядре JATP

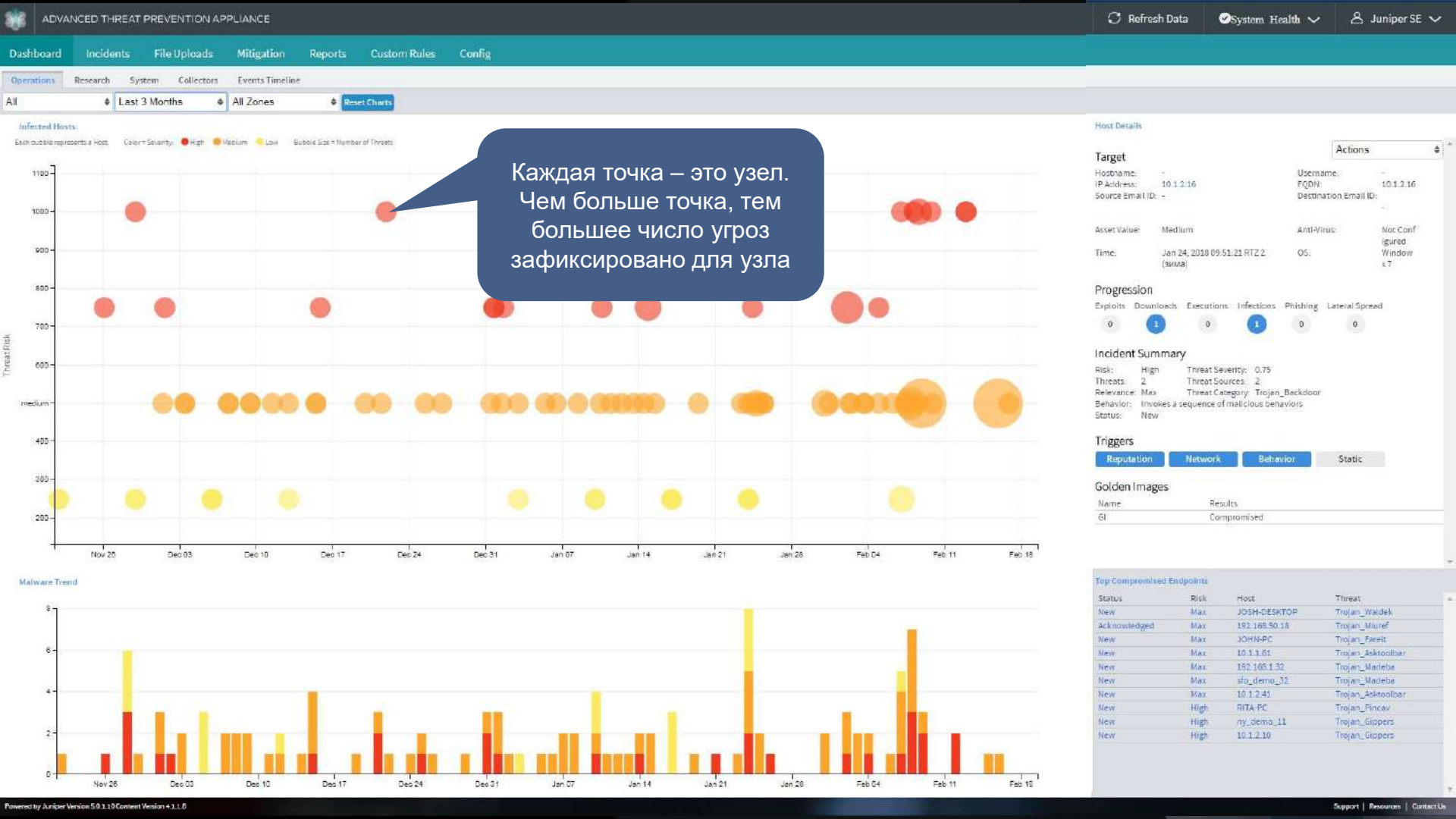
Упрощенный алгоритм IR



1. Идентификация

1. **Идентификация – Dashboard, Email, SIEM, API**
2. Расследование
3. Подтверждение
4. Действие




ADVANCED THREAT PREVENTION APPLIANCE
Refresh Data
System Health
Juniper SE
Dashboard
Incidents
File Uploads
Mitigation
Reports
Custom Rules
Config
Operations
Research
System
Collectors
Events Timeline
All
Last 3 Months
All Zones
Reset Charts
Infected Hosts
Each bubble represents a Host.
Color = Severity:
High
Medium
Low
Bubble Size = Number of Threats
Threat Risk
1100
1000
900
800
700
600
medium
400
300
200
Nov 26
Dec 03
Dec 10
Dec 17
Dec 24
Dec 31
Jan 07
Jan 14
Jan 21
Jan 28
Feb 04
Feb 11
Feb 18
Malware Trend
8
6
4
2
0
Nov 26
Dec 03
Dec 10
Dec 17
Dec 24
Dec 31
Jan 07
Jan 14
Jan 21
Jan 28
Feb 04
Feb 11
Feb 18
Каждая точка – это узел. Чем больше точка, тем большее число угроз зафиксировано для узла
Host Details
Actions
Target
Hostname:
IP Address: 10.1.2.16
Source Email ID:
Username:
FQDN: 10.1.2.16
Destination Email ID:
Asset Value: Medium
Anti-Virus: Not Configured
Time: Jan 24, 2019 09:51:21 RTZ 2 (зима)
OS: Windows 7
Progression
Exploits
Downloads
Executions
Infections
Phishing
Lateral Spread
0
1
0
1
0
0
Incident Summary
Risk: High
Threats: 2
Relevance: Max
Behavior: Invokes a sequence of malicious behaviors
Status: New
Threat Severity: 0.75
Threat Sources: 2
Threat Category: Trojan_Backdoor
Triggers
Reputation
Network
Behavior
Static
Golden Images
Name
Results
GI
Compromised
Top Compromised Endpoints
Status
Risk
Host
Threat
New
Max
JOSH-DESKTOP
Trojan_Waldek
Acknowledged
Max
192.168.50.18
Trojan_Maref
New
Max
JOHN-PC
Trojan_Fareit
New
Max
10.1.1.61
Trojan_Asktoolbar
New
Max
192.168.1.32
Trojan_Madebe
New
Max
sfo_demo_32
Trojan_Madebe
New
Max
10.1.2.41
Trojan_Asktoolbar
New
High
RITA-PC
Trojan_Pincav
New
High
ny_demo_11
Trojan_Gippers
New
High
10.1.2.10
Trojan_Gippers
Powered by Juniper Version 5.0.1.10 Content Version 4.1.1.6
Support | Resources | Contact Us

All Incidents (64 shown, 64 total)

Search: | Show Threat | All Zones | Last Week | csv

Status	Incident ID	Risk	Threat	Progression	Collector Type	Threat Source	Threat Target	Zone	Target OS	Collector	Date & Time
New	4977	MAX	TROJAN_LMN.DC	DL	Web	pbjadaidd.pfvevgqji.com	sfo_demo_38	Zone-1	Windows 7	demo next x collector	Feb 2 10:11:03 PST
New	4976	LOW	PoisonIvy_2_RAT_static	DL	Web	sj_test_20	sj_test_34	Zone-1	Windows 7	demo next x collector	Feb 2 10:05:01 PST
New	4712	HIGH	TROJAN_Gippers.CY	IN		newcard.dyndns.biz	10.1.2.100	Zone-1		demo next x collector	Feb 2 03:15:43 PST
New	4975	HIGH	TROJAN_GIPPERS.DC	DL	Web	greatfilesarey.asia	ny_demo_100	Zone-1	Windows 7	demo next x collector	Feb 2 03:13:43 PST
New	4974	MAX	RANSOM_LOCKY.DC	DL	Web	dckiywy.aalmb.com	sfo_demo_37	Zone-1	Windows 7	demo next x collector	Feb 1 22:11:01 PST
New	4973	MAX	TROJAN_FAREIT.DC	DL	Web	phdkcegkt.oktrrs.com	sfo_demo_33	Zone-1	Windows 7	demo next x collector	Feb 1 16:11:01 PST
New	4720	MAX	TROJAN_Trojan.CY	DL+IN	Web	193.106.172.140	10.1.1.100	Zone-1	MacOS Macintosh X 10.7.3	demo next x collector	Feb 1 15:07:02 PST
New	4972	LOW	TROJAN_BAGSU.DC	DL	Web	greatfilesarey.asia	sample_100	Zone-1	MacOS Macintosh X 10.7.3	demo next x collector	Feb 1 15:05:01 PST
New	4971	HIGH	WORM_VERST.DC	DL	Web	greatfilesarey.asia	sj_demo_135	Zone-1	unknown	demo next x collector	Feb 1 13:05:01 PST
New	4970	HIGH	TROJAN_PATCHED.DC	PHS+DL	Web	greatfilesarey.asia	email_user2	Zone-1	unknown	demo next x collector	Feb 1 10:55:02 PST
New	4969	MAX	TROJAN_SKIDLO.DC	DL	Web	dnltprr.efombqoe.com	sfo_demo_40	Zone-1	Windows 7	demo next x collector	Feb 1 10:11:01 PST
New	4968	LOW	PoisonIvy_2_RAT_static	DL	Web	sj_test_20	sj_test_34	Zone-1	Windows 7	demo next x collector	Feb 1 10:05:01 PST
New	4967	MAX	TROJAN_WALDEK.DC	DL	Web	ppeupmfohh.qxlpold.com	sfo_demo_41	Zone-1	Windows 7	demo next x collector	Feb 1 04:11:07 PST
New	4966	MAX	TROJAN_MADEBA.DC	DL	Web	mvlsxut.sagldz.com	sfo_demo_32	Zone-1	Windows 7	demo next x collector	Jan 31 22:11:07 PST
New	4965	MAX	TROJAN_DYNAMER.DC	DL	Web	yulvylssaq.ujuqvm.com	sfo_demo_35	Zone-1	Windows 7	demo next x collector	Jan 31 16:11:06 PST
New	4964	LOW	TROJAN_BAGSU.DC	DL	Web	greatfilesarey.asia	sample_100	Zone-1	MacOS Macintosh X 10.7.3	demo next x collector	Jan 31 15:05:02 PST
New	4963	HIGH	WORM_VERST.DC	DL	Web	greatfilesarey.asia	sj_demo_135	Zone-1	unknown	demo next x collector	Jan 31 13:05:01 PST

Details for TROJAN_ASKTOOLBAR.CY

Summary | Exploits | Downloads | Infections | Lateral Spread

Actions

Target:

Zone:	Zone-1
Hostname:	-
Username:	-
IP Address:	10.1.2.168
FQDN:	10.1.2.168
Source Email ID:	-
Destination Email ID:	-
Risk:	Max
Threat Category:	Unknown
Asset Value:	Medium
Target OS:	Windows 7
Relevance:	Max
OS Matched:	No
Virus Scanner Recognised:	AntiVirus not configured
Summary:	Max Risk Threat: infected by TROJAN_ASKTOOLBAR.CY
Collectors:	demo next x collector
Source:	10.2.19.51 (18.23.92.114) USA
Progression:	Exploit + Download + Infection + Lateral Spread
Protocol:	HTTP
Behavior:	Invokes a sequence of malicious function calls

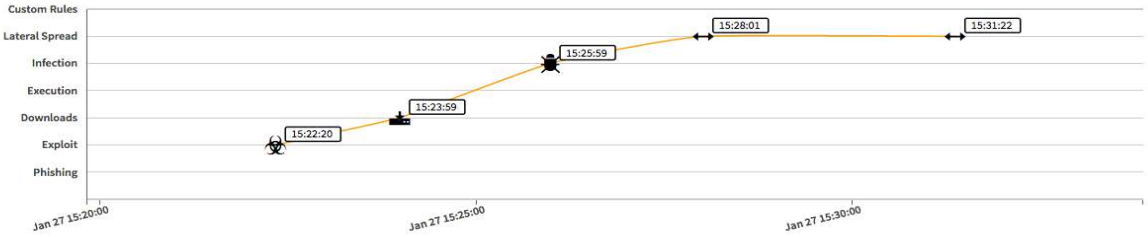
Progression:

DELIVERY > EXPLOITATION & INSTALLATION > COMMAND & CONTROL > ACTION ON TARGETS

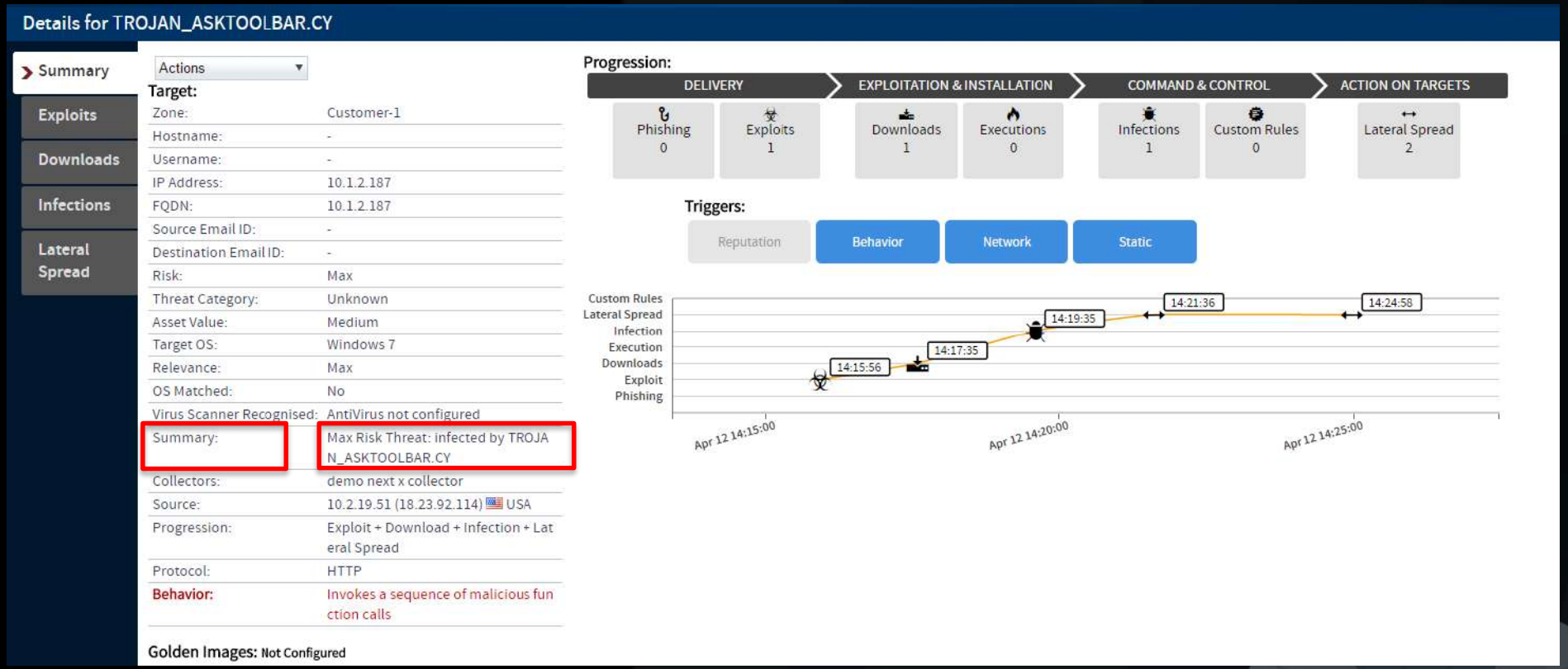
Phishing	Exploits	Downloads	Executions	Infections	Custom Rules	Lateral Spread
0	1	1	0	1	0	2

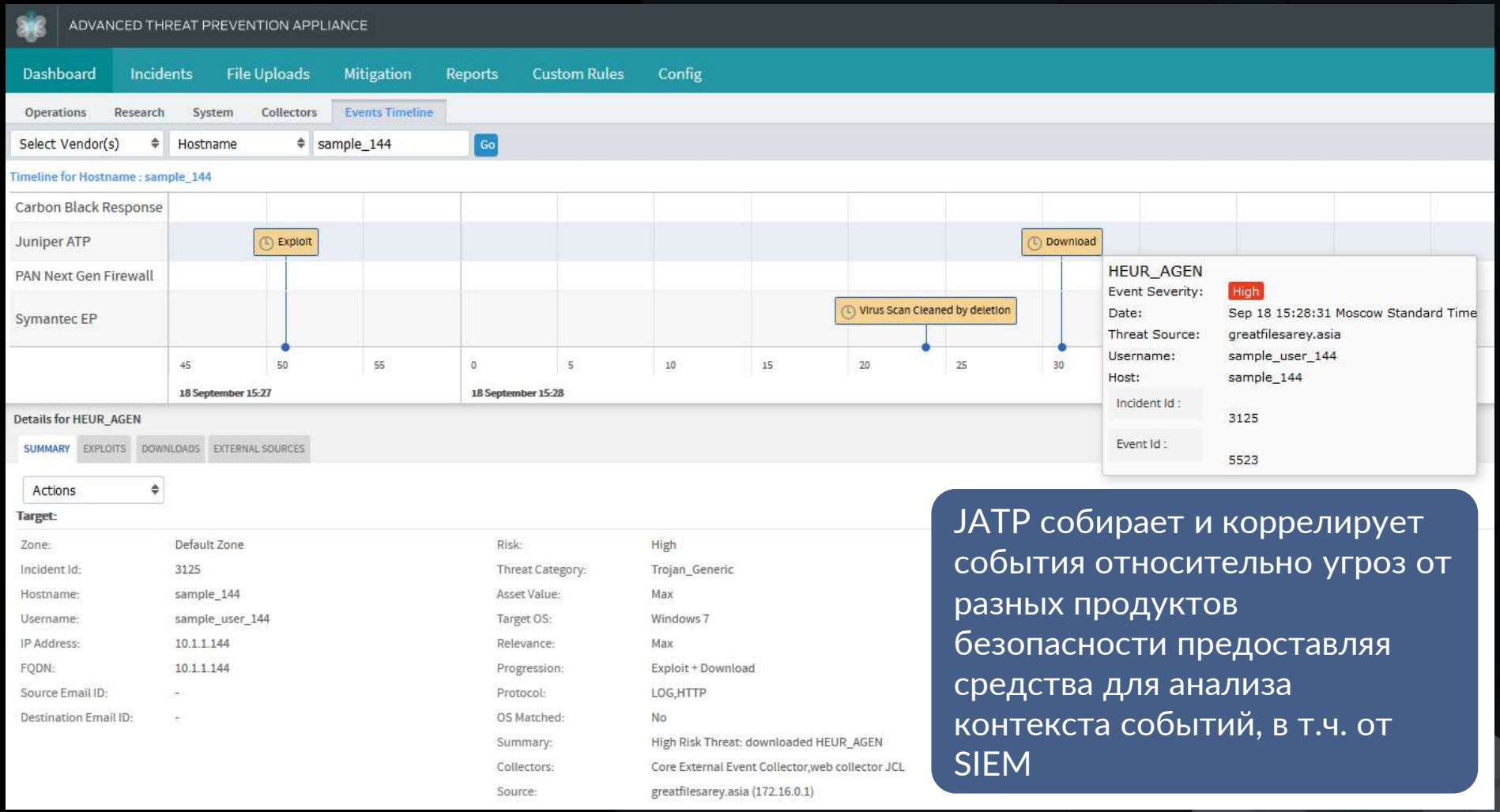
Triggers:

Reputation | Behavior | Network | Static



2. Расследование



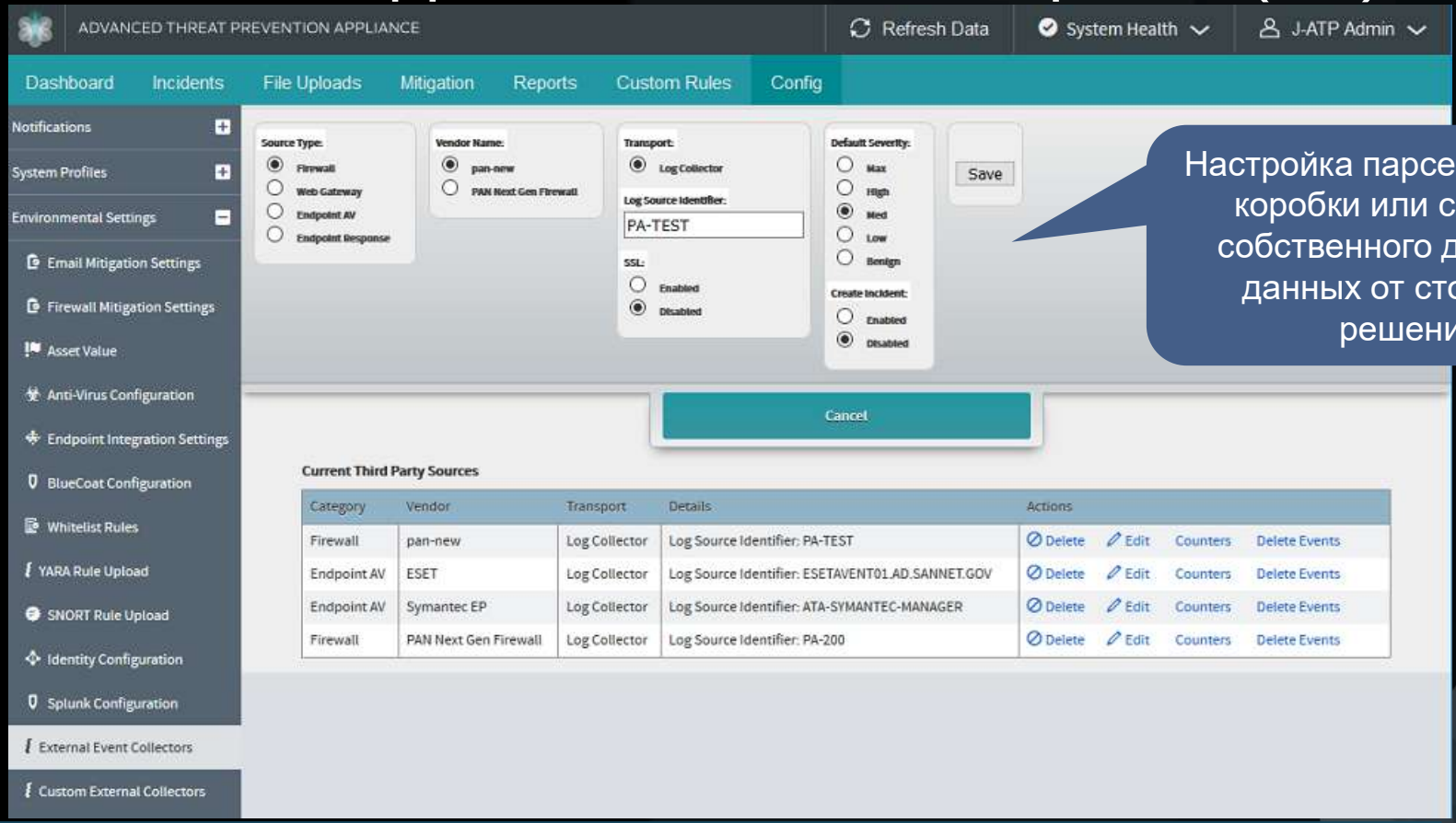


JATP собирает и коррелирует события относительно угроз от разных продуктов безопасности предоставляя средства для анализа контекста событий, в т.ч. от SIEM

Анализ и корреляция логов из коробки (1/2)

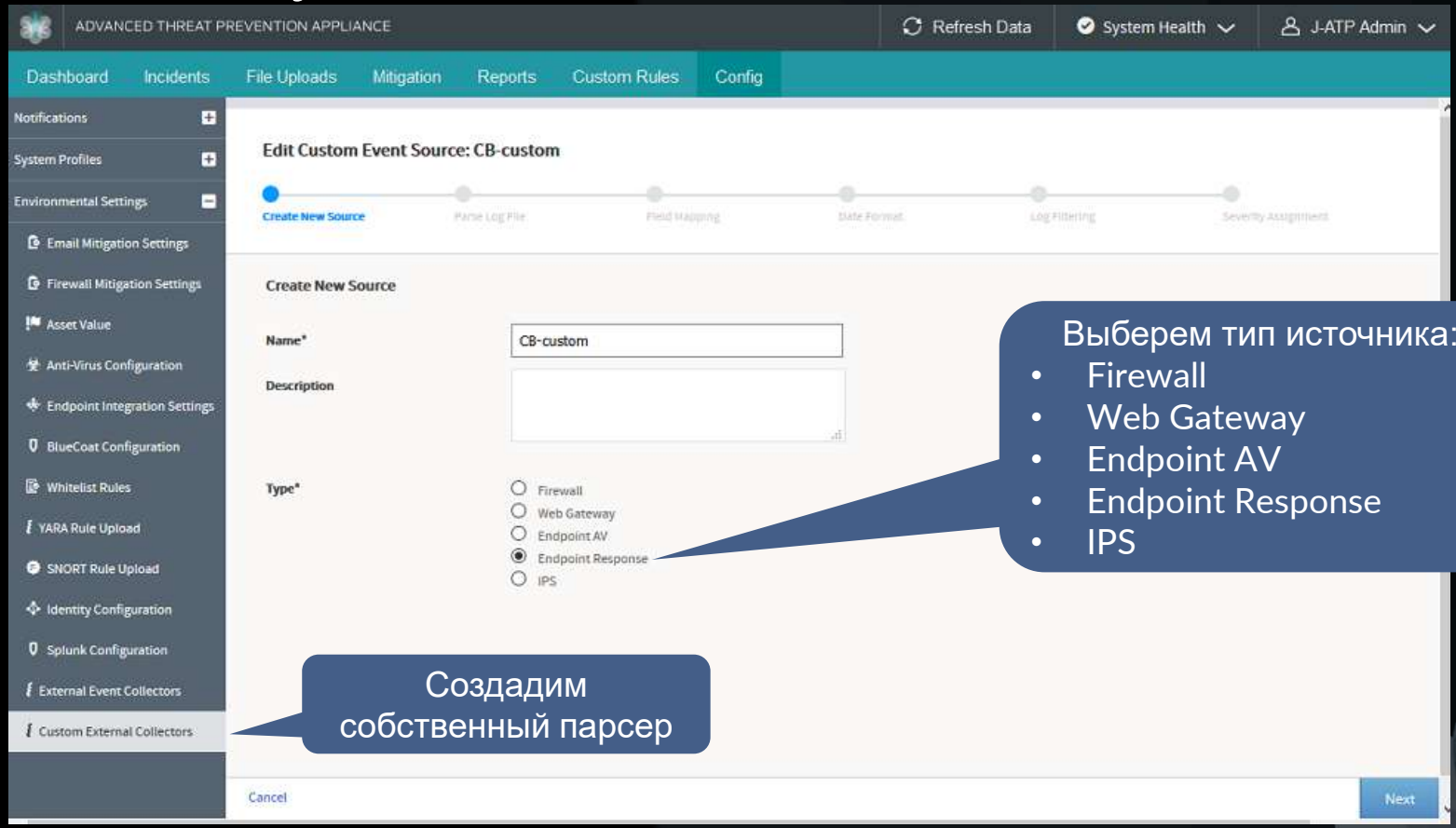
- Firewall:
  - Palo Alto Networks
- Security Web Gateway:
  - Symantec Blue Coat SWG
- Intrusion Prevention Systems
  - Palo Alto Networks
  - Juniper SRX
- Endpoint AV
  - ESET
  - McAfee ePO
  - Symantec EP
- Endpoint Detection & Response
  - CarbonBlack Response

Анализ и корреляция логов из коробки (2/2)



Настройка парсера логов из коробки или создание собственного для сбора данных от сторонних решений

А если нужно понимать еще какие-то логи?

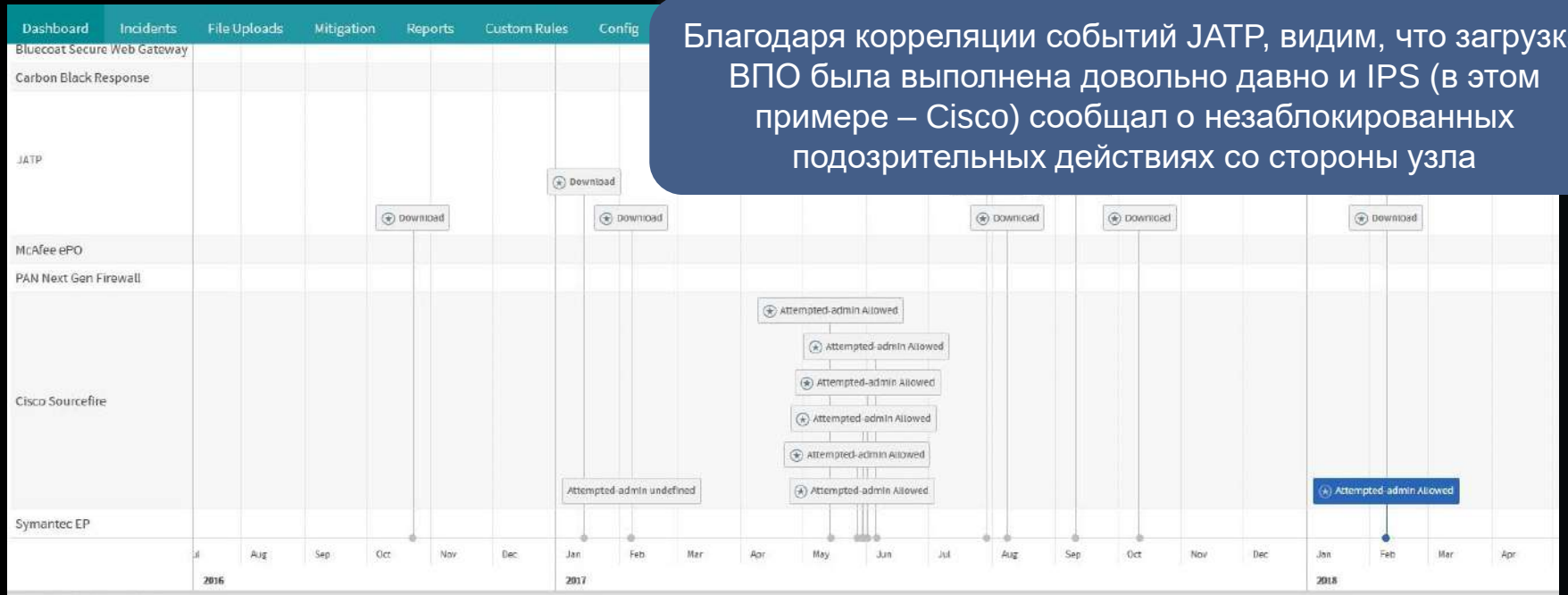


Выберем тип источника:

- Firewall
- Web Gateway
- Endpoint AV
- Endpoint Response
- IPS

Создадим собственный парсер

Благодаря корреляции событий JATP, видим, что загрузка ВПО была выполнена довольно давно и IPS (в этом примере – Cisco) сообщал о незаблокированных подозрительных действиях со стороны узла



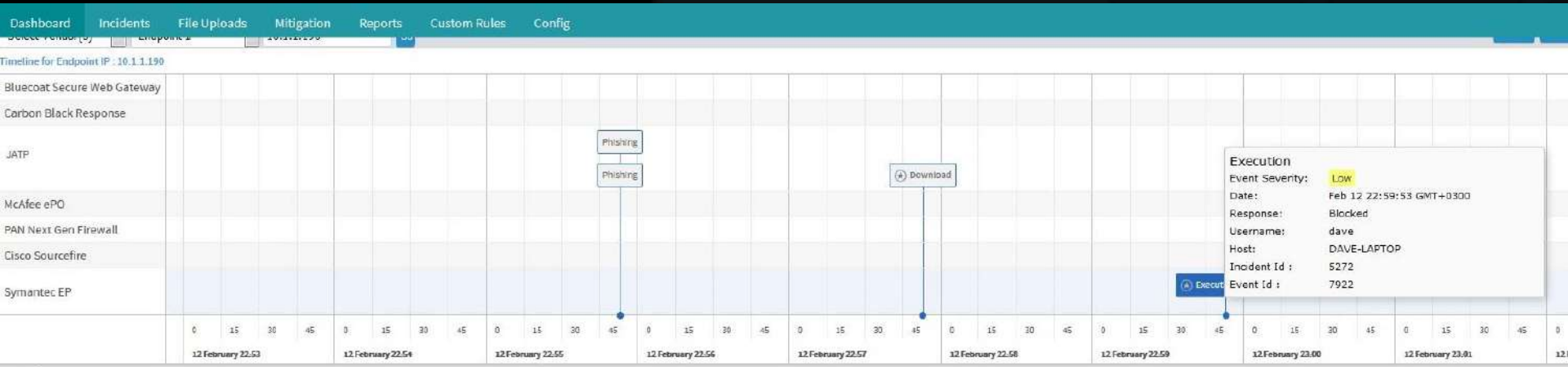
Details for TROJAN_Pincav.CY

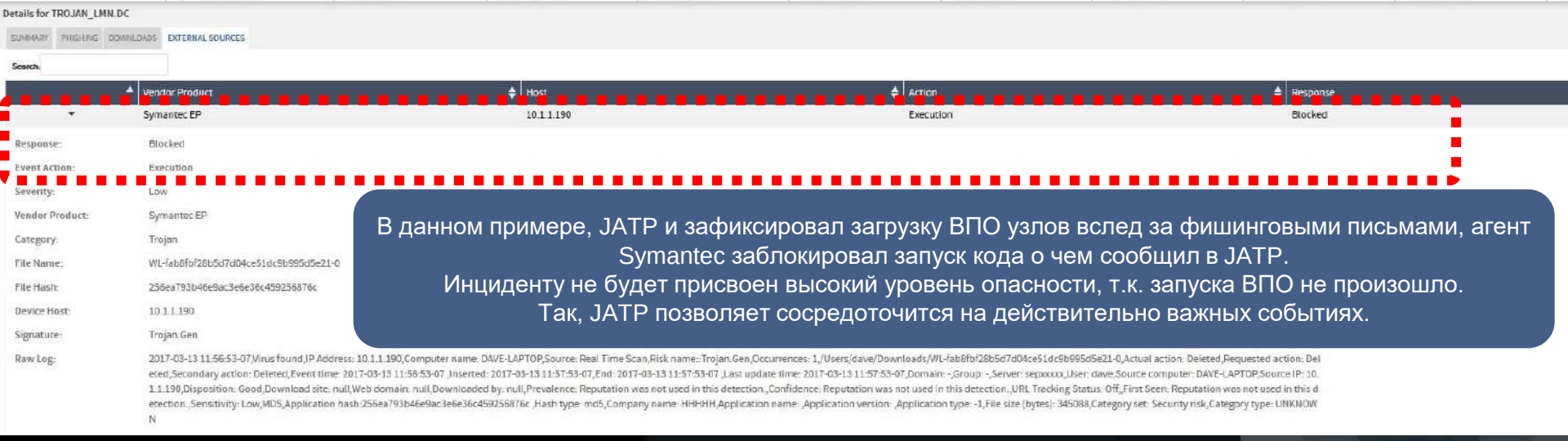
SUMMARY | DOWNLOADS | EXTERNAL SOURCES | INFECTIONS

Search:

	Vendor Product	Host	Action	Response
	Cisco Sourcefire	10.1.3.103	Attempted-admin	Allowed

Response:	Allowed
Event Action:	Attempted-admin
Severity:	Medium
Vendor Product:	Cisco Sourcefire
Device Host:	10.1.3.103
Raw Log:	rec_type=400 rec_type_simple=\"IPS EVENT\" event_sec=1489540087 event_usec=889189 sensor=10.0.0.1 http://10.0.0.1 event_id=11838 msg=\"EXPLOIT dhclient subnet mask option buffer overflow attempt\" sid=15700 gid=3 rev=2 class_desc=\"Attempted Administrator Privilege Gain\" class=attempted-admin priority=high src_ip=10.1.3.103 dest_ip=199.59.243.108 src_port=68 dest_port=68 ip_proto=UDP impact_flag=7 impact=2 blocked=No mpls_label=0 vlan_id=0 ids_policy=\"VRT Provided Strikes - IPS Policy\" user=User18 web_app=Unknown client_app=\"DHCP client\" app_proto=DHCP fw_rule=\"IPS and File Detection\" fw_policy=\"TSG PROD\" iface_ingress=s1p1 iface_egress=s1p2 sec_zone_ingress=Internal sec_zone_egress=External connection_second=1489540087 connection_instance_id=1 connection_counter=59340 src_ip_country=unknown dest_ip_country=unknown\n





В данном примере, JATP и зафиксировал загрузку ВПО узлов вслед за фишинговыми письмами, агент Symantec заблокировал запуск кода о чем сообщил в JATP.
Инциденту не будет присвоен высокий уровень опасности, т.к. запуска ВПО не произошло.
Так, JATP позволяет сосредоточится на действительно важных событиях.

Search:

	Severity	Threat Name	File Type	Collector
▼	0.75	Trojan_Generic.DC	PE32 executable (console) Intel 80386, for MS Windows	demo next x collector

1

Threat Name:	Trojan_Generic.DC
Threat Category:	Trojan_Generic
Captured From:	HTTP Traffic
Source:	18.23.92.114
Source Address:	vibmdyapl.idlima.com (18.23.92.114) USA
Source URL:	http://vibmdyapl.idlima.com/IOAYWqBH/IIGDKC.html, Alexa Rank: -1
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Golden Images:	
File Size:	159,744 (156KB), MIME type: application/octet-stream
File Hashes:	MD5: 18ccf42cc51f02a59803bc995ac16fdb SHA1: 7fab7695a10b101ae240c5f4e87553fcc0cf06d5 SHA256: 9ee2d976ff311c47311396508f0dfcbafee2298361dce78e54eb8ae51e8d1dd5
Signed by:	N/A
Malware Referrer URL:	N/A

2

3

5

Find on VirusTotal
Download Sample
Download Behavior Log

6

Generate IVP
Add to Whitelist
Report False Positive

Screenshot

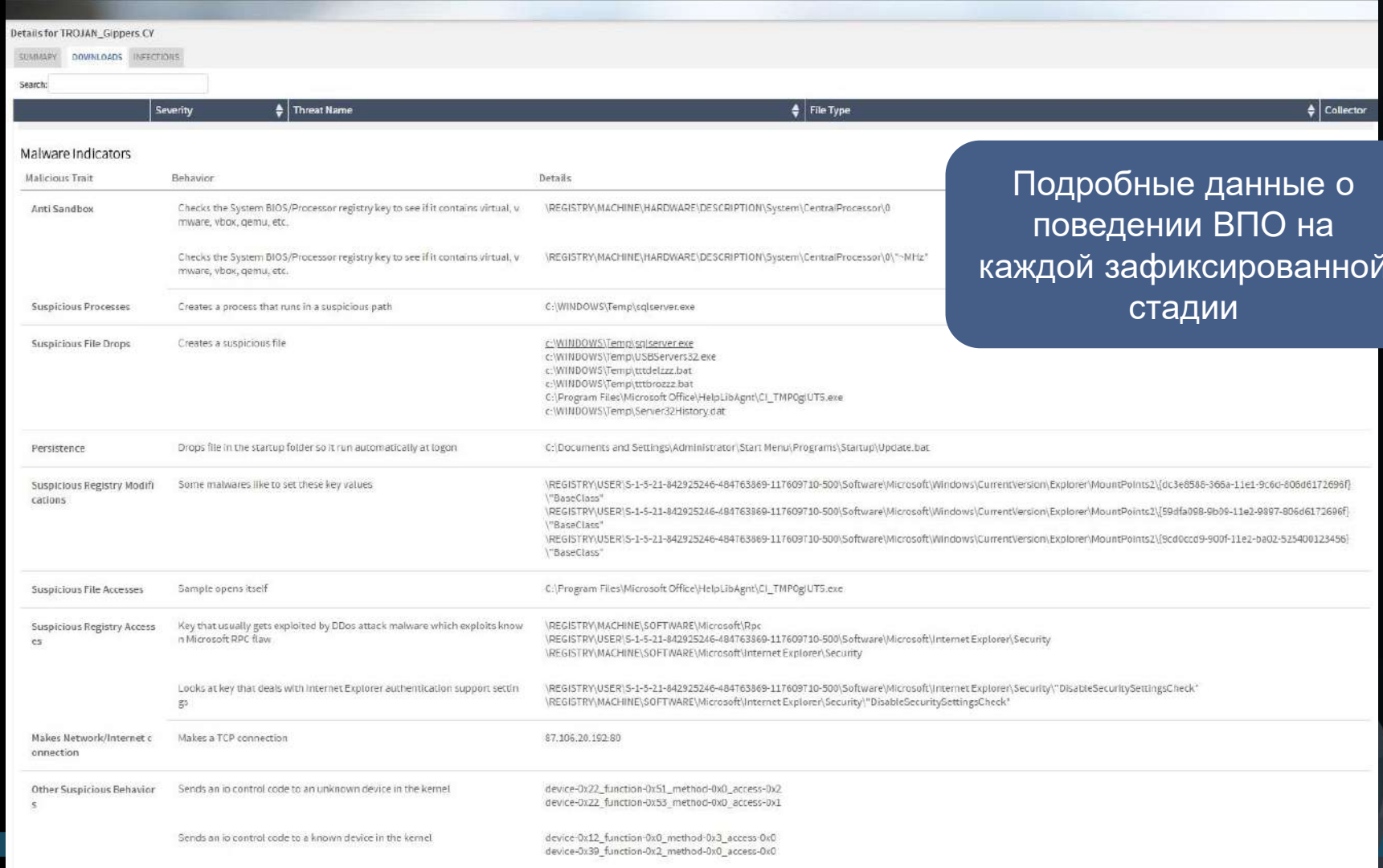
History

Analysis Timestamps:	Apr 4 11:19:50 Pacific Daylight Time High

4

Behavior Information

Top Indicators:	Creates a process in some suspicious paths which are temporary in nature (1) Sets a page of memory to EXECUTE Masquerades as standard Windows component (1) Sleeps for an excessive amount of time Highest total committed memory for a process in a cook
VM Network Callbacks:	None
Anti-Debugging:	None



Подробные данные о поведении ВПО на каждой зафиксированной стадии

Переместимся в раздел с информацией о событиях, свидетельствующих об инфицировании узла.
Узел пытался связаться с C&C-сервером

POST http://newcard.dyndns.biz:80/result%3Fhl%3Den%26meta%3Dzkryttyqzmtqaalbieldmttmpfxsagn HTTP/1.1..Accept: */*..Accept-Language: en-us..User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)..Connection: close..Content-Length: 293..Content-Type: application/x-www-form-urlencoded..Encoding: gzip, deflate..Pragma: no-cache..Host: newcard.dyndns.biz:80....Mjtdkj..=;??<=?ACEGI.....!"#$%&'(,*+,^.r..afgnh....;<=B?@ABCD....v.....\]^_`abcdefghijklmnopqrstuvwxyz{|}~.....+47=/..2@E5C.....`.W...c.
...&.%..... !"#$...

ADVANCED THREAT PREVENTION APPLIANCE

Details for TROJAN_Gippers.CY

SUMMARY | DOWNLOADS | INFECTIONS

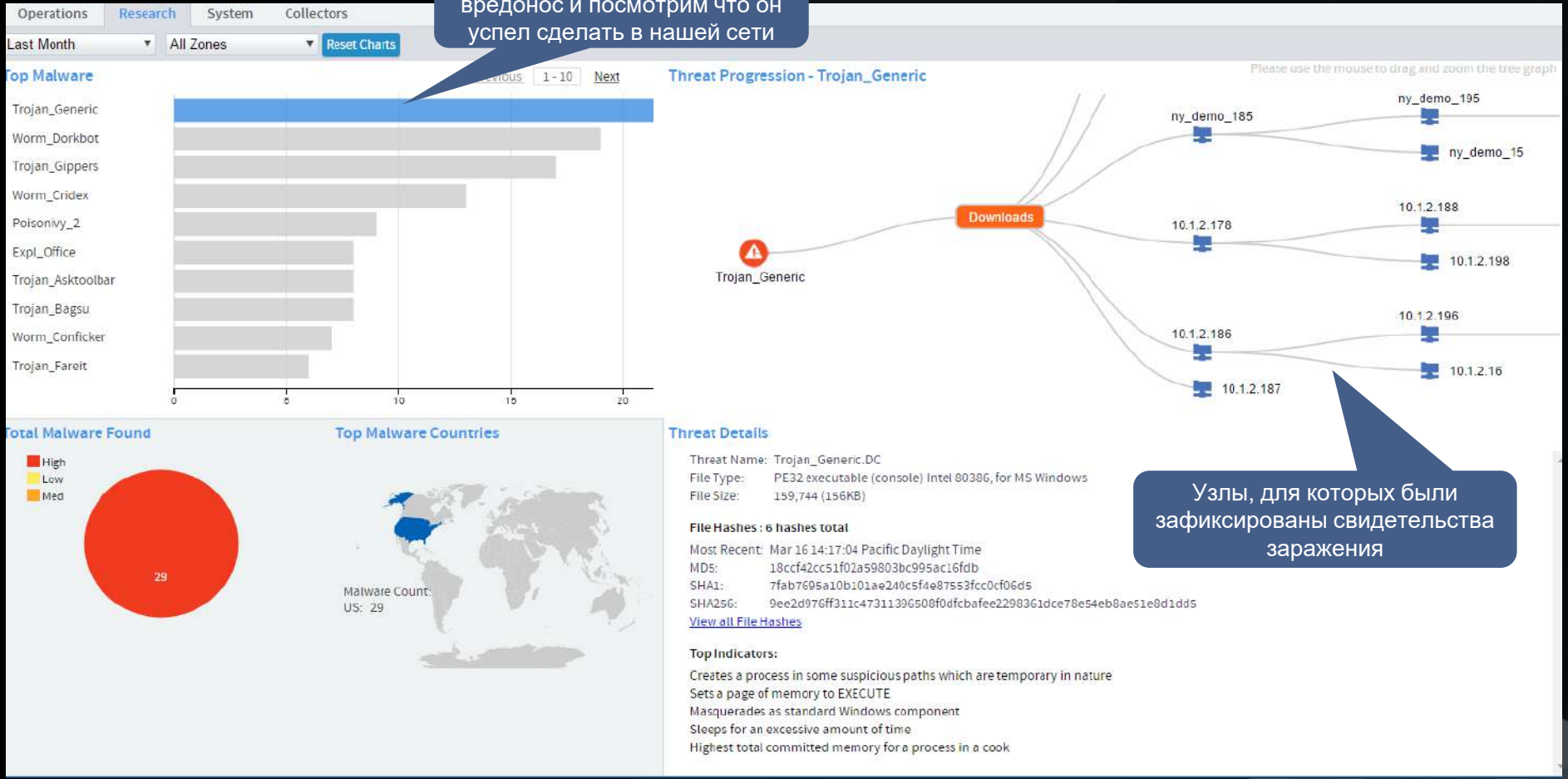
Infection Summary:

Name: TROJAN_Gippers.CY
Severity: High
Category: Trojan_Backdoor
Derived MD5: 015cb59778056a2689469bf38d6773e1 Find on VirusTotal
Collector: Sales Demo collector

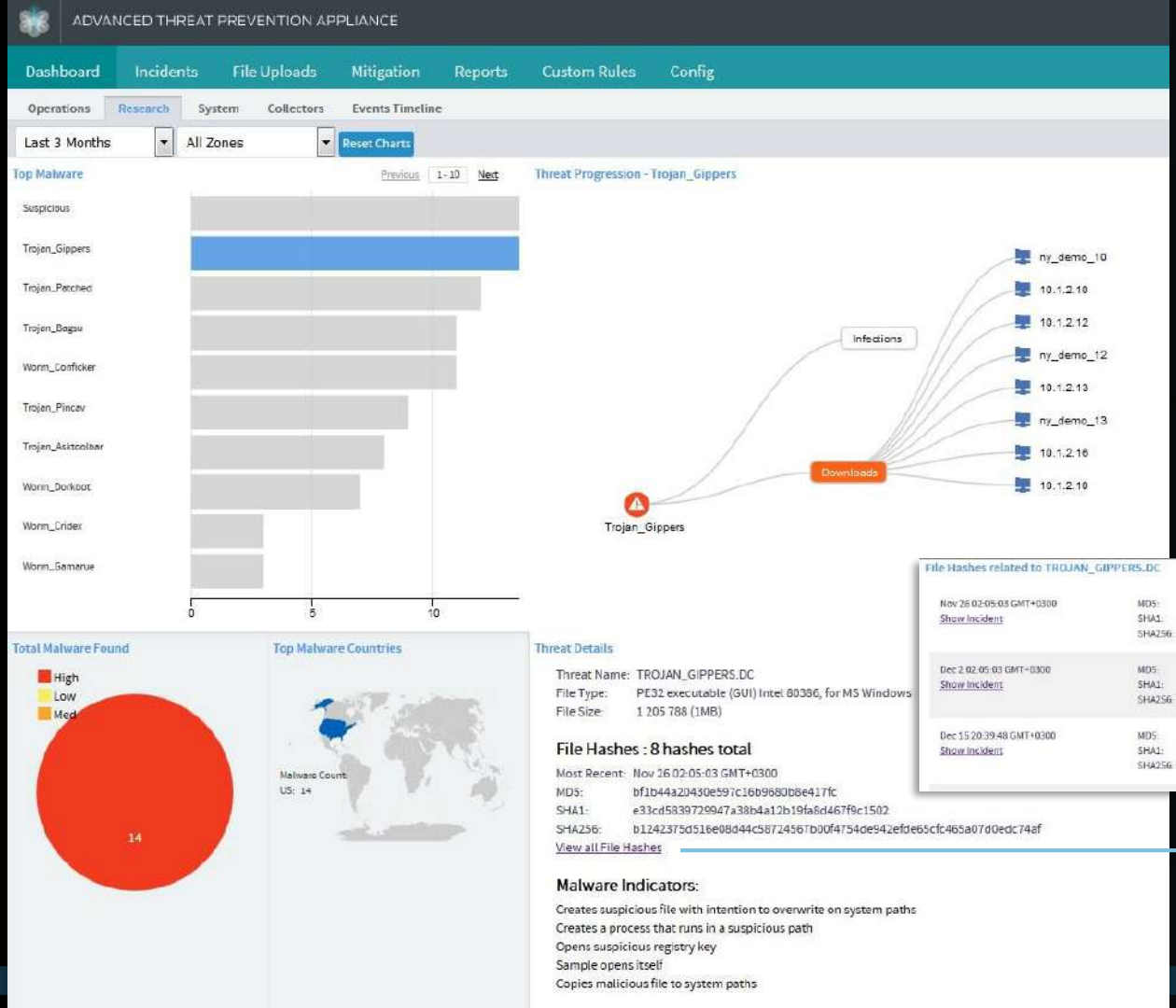
Network Information:

Date	Rule Id	Summary	CnC Server	Details	Actions
Jan 24 09:51:21 RTZ 2 (зима)	1990070	CY TROJAN TrojanDownloader:Win32/Gippers.A Client Callback Attempt Detected 1990070	newcard.dyndns.biz	POST http://newcard.dyndns.biz:80/result%3Fhl%3Den%26meta%3Dzkryttyqzmtqaalbieldmttmpfxsagn HTTP/1.1..Accept: */*..Accept-Language: en-us..User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)..Connection: close..Content-Length: 293..Content-Type: application/x-www-form-urlencoded..Encoding: gzip, deflate..Pragma: no-cache..Host: newcard.dyndns.biz:80....Mjtdkj..=;??<=?ACEGI.....! Show Full Details	Add to Whitelist Report False Positive Download Signature
Jan 24 09:51:21 RTZ 2 (зима)	1990070	CY TROJAN TrojanDownloader:Win32/Gippers.A Client Callback Attempt Detected 1990070	newcard.dyndns.biz	POST http://newcard.dyndns.biz:80/result%3Fhl%3Den%26meta%3Diktbsairipsqjadekakoydecqbkatfj HTTP/1.1..Accept: */*..Accept-Language: en-us..User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)..Connection: close..Content-Length: 293..Content-Type: application/x-www-form-urlencoded..Encoding: gzip, deflate..Pragma: no-cache..Host: newcard.dyndns.biz:80....Mjtdkj..=;??<=?ACEGI.....! Show Full Details	Add to Whitelist Report False Positive Download Signature

Выберем конкретный вредонос и посмотрим что он успел сделать в нашей сети



Узлы, для которых были зафиксированы свидетельства заражения



Посмотрим кто из узлов загрузил Trojan_Gippers, детали о нем, индикаторы компрометации и хэш-суммы образцов

juniper NETWORKS

3. Подтверждение: VirusTotal

virustotal

SHA256: 33ba0d6289e63c85b7e7beb92c7ab981064392d82edfceb59a50e1895e3d75fa

File name: sarconsogulpe.exe

Detection ratio: 35 / 53

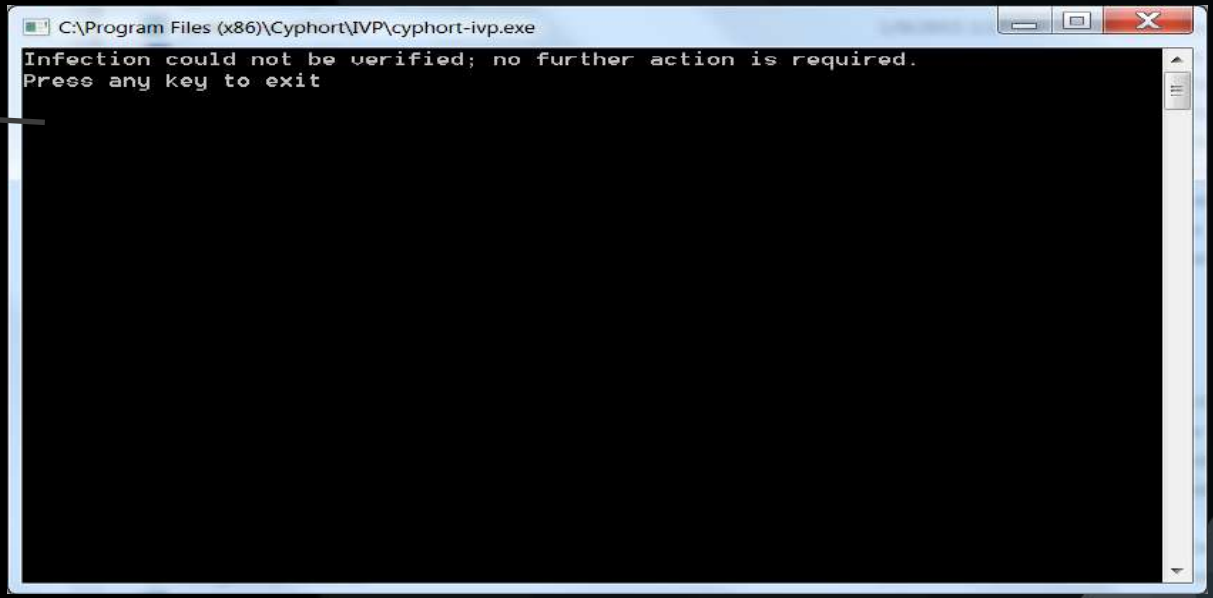
Analysis date: 2014-11-07 15:51:27 UTC (1 week, 5 days ago)

1 1

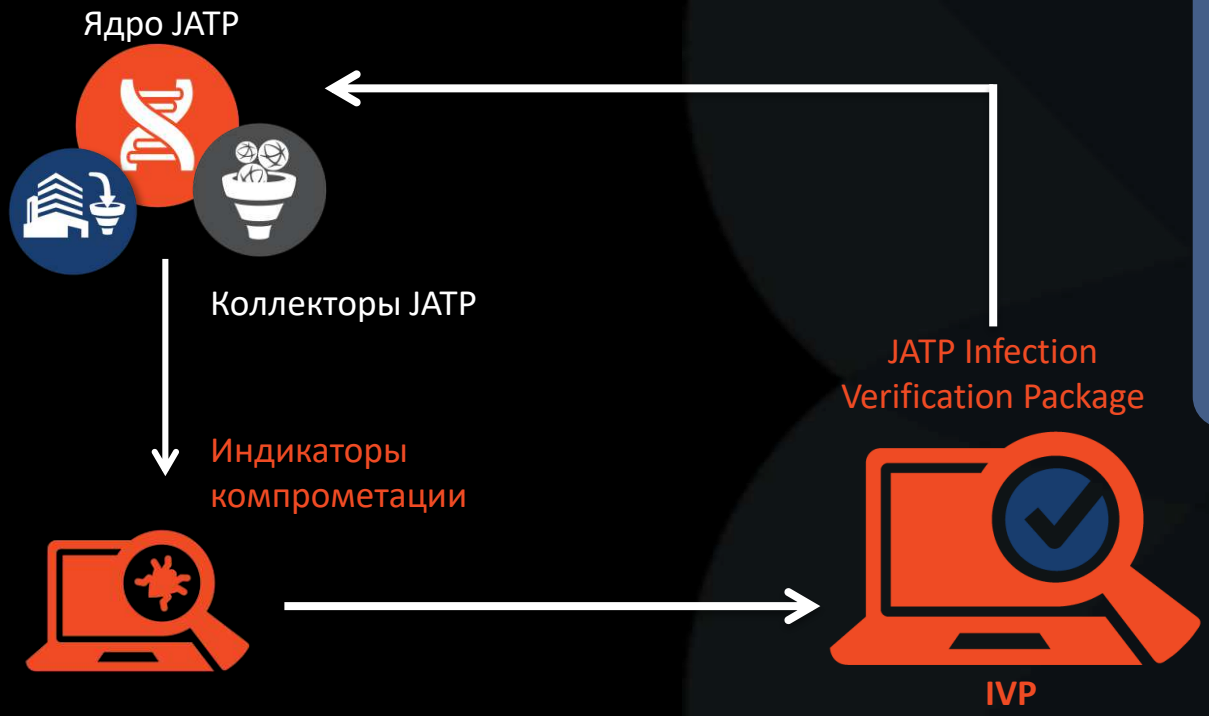
Analysis | File detail | Relationships | Additional information | Comments 0 | Votes | Behavioural information

Antivirus	Result	Update
AVG	Generic5.BRKI	20141107
AVware	Trojan.Win32.Generic!BT	20141107
Ad-Aware	Trojan.GenericKD.1875668	20141107
Agnitum	Trojan.Rogue!rrg7Qf4TcqE	20141107
Antiy-AVL	GrayWare[AdWare:not-a-virus]/Win32.Agent	20141107

3. Подтверждение: Infection Verification Pack (IVP)



Infection Verification Pack



JATP позволяет создать пакет IVP для запуска на оконечном узле для проверки заражен этот узел или нет.
IVP анализирует наличие индикаторов заражения (IoC).
IVP может быть загружен на подозрительный узел и запущен там для вынесения вердикта

Изменения в ОС:
Ключи реестра, созданные Mutex, запущенные процессы, загруженные файлы и т.д.

3. Подтверждение: проверка целевых узлов IVP

IP Filtering | URL Filtering | IPS Signatures | Endpoint Infection Verification | Emails

I·V·P

Endpoint Infections to be Verified

Search:

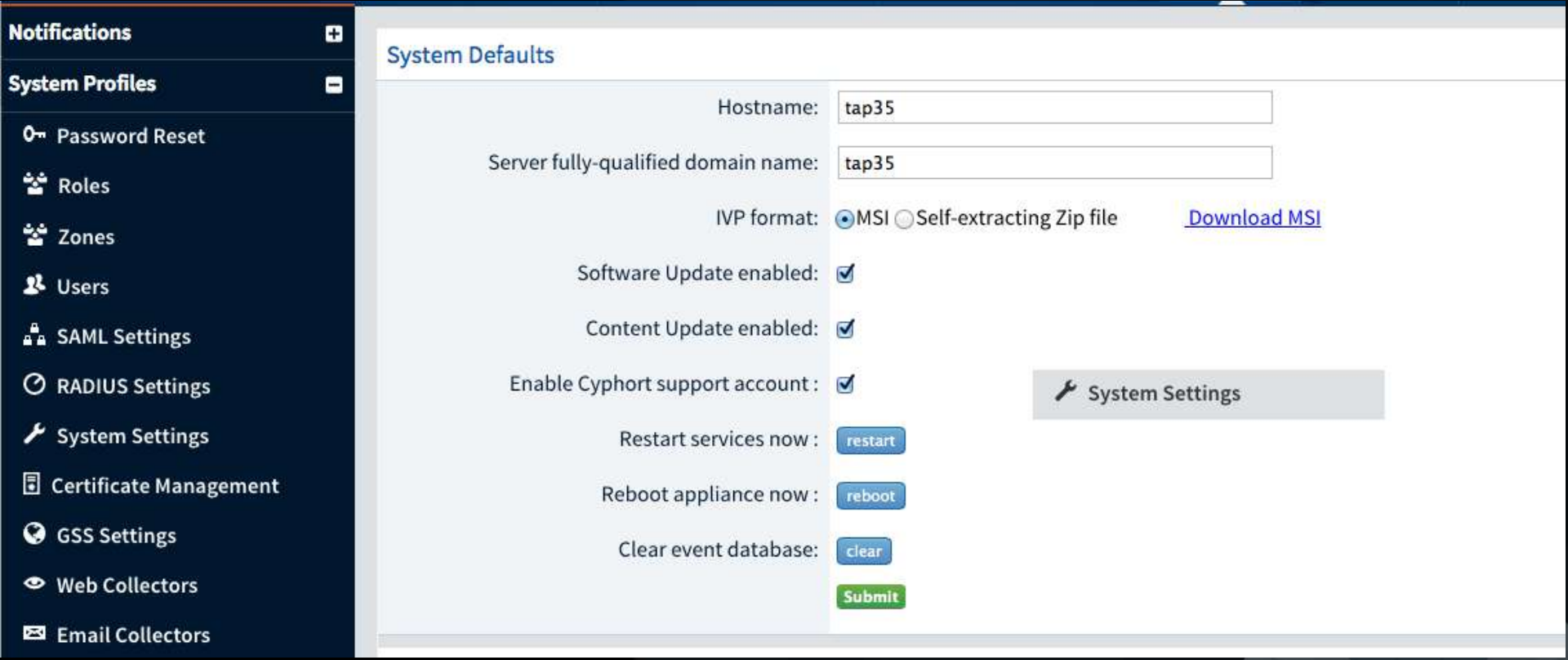
Severity	Target	Threat	Exposure Date	Action
HIGH	10.1.3.124	Trojan_Generic.DC	Apr 26 12:04:35 Pacific Daylight Time	Download IVP
HIGH	ny_demo_169	Trojan_Generic.DC	Dec 12 15:23:34 Pacific Daylight Time	Download IVP
HIGH	101.116.55.210	WORM_WECYKLER.DC	Jun 4 02:58:22 Pacific Daylight Time	Download IVP
HIGH	10.3.1.133	TROJAN_GIPPERS.DC	Jul 20 05:18:54 Pacific Daylight Time	Download IVP
HIGH	10.1.2.127	Trojan_Generic.DC	May 24 13:49:55 Pacific Daylight Time	Download IVP
HIGH	10.1.2.32	TROJAN_GIPPERS.DC	Apr 6 12:22:03 Pacific Daylight Time	Download IVP
HIGH	10.3.1.111	TROJAN_GIPPERS.DC	Jun 6 14:25:09 Pacific Daylight Time	Download IVP
HIGH	ny_demo_191	Trojan_Generic.DC	Oct 21 18:41:20 Pacific Daylight Time	Download IVP
HIGH	10.3.1.146	TROJAN_GIPPERS.DC	Aug 21 22:13:11 Pacific Daylight Time	Download IVP
HIGH	10.1.5.45	WORM_BRONTOK.DC	Jul 21 08:04:08 Pacific Daylight Time	Download IVP
HIGH	10.3.1.157	TROJAN_GIPPERS.DC	Sep 18 14:22:10 Pacific Daylight Time	Download IVP
HIGH	10.1.5.112	WORM_BRONTOK.DC	Nov 20 03:56:31 Pacific Daylight Time	Download IVP
HIGH	10.1.2.144	Trojan_Generic.DC	May 4 12:43:29 Pacific Daylight Time	Download IVP

Endpoint Infection Status

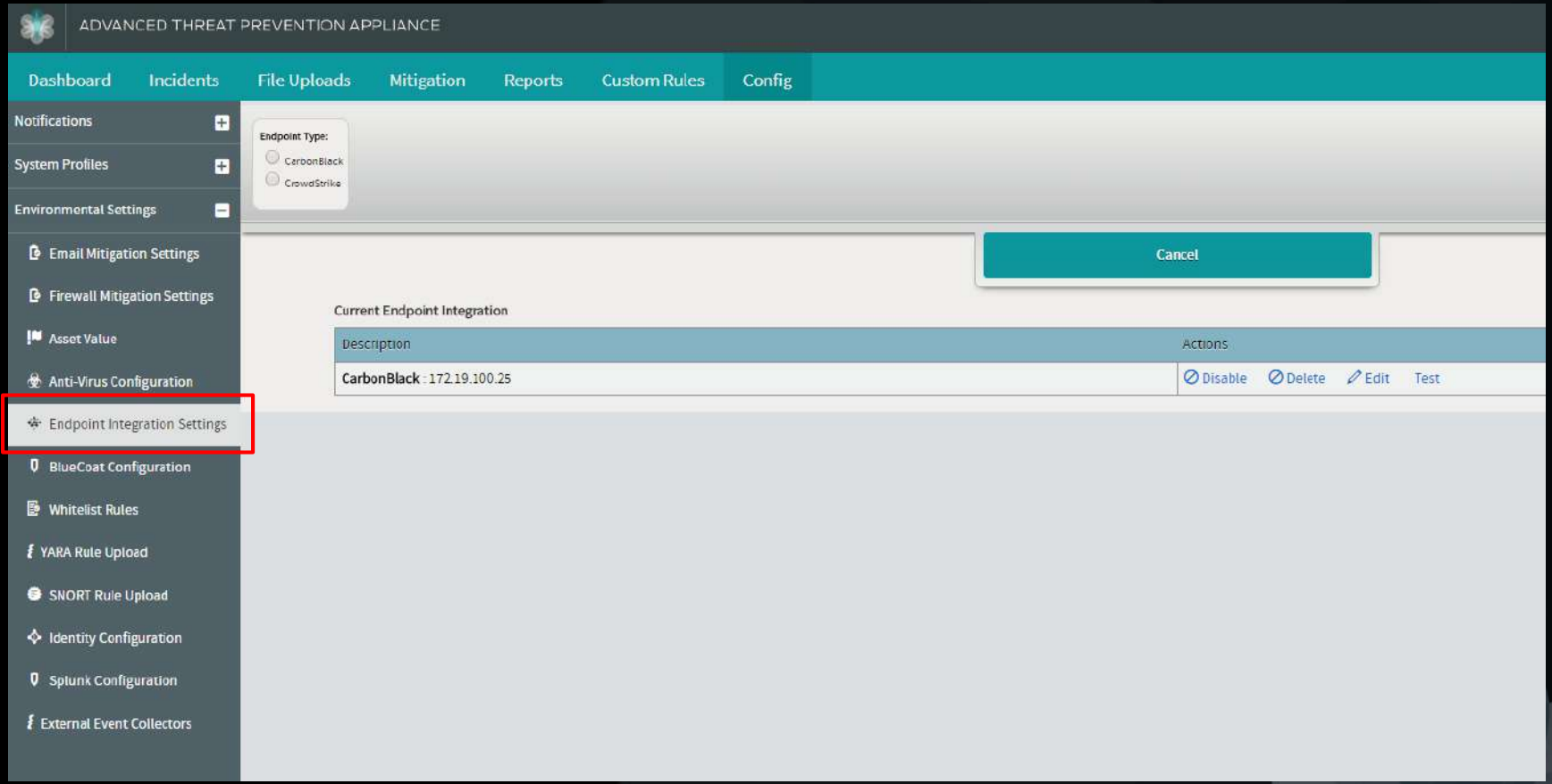
Search:

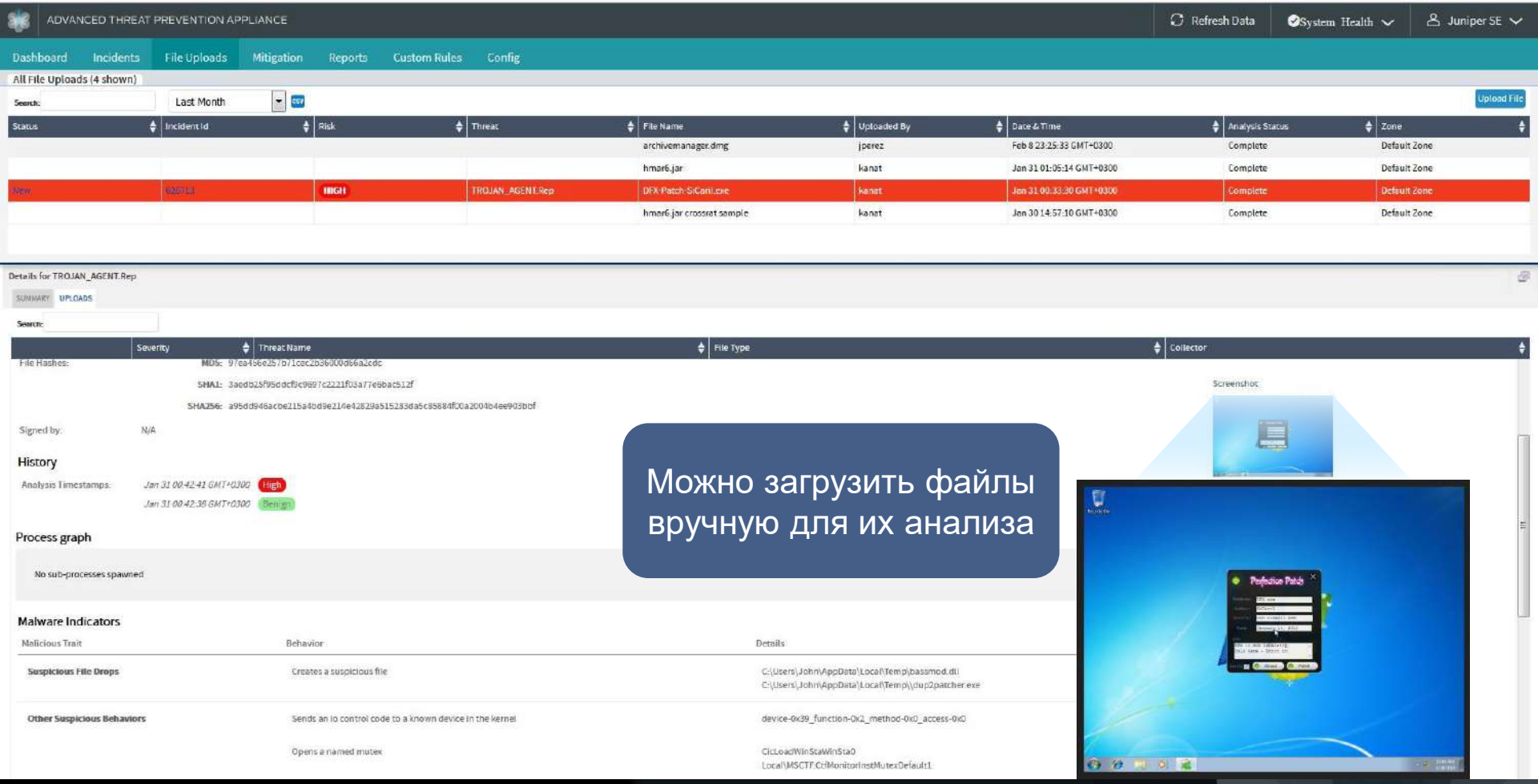
Severity	Target	Threat	Date Identified	Infection Status
HIGH	sj_test_160	TROJAN_GIPPERS.DC	Oct 6 15:21:40 Pacific Daylight Time	Unconfirmed

Infection Verification Pack



Интеграция с EDR

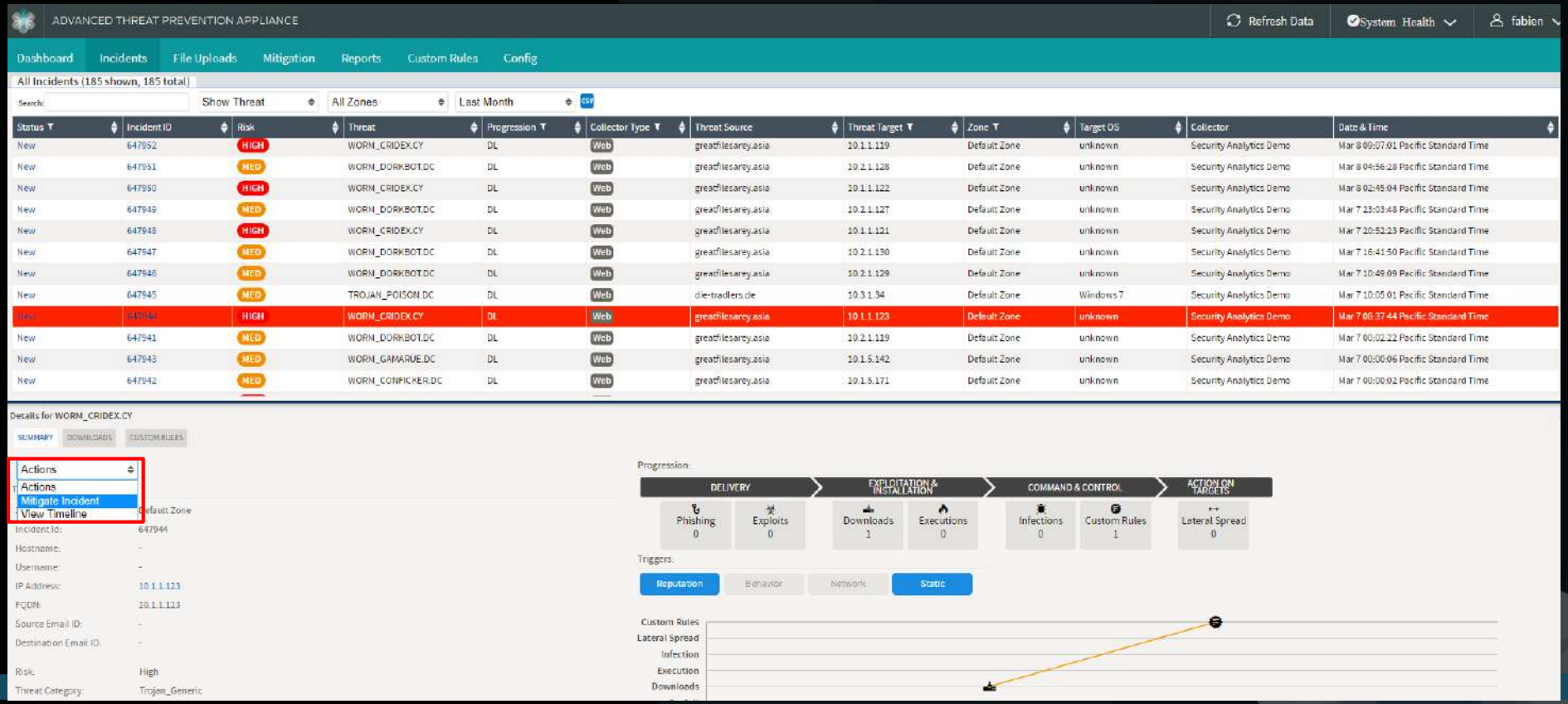




Можно загрузить файлы вручную для их анализа

4. Действие: переход от Инцидента к нейтрализации

Actions > Mitigate Incident



ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data | System Health | Juniper SE

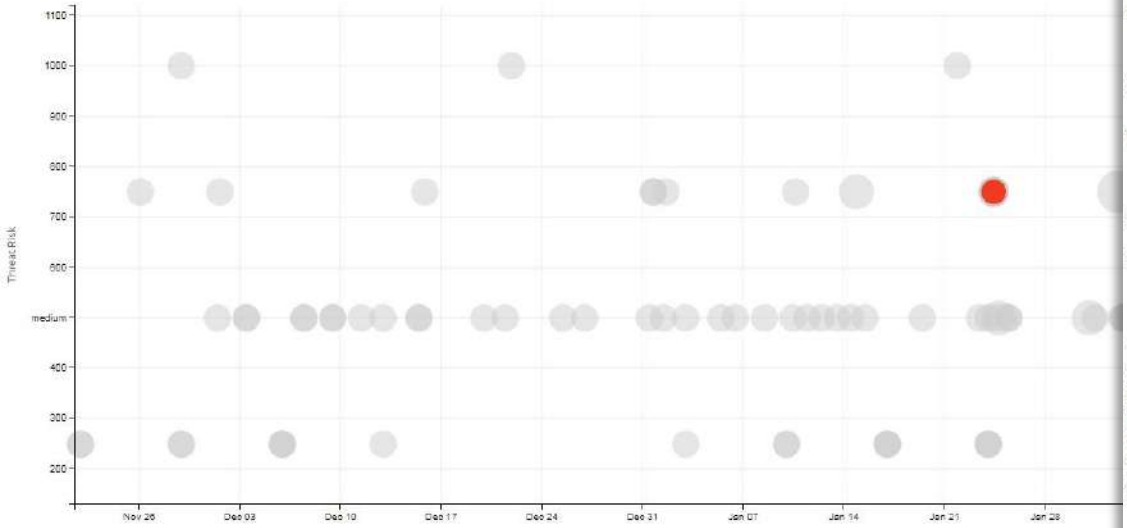
Dashboard | Incidents | File Uploads | Mitigation | Reports | Custom Rules | Config

Operations | Research | System | Collectors | Events Timeline

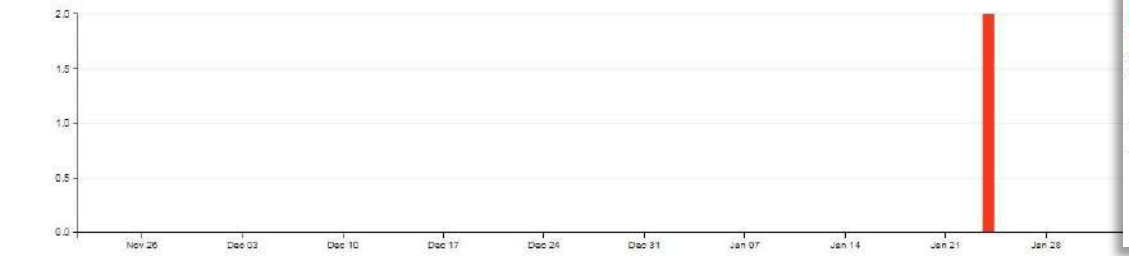
All | Last 3 Months | All Zones | Reset Charts

Infected Hosts:

Each bubble represents a Host. Color = Severity: High Medium Low Bubble Size = Number of Threats



Malware Trend



Host Details

Actions

- Actions
- View Incident
- View Timeline
- Mitigate Incident

Target

Hostname:	-	Usernan	
IP Address:	10.1.2.16	FQDN:	
Source Email ID:	-	Destinat	
Asset Value:	Medium	Anti-Virus:	Not Conf igured
Time:	Jan 24, 2018 09:51:21 RTZ 2 (зима)	OS:	Window s 7

Progression

Exploits	Downloads	Executions	Infections	Phishing	Lateral Spread
0	1	0	1	0	0

Incident Summary

Risk:	High	Threat Severity:	0.75
Threats:	2	Threat Sources:	2
Relevance:	Max	Threat Category:	Trojan_Backdoor
Behavior:	Invokes a sequence of malicious behaviors		
Status:	New		

Triggers

Reputation | Network | Behavior | Static

Golden Images

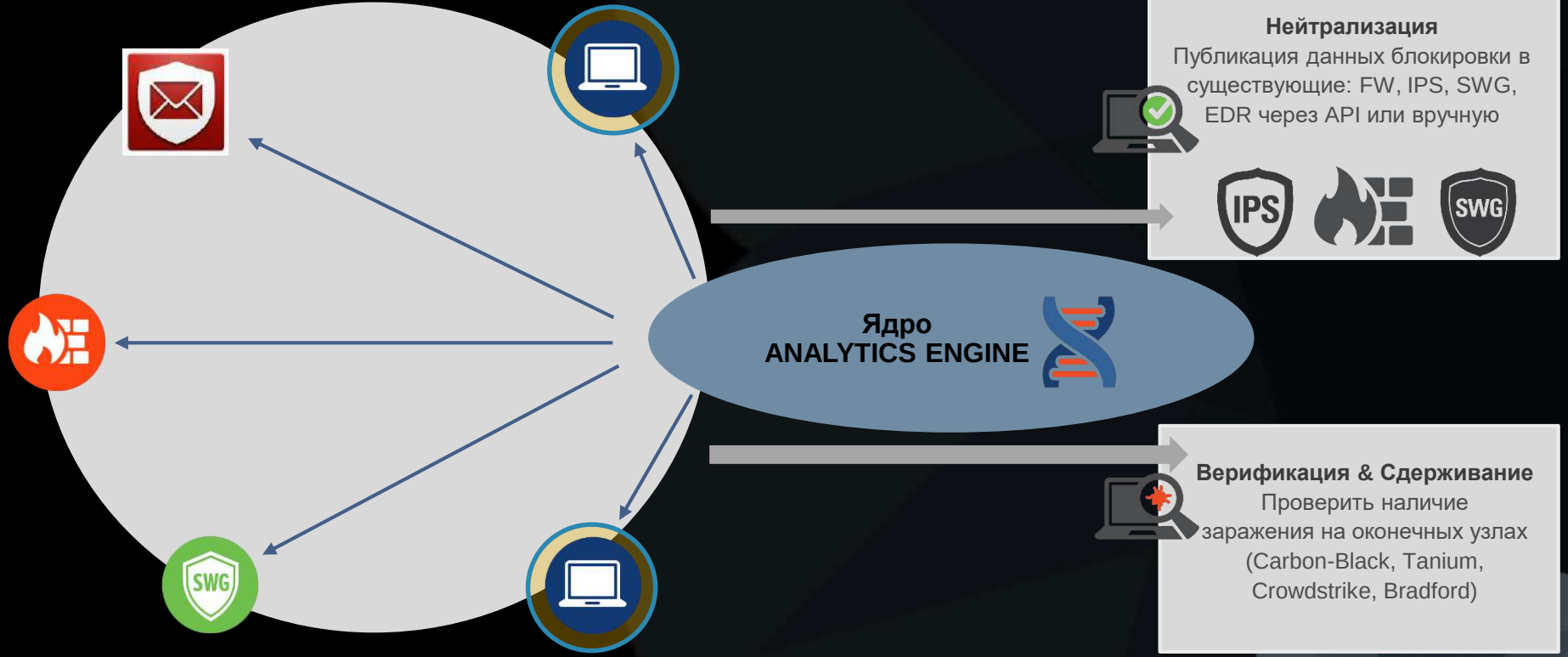
Name	Results
GI	Compromised

Переход в раздел Mitigation

Блокировка IP, URL, генерирование сигнатуры IPS, IVP, карантин почты

В разделе нейтрализации угроз можно выбрать действия для предотвращения заражения.
JATP умеет взаимодействовать со сторонними продуктами безопасности

Нейтрализация в один клик для команд Incident Response

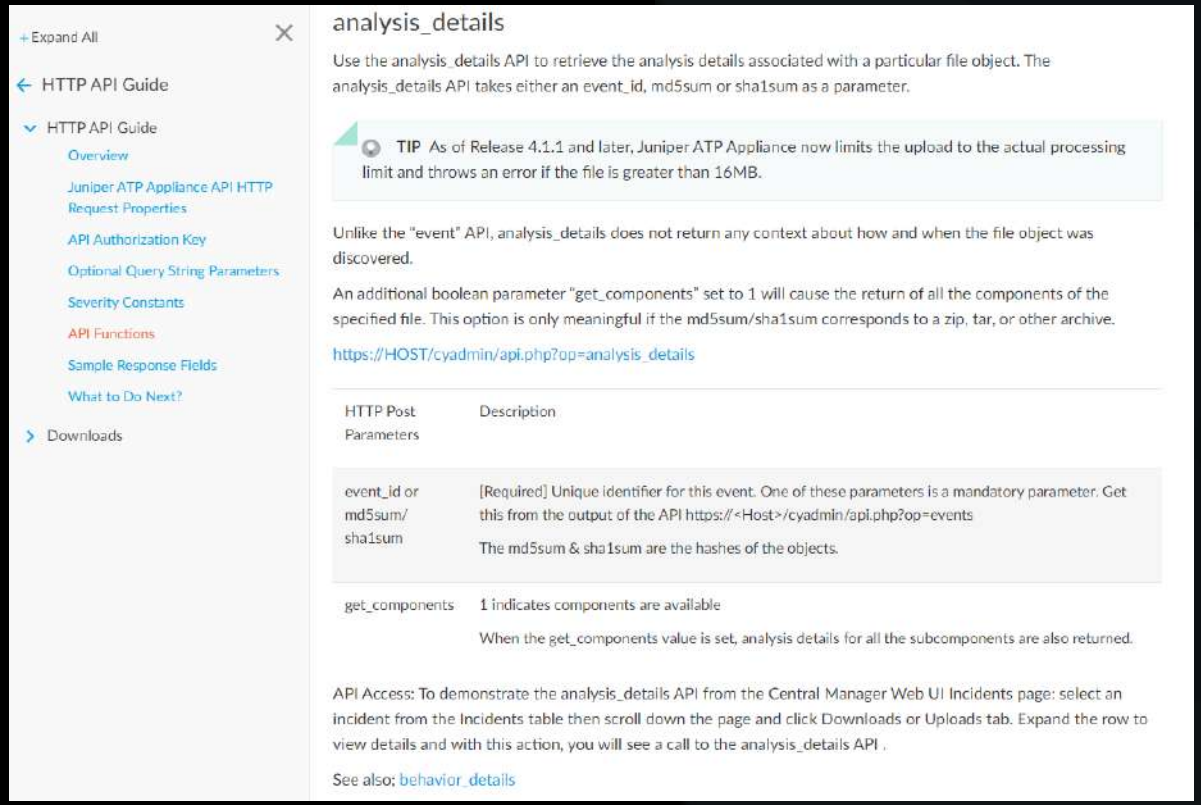


Нейтрализация угроз

- Интеграция с решениями EDP/EPP для получения информации о запуске вредоносного кода на узле, сообщения решению EDR о необходимости блокировки запуска кода
- Получение файлов от EDR/EPP для проверки (CarbonBlack)
- Взаимодействие со сторонними решениями через API или CLI для нейтрализации угрозы: блокировка IP, URL, создание сигнатуры IPS, помещение письма в карантин

HTTP API

Данные анализа по инциденту, деталей поведения и проч. через API



+Expand All

HTTP API Guide

- HTTP API Guide
  - Overview
  - Juniper ATP Appliance API HTTP Request Properties
  - API Authorization Key
  - Optional Query String Parameters
  - Severity Constants
  - API Functions
  - Sample Response Fields
  - What to Do Next?
- Downloads

analysis_details

Use the analysis_details API to retrieve the analysis details associated with a particular file object. The analysis_details API takes either an event_id, md5sum or sha1sum as a parameter.

TIP As of Release 4.1.1 and later, Juniper ATP Appliance now limits the upload to the actual processing limit and throws an error if the file is greater than 16MB.

Unlike the "event" API, analysis_details does not return any context about how and when the file object was discovered.

An additional boolean parameter "get_components" set to 1 will cause the return of all the components of the specified file. This option is only meaningful if the md5sum/sha1sum corresponds to a zip, tar, or other archive.

https://HOST/cyadmin/api.php?op=analysis_details

HTTP Post Parameters	Description
event_id or md5sum/ sha1sum	[Required] Unique identifier for this event. One of these parameters is a mandatory parameter. Get this from the output of the API https://<Host>/cyadmin/api.php?op=events The md5sum & sha1sum are the hashes of the objects.
get_components	1 indicates components are available When the get_components value is set, analysis details for all the subcomponents are also returned.

API Access: To demonstrate the analysis_details API from the Central Manager Web UI Incidents page: select an incident from the Incidents table then scroll down the page and click Downloads or Uploads tab. Expand the row to view details and with this action, you will see a call to the analysis_details API .

See also: behavior_details


Немного общей
информации

Обзор Cyphort и признание в индустрии

Компания

Основана: 2011, Santa Clara, CA (HQ)

Решение: Обнаружение продвинутых угроз, аналитика и нейтрализация

Приобретения: Cyphort была приобретена Juniper Networks в сентябре 2017. Тесная интеграция и встраивание в существующее портфолио

Признание

2017

CYBERSECURITY 500 — WORLD'S HOTTEST SECURITY COMPANIES

ICSA labs CERTIFIED

2016

FORRESTER®

Leader in Forrester Wave™
Automated Malware Analysis Report

SC MAGAZINE AWARDS 2016 WINNER Honored in the U.S.

THE CHANNEL CO. CRN SECURITY 100 2016

2015

Forbes
Hottest Security Startups of 2015

SC MAGAZINE AWARDS 2015 WINNER Honored in the U.S.

2014

RSAC Innovation Sandbox FINALIST

Высокие результаты независимых тестов

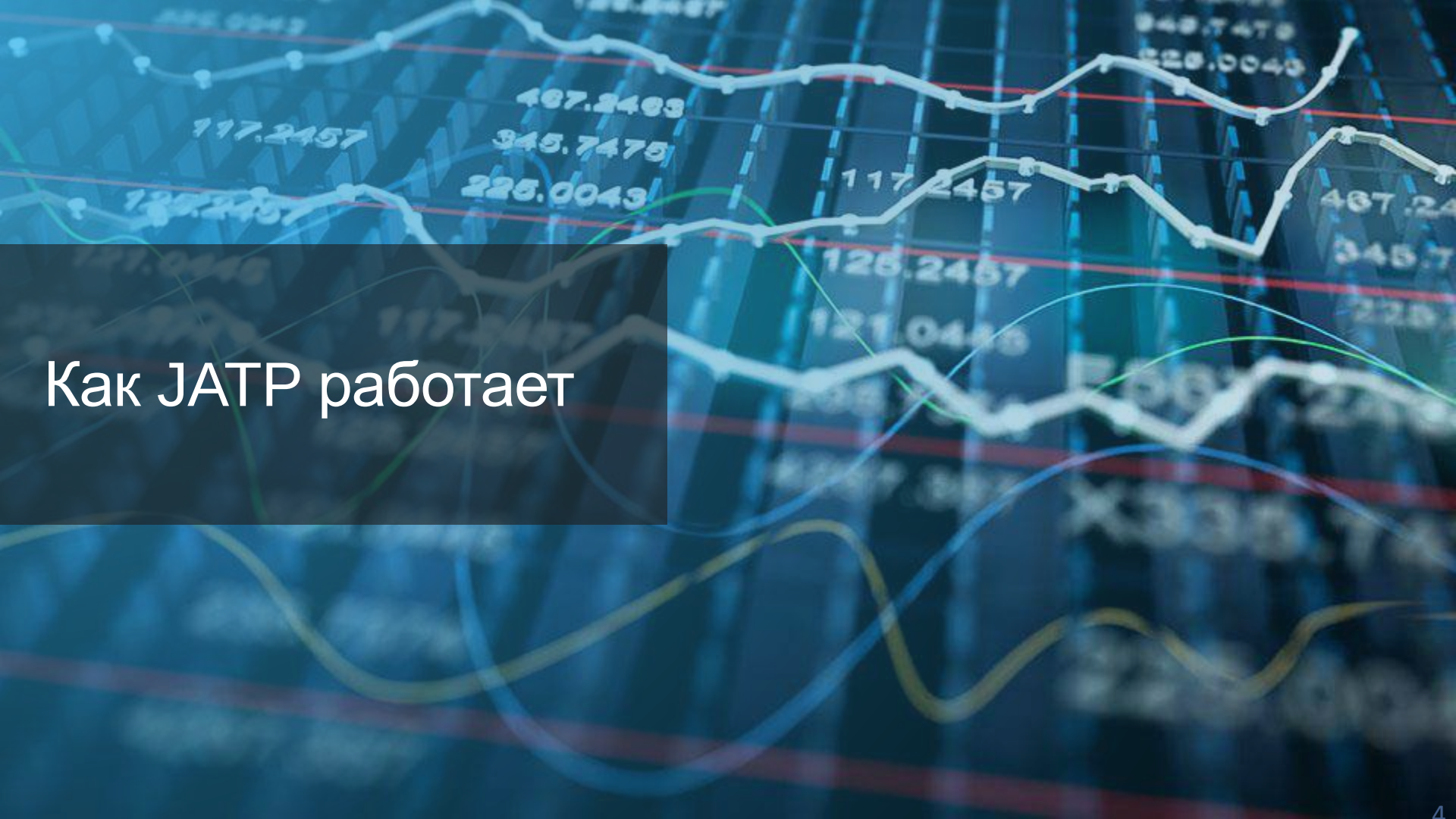
FORRESTER®

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

Высокая эффективность подтверждается независимыми исследованиями ICSA Labs, апрель 2017

Test Length	37 days	**Malicious Samples**	614	**Innocuous Apps**	519
Test Runs	1133	**% Detected**	**100.0%**	**% False Positives**	**1.5%**

Образцы ВПО для тестов ICSA получает с собственных спам- и ханипотов, Интернет и известных вредоносных URL

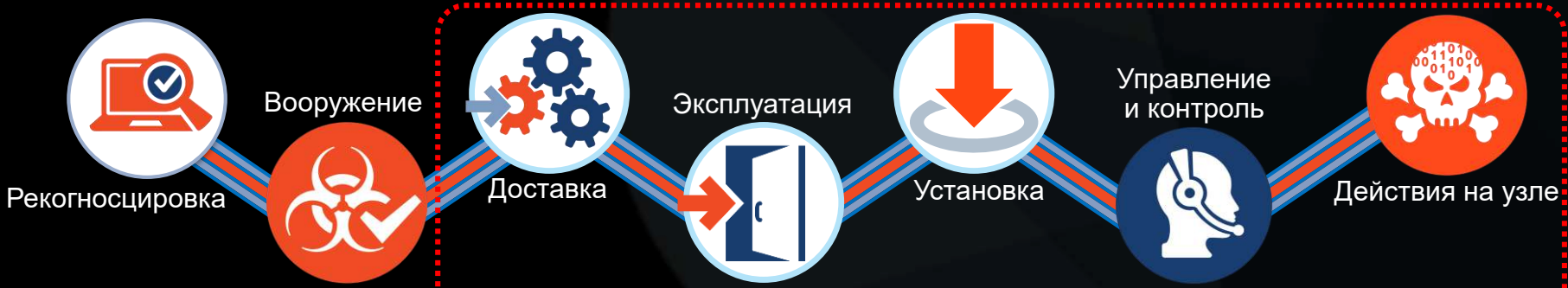


Как JATP работает

Ключевые компоненты JATP

Глубокий анализ JATP значительно эффективнее сигнатурного анализа

Продвижение угрозы по Cyber Kill Chain



Juniper Advanced Threat Prevention Appliance (JATP)

Exploits	XP	Активность, подвергающая пользователей опасности
Downloads	DL	Загрузка вредоносного объекта
User Uploads	UP	Отправка вредоносного объекта с оконечной точки
Executions	EX	Запуск вредоносного кода на оконечной точке
Infections	IN	Получение свидетельств заражения (C&C, IVP)
Lateral Spread	LS	Горизонтальное распространение ВПО внутри сети
Phishing	PHS	Почтовое сообщение с вредоносным URL

Определение значимости угрозы

Значимость, Приоритет, Риск

Обнаружение угрозы

Оценка опасности угрозы

- Adware
- Virus
- Worm
- Ransomware
- Trojan Hijack, Backdoor
- Exploit
- Data Theft
- и т.д.

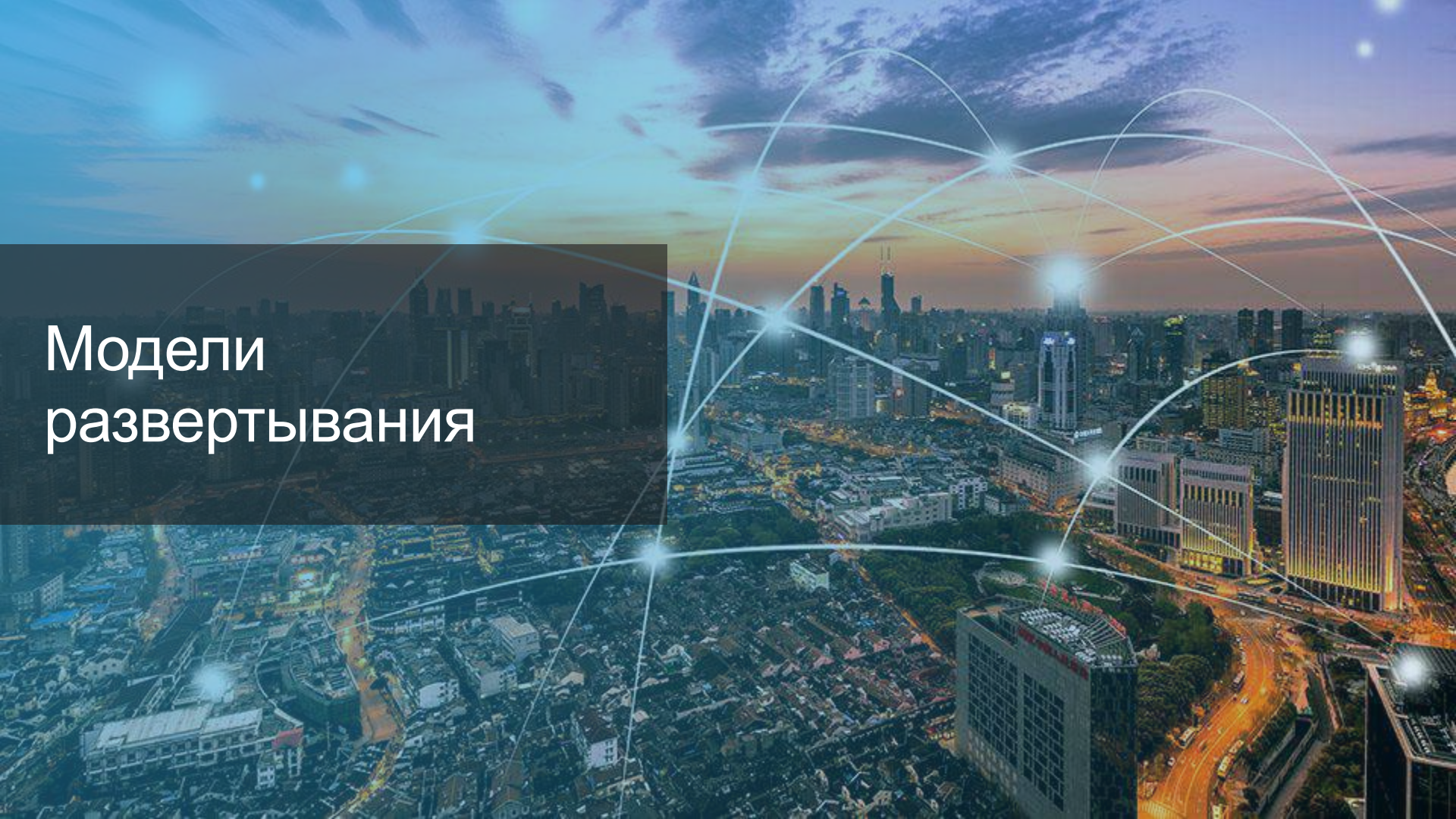
Значимость атакуемого актива

- Низкая
- Средняя
- Высокая
- Критичная

Верификация заражения актива

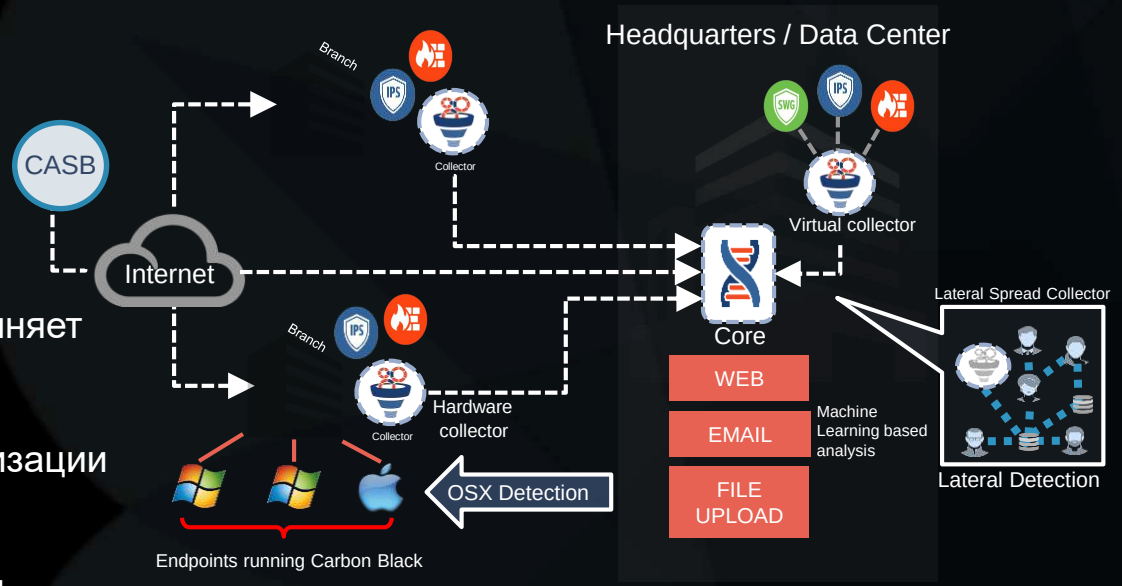
- Насколько далеко по Cyber Kill Chain продвинулось ВПО?
- Выполнился ли код на машине жертвы?
- ОС жертвы совпадает с целевой ОС ВПО?
- Установлен ли Антивирус на машине жертвы?
- Этот Антивирус был способен детектировать угрозу?
- Угроза сработала для собственного образа ОС?
- и т.д.

Модели развертывания



Развертывание

- Центральное Ядро JATP собирает информацию от коллекторов, выполняет детектирование и анализ;
- Компоненты управления и нейтрализации угроз входят в состав Ядра;
- Коллекторы собирают данные о Web и SMB трафике со SPAN/TAP портов сетевых устройств;
- Коллекторы почты собирают данные с почтовых серверов или работают как MTA-получатели;

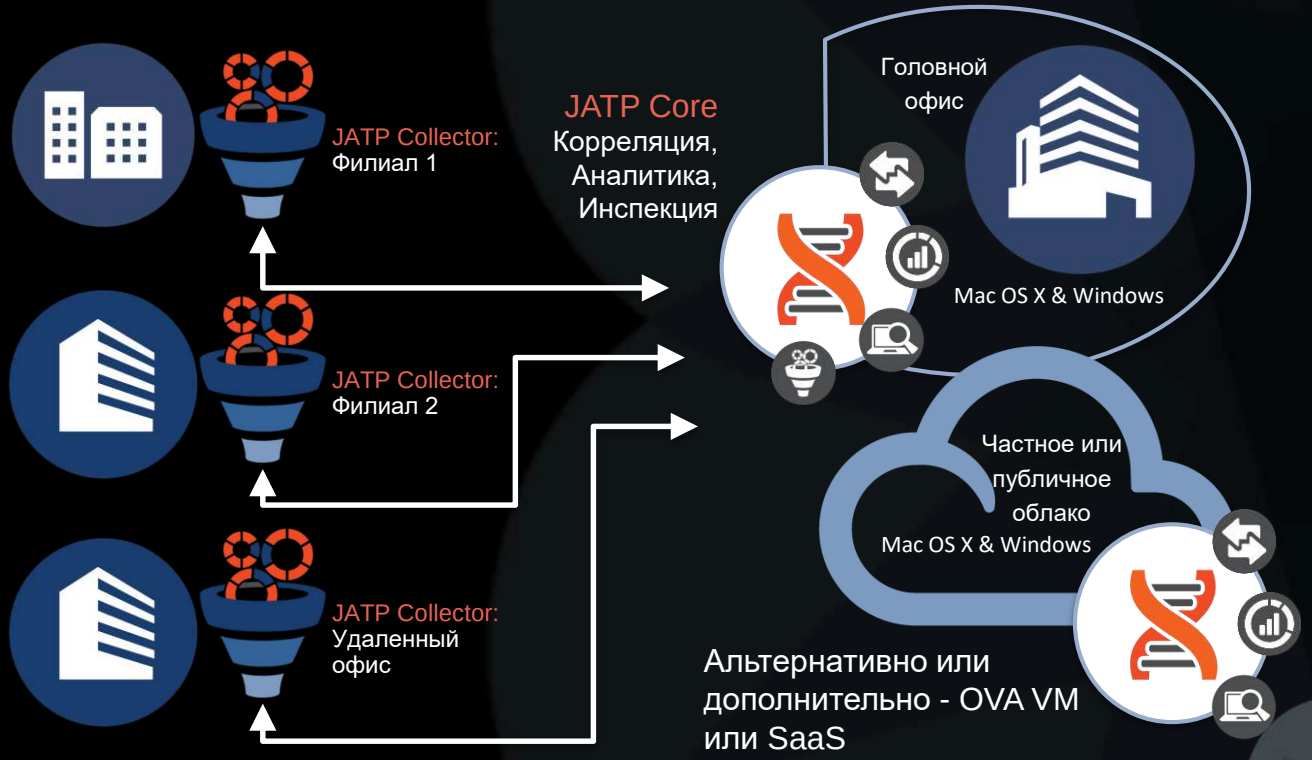


Опции для Ядра и Коллекторов:

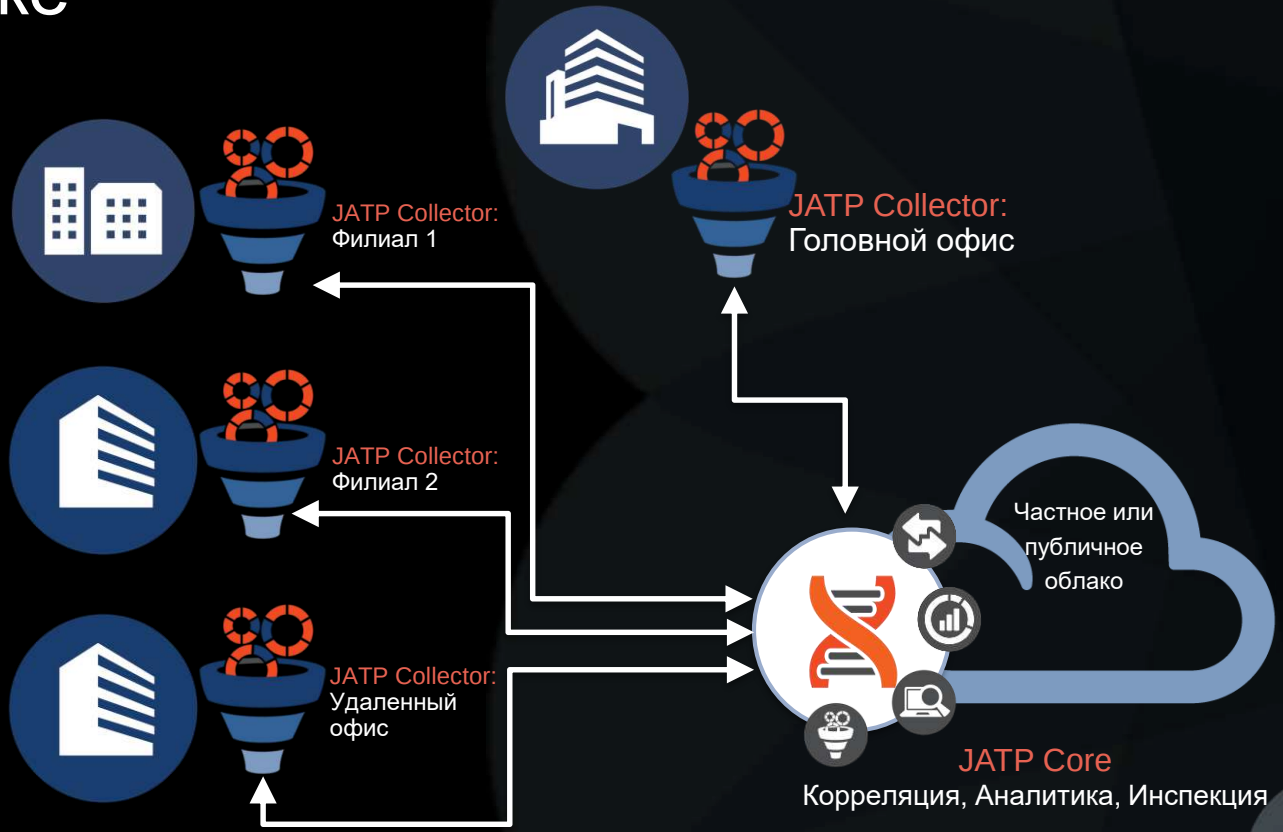
- **программно-аппаратный комплекс (appliance),**
- **виртуальные машины,**
- **ISO для Mac Mini**
- **NGFW SRX и VSRX (Web-коллектор)**

Развертывание в центральном офисе

Развертывание на нескольких площадках

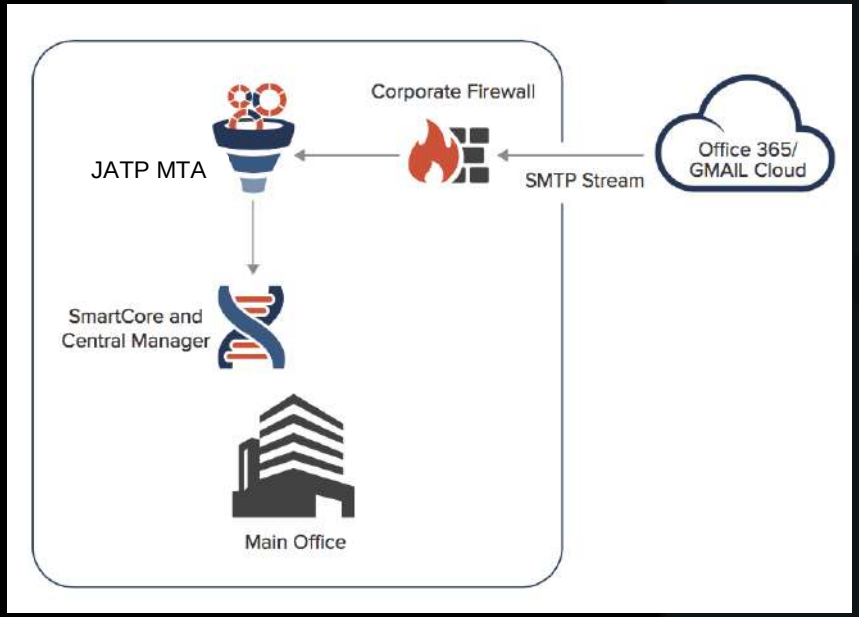


Развертывание в частном или публичном облаке



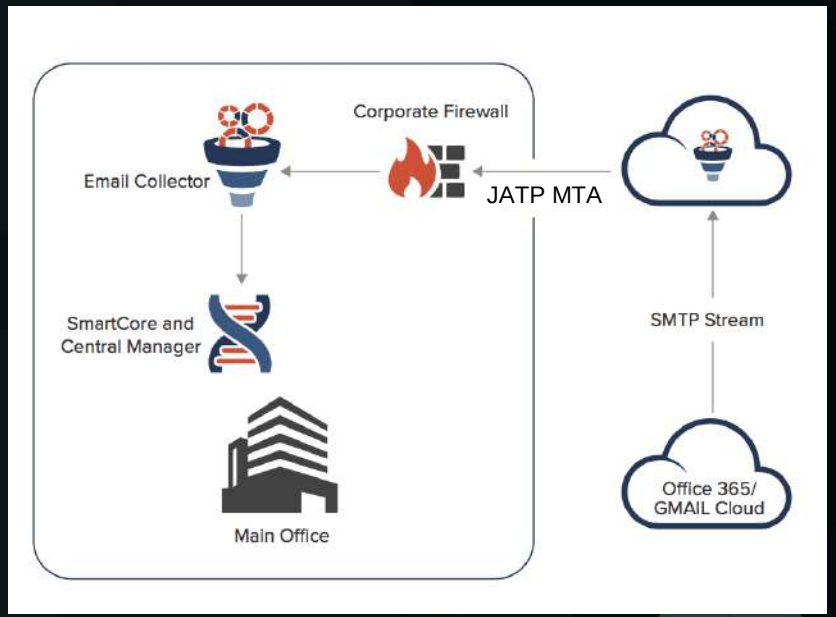
Развертывание – анализ почты

Сбор почты локальным коллектором



JATP MTA развернут локально

Сбор почты коллектором в облаке

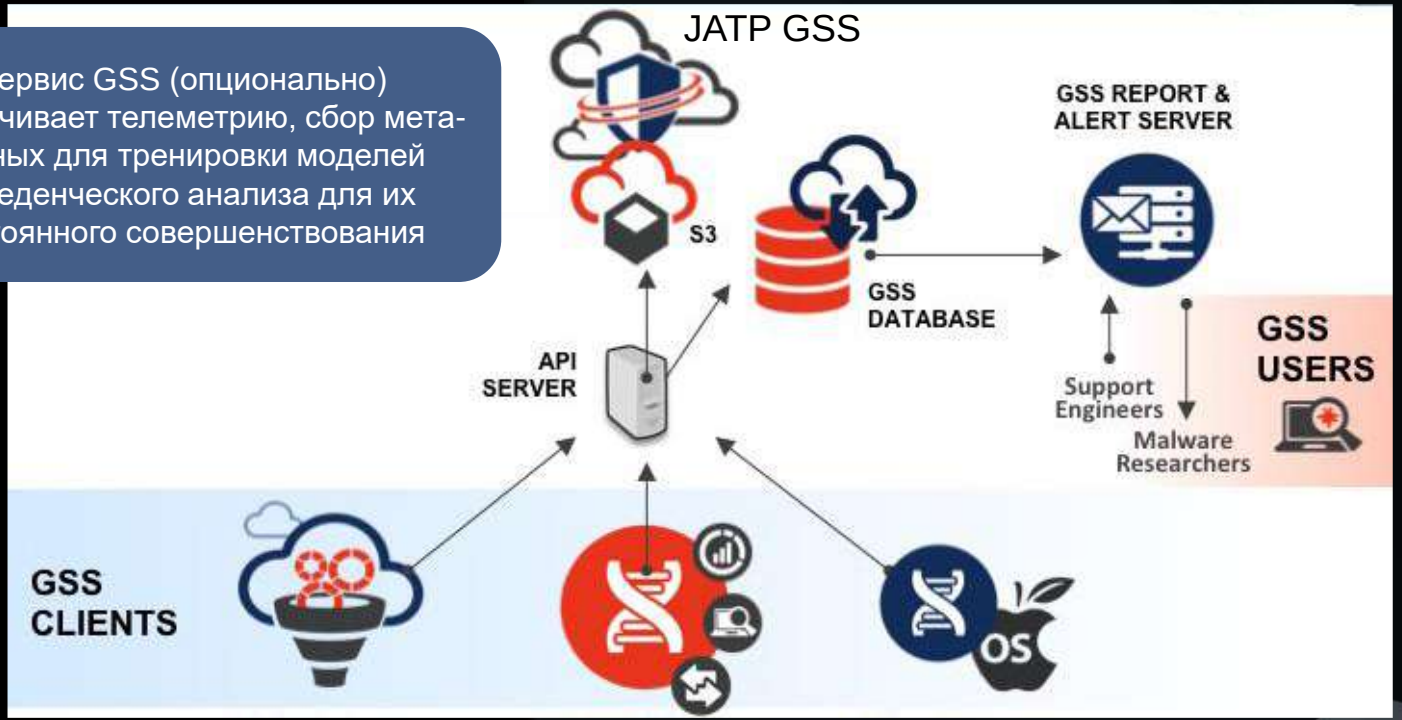


JATP MTA развернут в частном облаке

JATP MTA устанавливается out-of-band, не inline

Global Security Service

Сервис GSS (опционально) обеспечивает телеметрию, сбор мета-данных для тренировки моделей поведенческого анализа для их постоянного совершенствования



Коллектор

Основное ядро

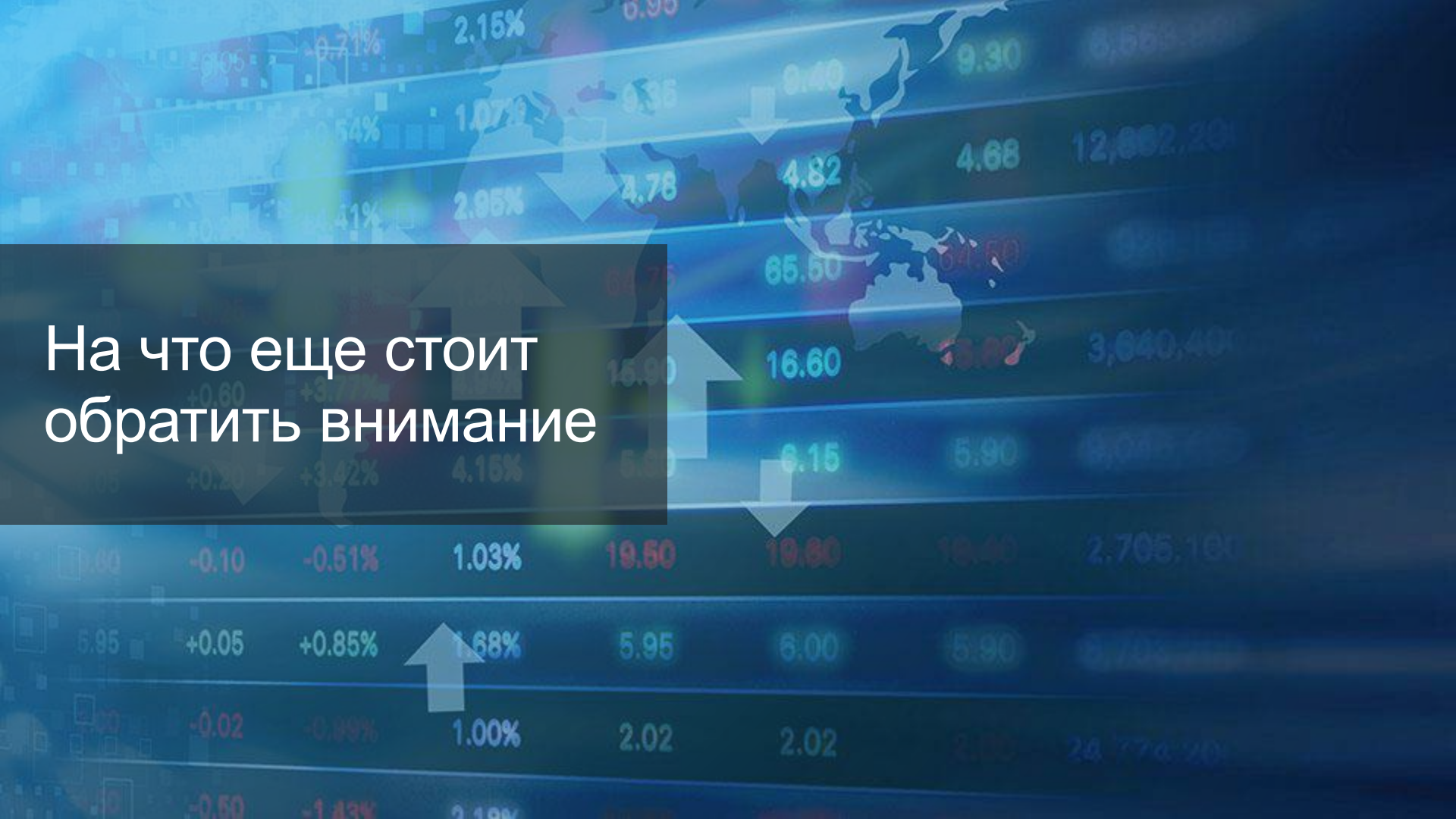
Вторичное ядро

Juniper Threat Network

Однонаправленная и двунаправленная модели взаимодействия (опционально) :

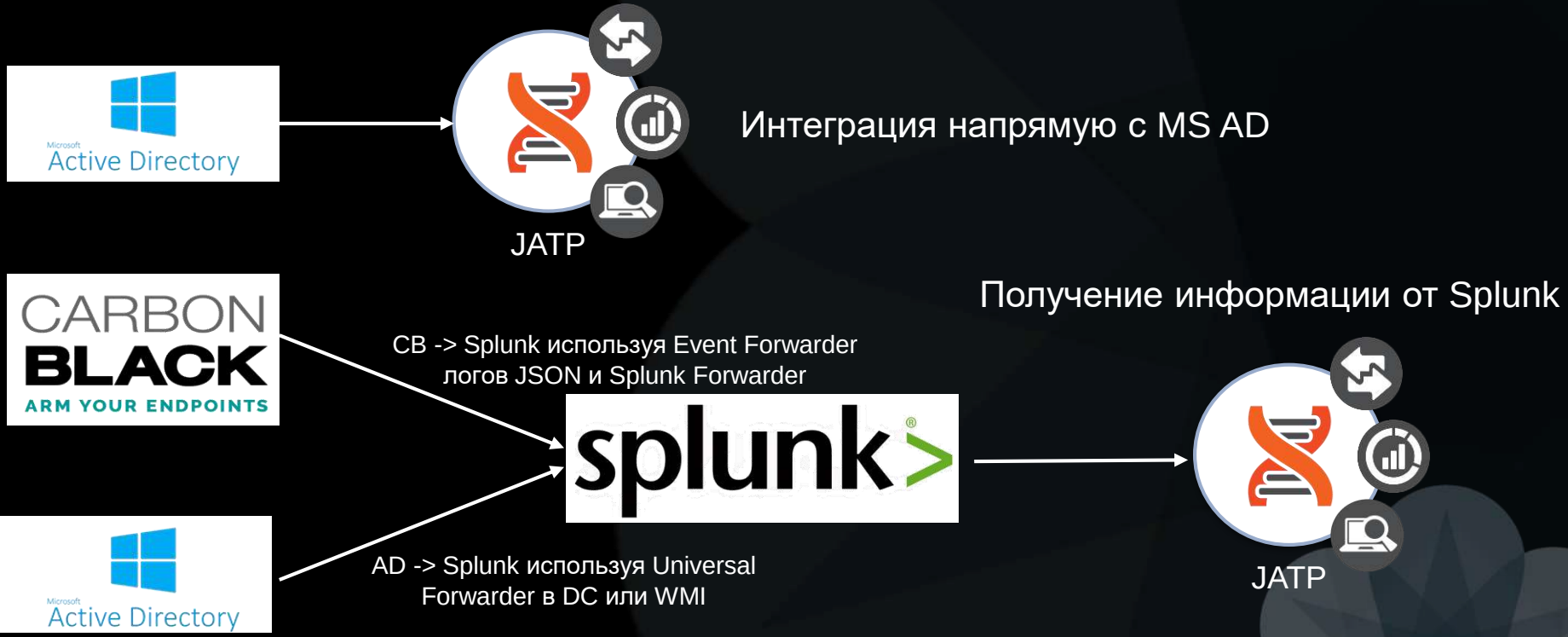
- Пользователь получает обновления, но сам ничего не отправляет;
- Пользователь получает обновления, отправляет мета-данные и телеметрию.

- Обновления моделей машинного обучения
- Обновления данных Threat intelligence
- Обновление модулей репутационного и статического анализа

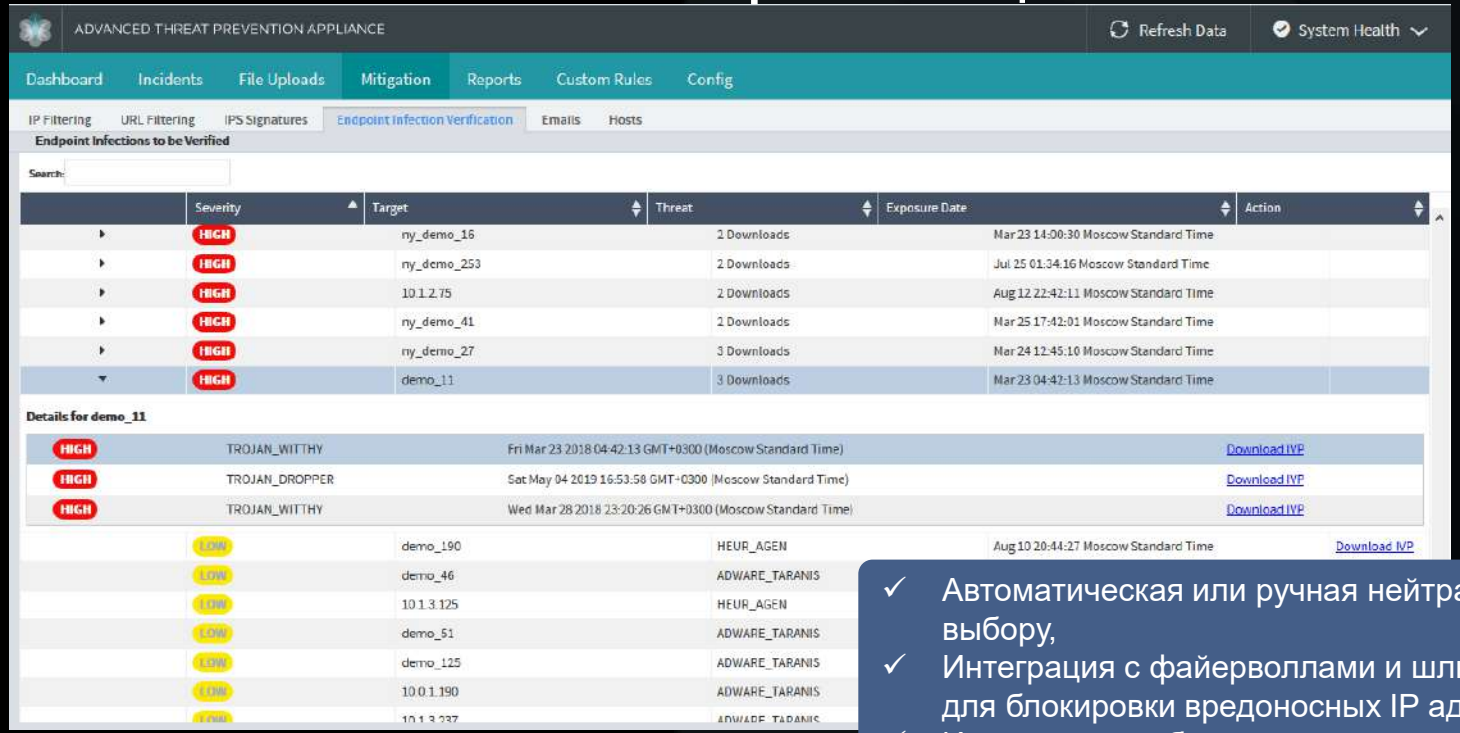

На что еще стоит
обратить внимание

Интеграция с Active Directory

Получение подробных данных о пользователях и машинах

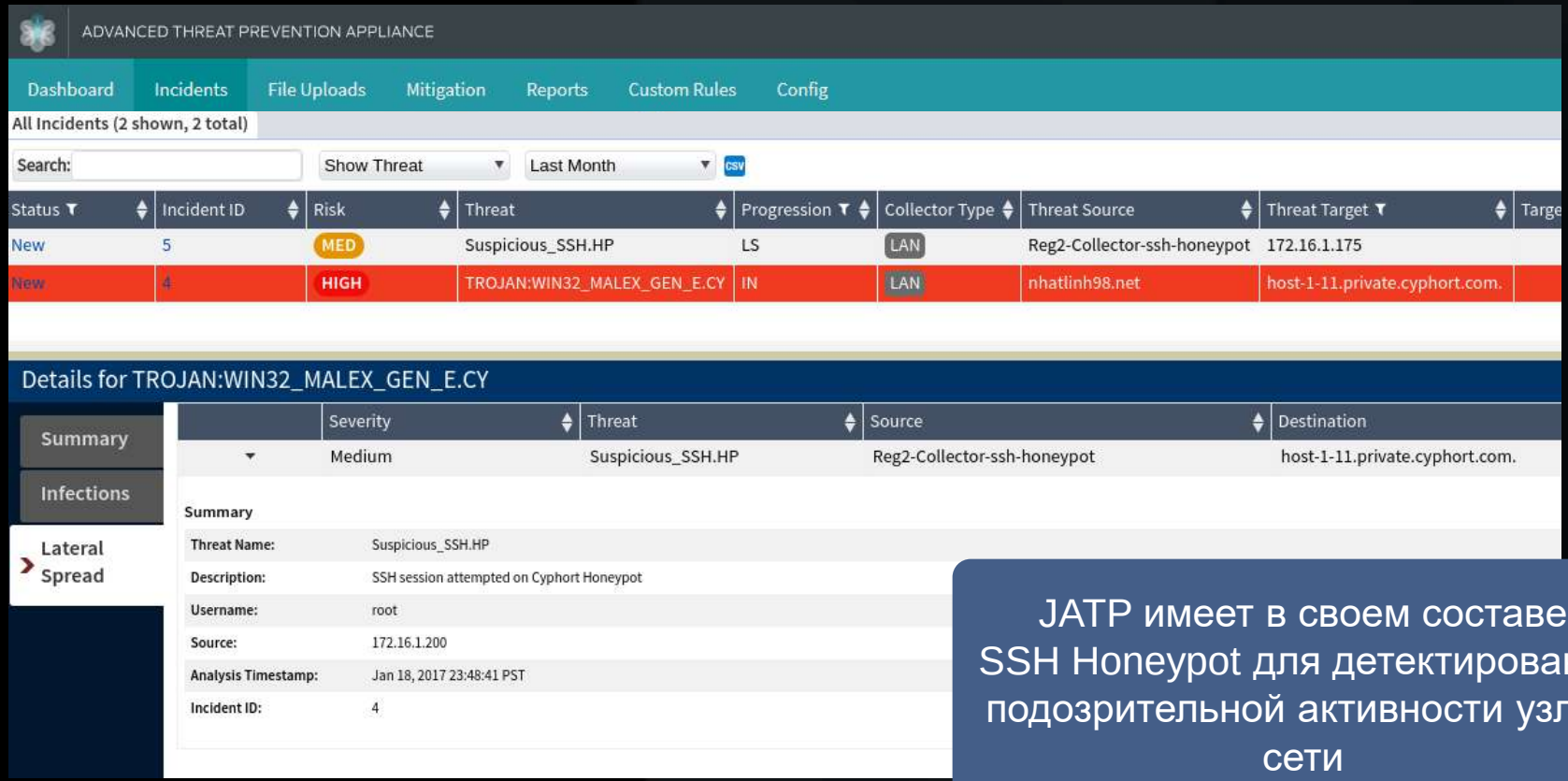


Автоматическая нейтрализация ВПО



- ✓ Автоматическая или ручная нейтрализация по Вашему выбору,
- ✓ Интеграция с файерволлами и шлюзами безопасности для блокировки вредоносных IP адресов и URL,
- ✓ Интеграция с облачными почтовыми сервисами для помещения письма в карантин
- ✓ Компонент Juniper Connected Security для блокировки хостов на уровне сети

SSH Honeypot



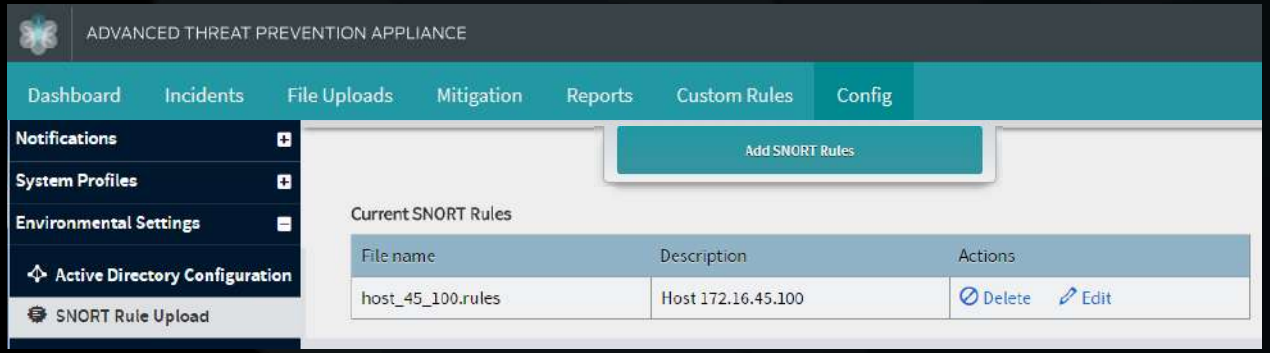
JATP имеет в своем составе SSH Honeypot для детектирования подозрительной активности узлов сети

Анализ горизонтального трафика

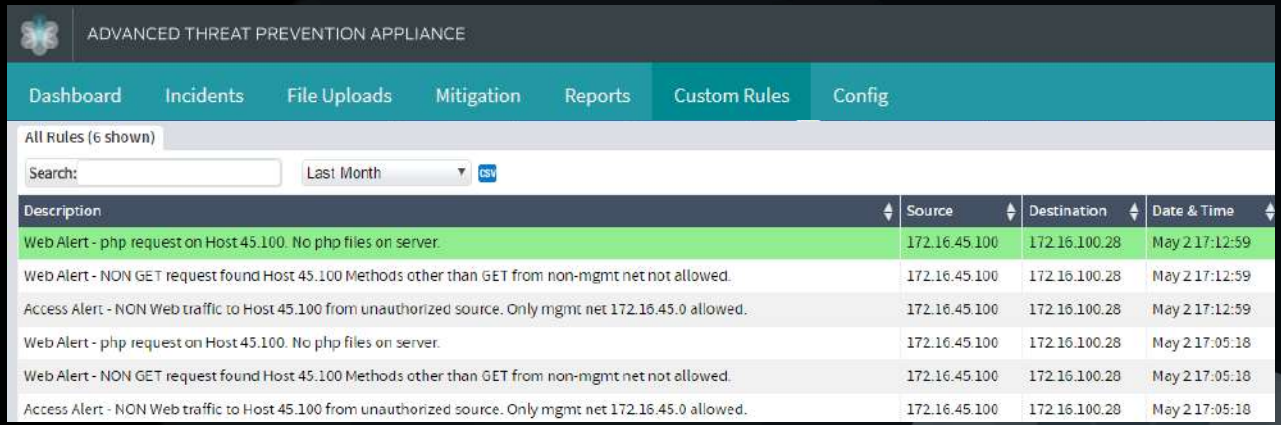
- Обнаруживаются перемещения ВПО внутри сети по протоколу SMB,
- Использование правил YARA детектирует Remote Access Trojans (RAT)

Собственные правила SNORT

- Оператор может создавать и загружать собственные правила SNORT для усиления защиты и детектирования специфичных для сети атак

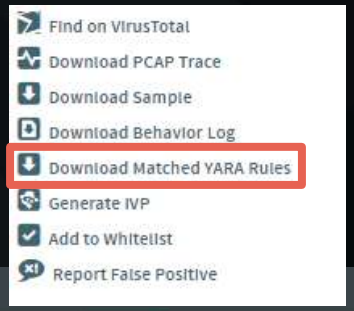


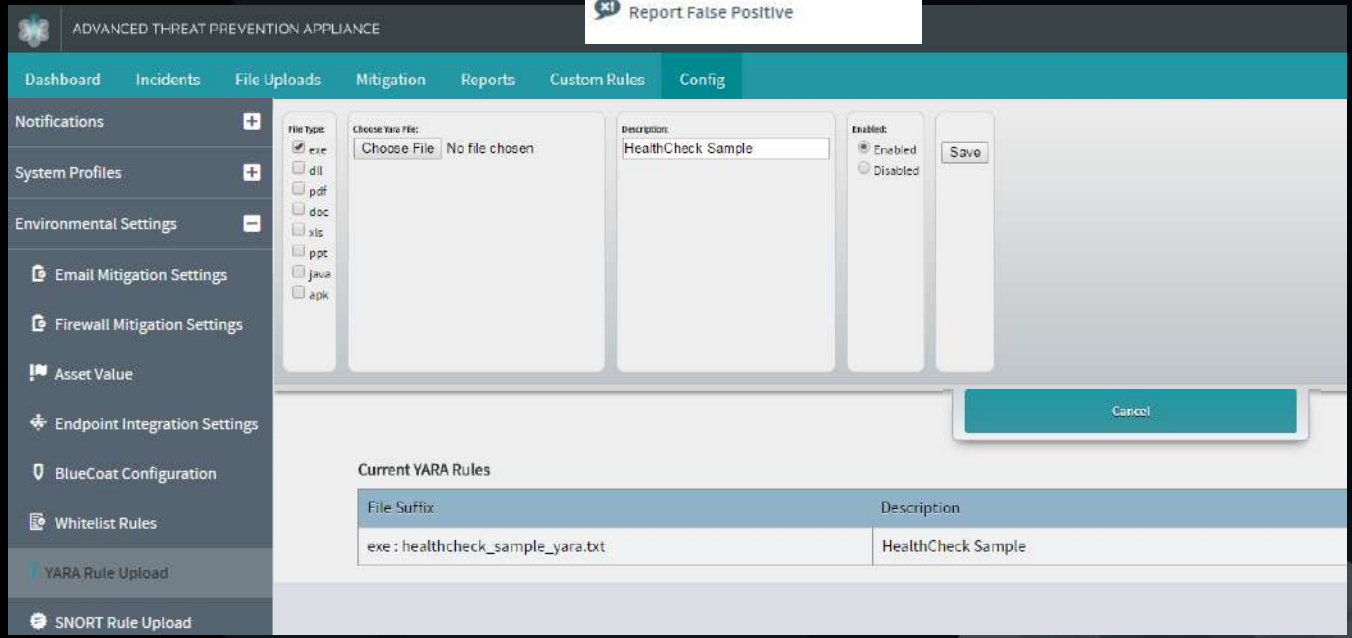
- Подозрительный трафик, обнаруженный собственным правилом будет отображаться в отдельной вкладке для удобства



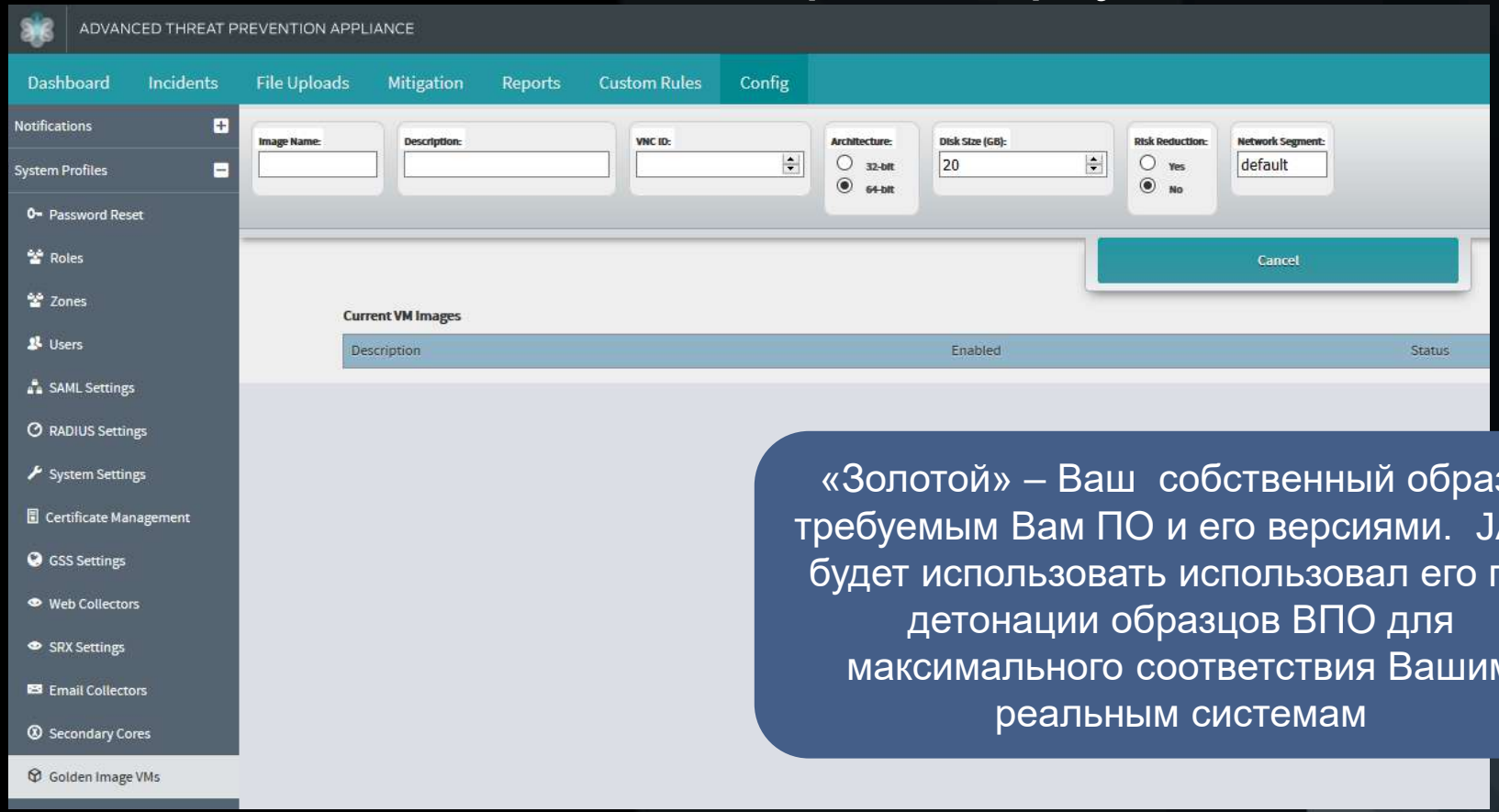
Собственные правила YARA

- Оператор может создавать и загружать собственные правила YARA для усиления защиты и детектирования специфичного ВПО,
- Триггер для таких инцидентов будет отображаться как Static





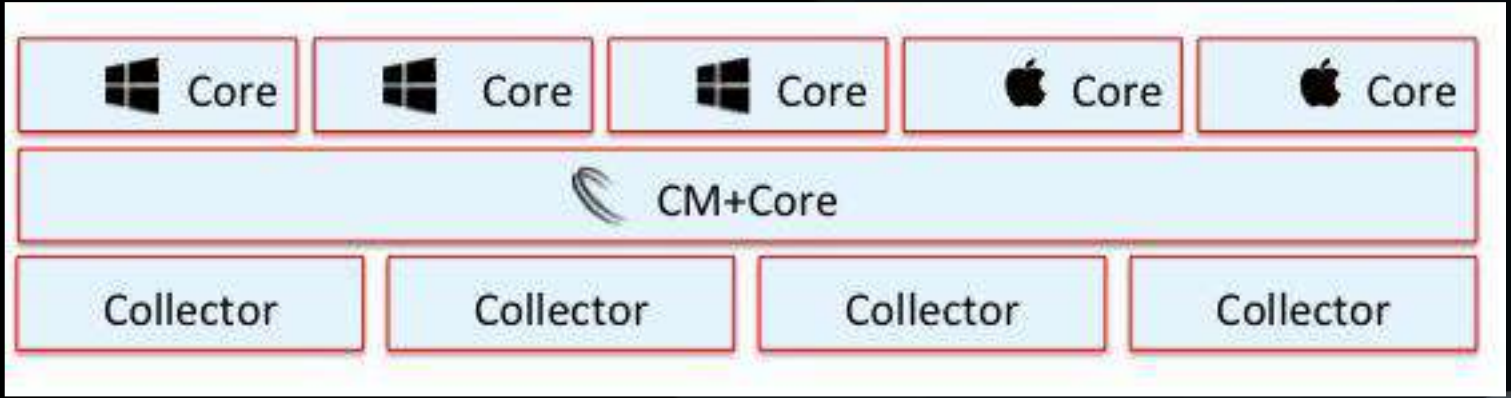
Собственный «Золотой образ» виртуальной машины



«Золотой» – Ваш собственный образ с требуемым Вам ПО и его версиями. JATP будет использовать использовал его при детонации образцов ВПО для максимального соответствия Вашим реальным системам

Работа в кластере

- JATP скажет когда нагрузка стала большой и нужно добавлять новые Core
- Балансировка нагрузки между Core - автоматически



Форм-фактор

Апплайнсы физические и виртуальные

JATP 400	JATP 700	vJATP Core, Mail & Web vCollector
• 10 ядер, • 32G RAM DDR4, • 4 x 2TB HDD (RAID 6) • 8 NICs (2 x 10G SFP+, 2 x 10G, 4x 1GE) • 500Вт AC или 650Вт DC (резервируемые) • 1 RU • Воздушный поток: к задней панели	• 40 ядер, • 128G RAM, • 8 x 900G HDD (RAID10) • 6 NICs (2 x 10G SFP+ и 4 x 1G) • 920Вт AC или 650Вт DC (резервируемые) • 2 RU • Воздушный поток: к задней панели	• 4-24 vCPU, • 16-96G vRAM • 512 GB vHDD • до 4 vNICs

Варианты развертывания

Физические апплайнсы

All in One

Модель	Производительность (объектов в день)	Производительность
JATP700	до 61 000	2.5 Gbps
JATP400	до 25 000	1 Gbps

Smart Core

Модель	Производительность (объектов в день)
JATP700	до 130 000
JATP400	до 50 000

Web Collector

Модель	Производительность
JATP700	4 Gbps
JATP400	1.5 Gbps

eMail MTA-приемник

Модель	Писем в день
JATP700	2 000 000
JATP400	700 000

Виртуальные

Virtual Smart Core Engine

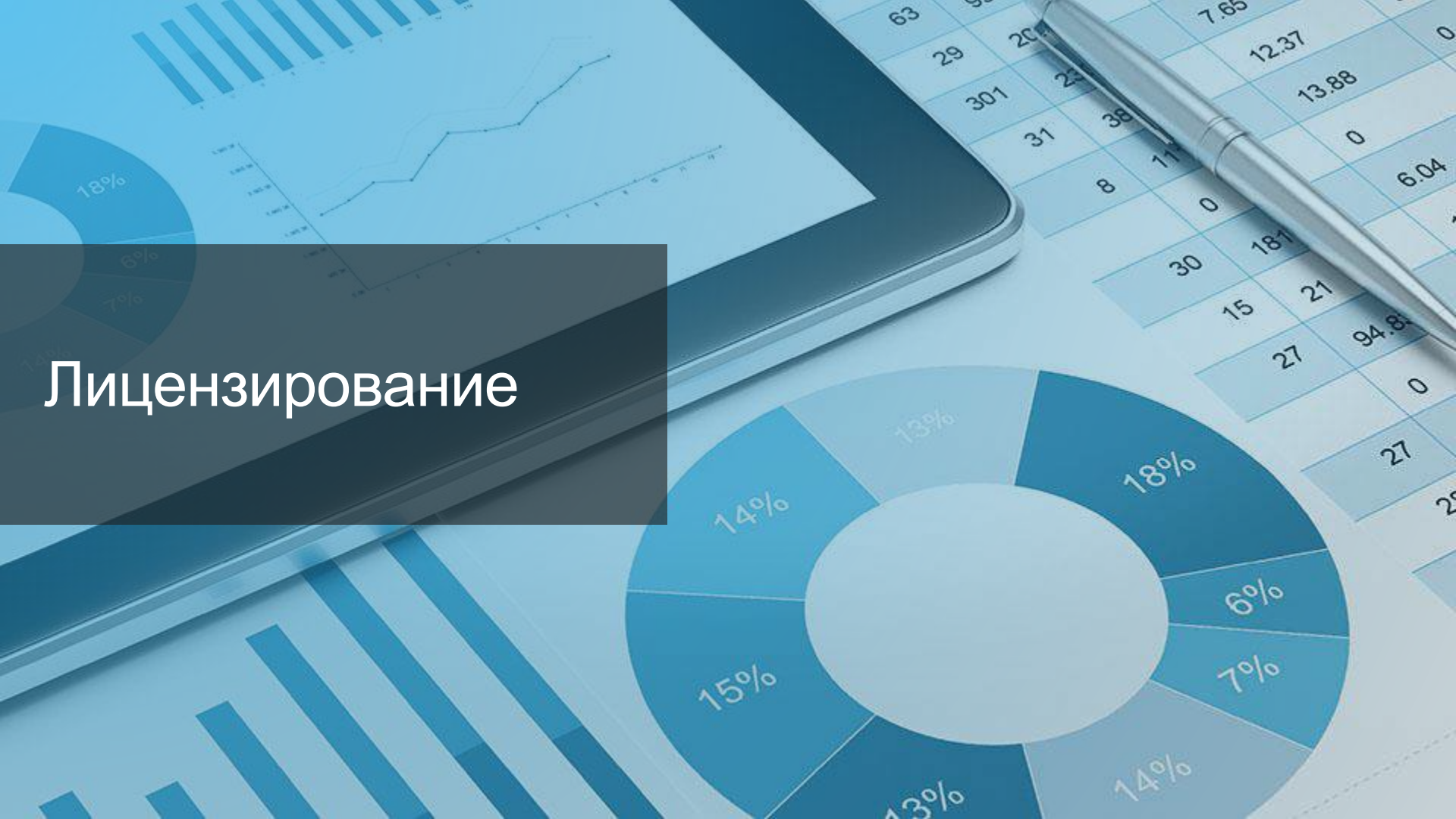
Модель	Производительность (объектов в день)	vCPU	vRAM	vHDD
vSC-8	до 46 000	8	32 GB	1.5 TB
vSC-24	до 116 000	24	96 GB	1.5 TB

Virtual Web Collector

Модель	Производительность	vCPU	vRAM	vHDD
FC-v500M	500 Mbps	4	16 GB	512 GB
FC-v1G	1 Gbps	8	32 GB	512 GB
FC-v2.5G	2.5 Gbps	24	64GB	512 GB

Virtual eMail MTA-приемник

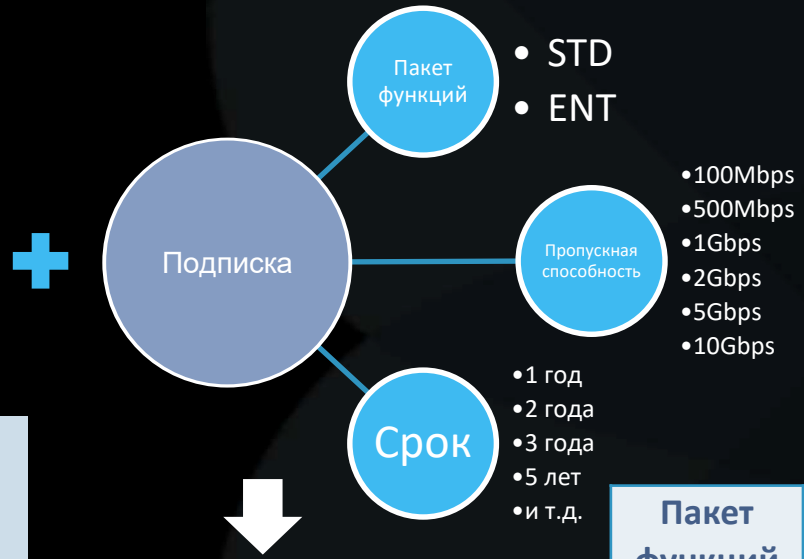
Модель	Писем в день	vCPU	vRAM	vHDD
vMTA-M	720 000	8	16 GB	512 GB
vMTA-L	1 400 000	16	16 GB	512 GB
vMTA-XL	2 400 000	24	24 GB	512 GB


Лицензирование

Тип лицензии в зависимости от набора функций

Апплайнс

✓ Апплайнс (модель, AC/DC)
+
✓ SKU исходя из пропускной способности и срока действия подписки



✓ Для виртуальных апплайнсов все то же самое только без HW SKU

Пакет функций	Включенные функции
Standard (STD)	North-South Web traffic, Auto Mitigation, Analytics, Email (BCC), manual upload
Enterprise (ENT)	All Standard features, Lateral traffic (SMB), Email (MTA)

СПАСИБО!

JUNIPER NETWORKS | Engineering Simplicity

Наш канал на Youtube