

НАЙТИ ИГОЛКУ В СТОГЕ СЕНА. JUNIPER ADVANCED THREAT PREVENTION

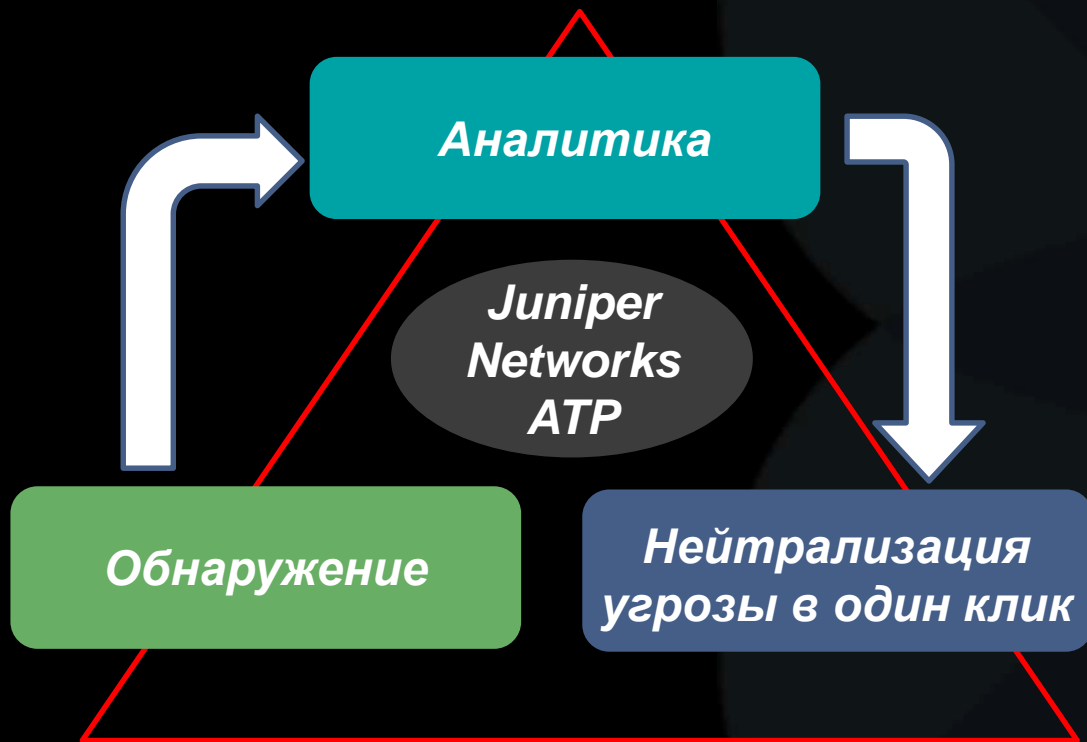
Павел Живов

системный инженер, pzhivov@juniper.net

JUNIPER
NETWORKS

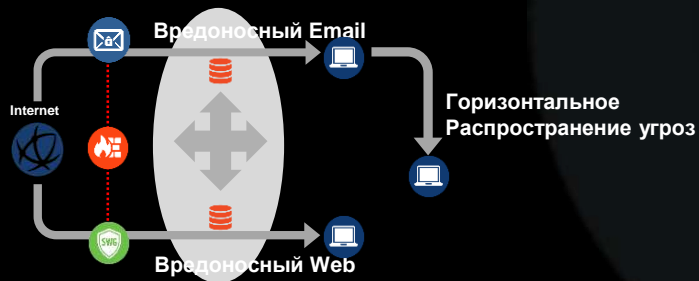
| Summit

3 ключевых функции решения Juniper ATP



- **Обнаружение** – Использование алгоритмов машинного обучения и поведенческого анализа непрерывно собирают данные и обнаруживают угрозы в почтовом-, веб- и горизонтальном трафике
- **Аналитика** – модуль аналитики коррелирует 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

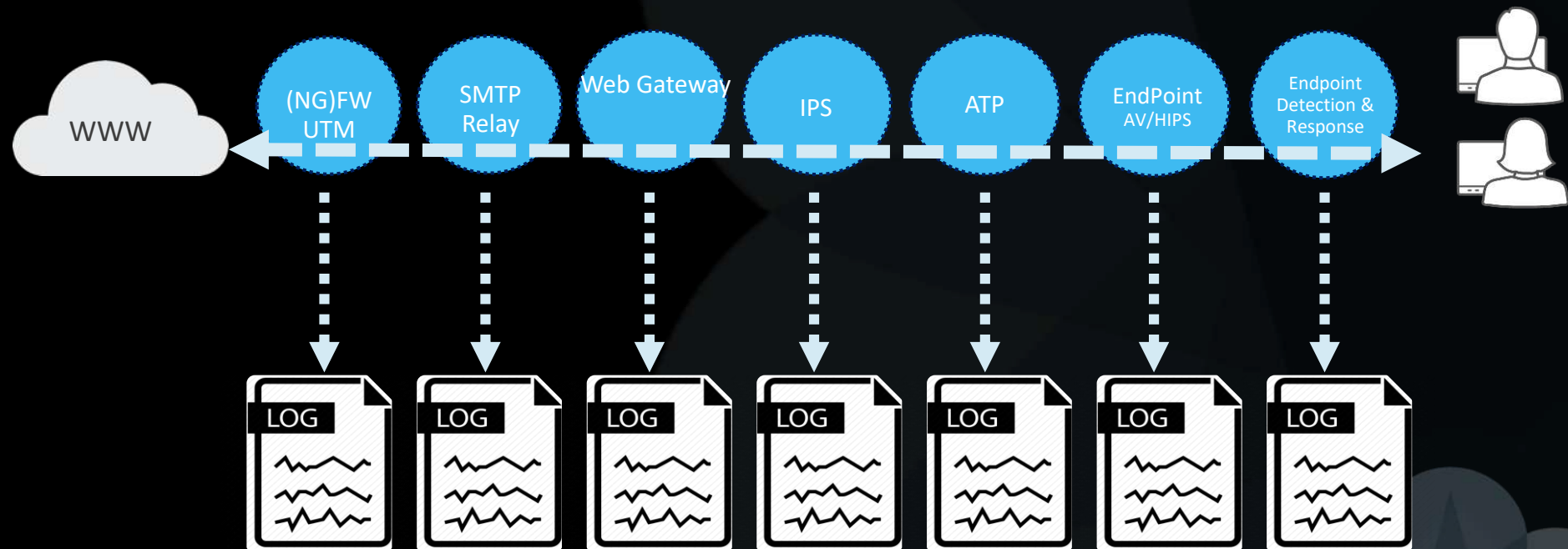
- 96% предупреждений в SOC игнорируется
- 69% требуется больше персонала для обработки задача IR
- 71% требуется больше автоматизации для решения задач IR

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

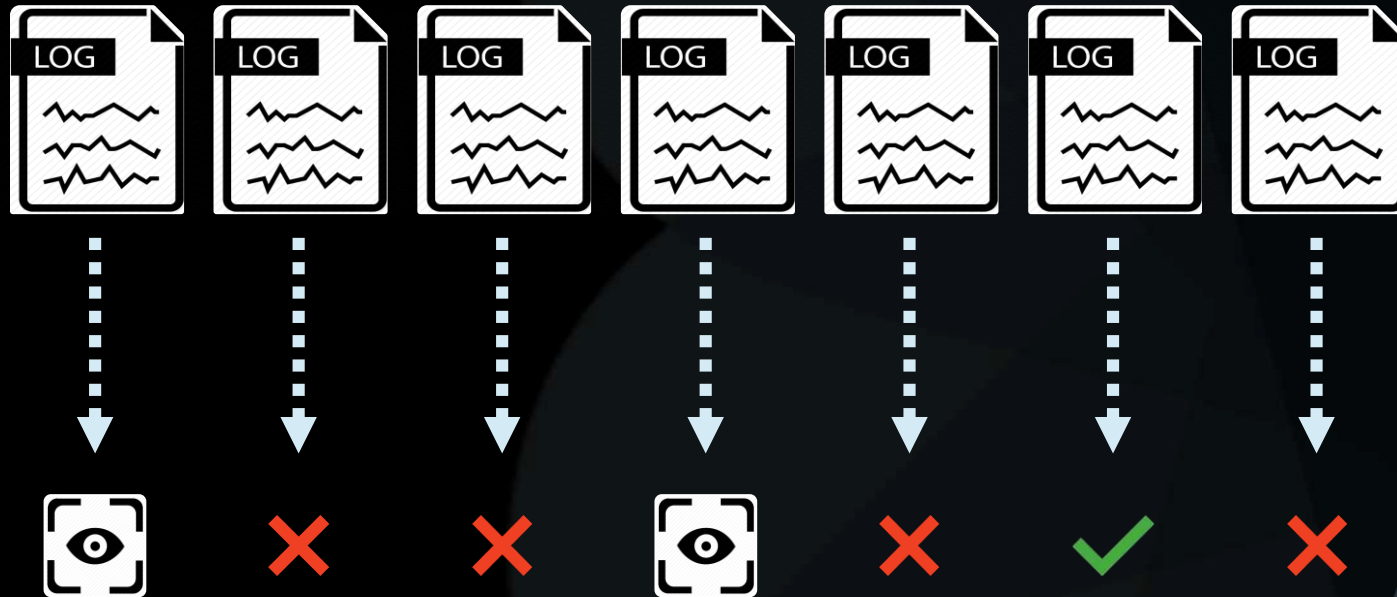


Реакция на инциденты и расследование

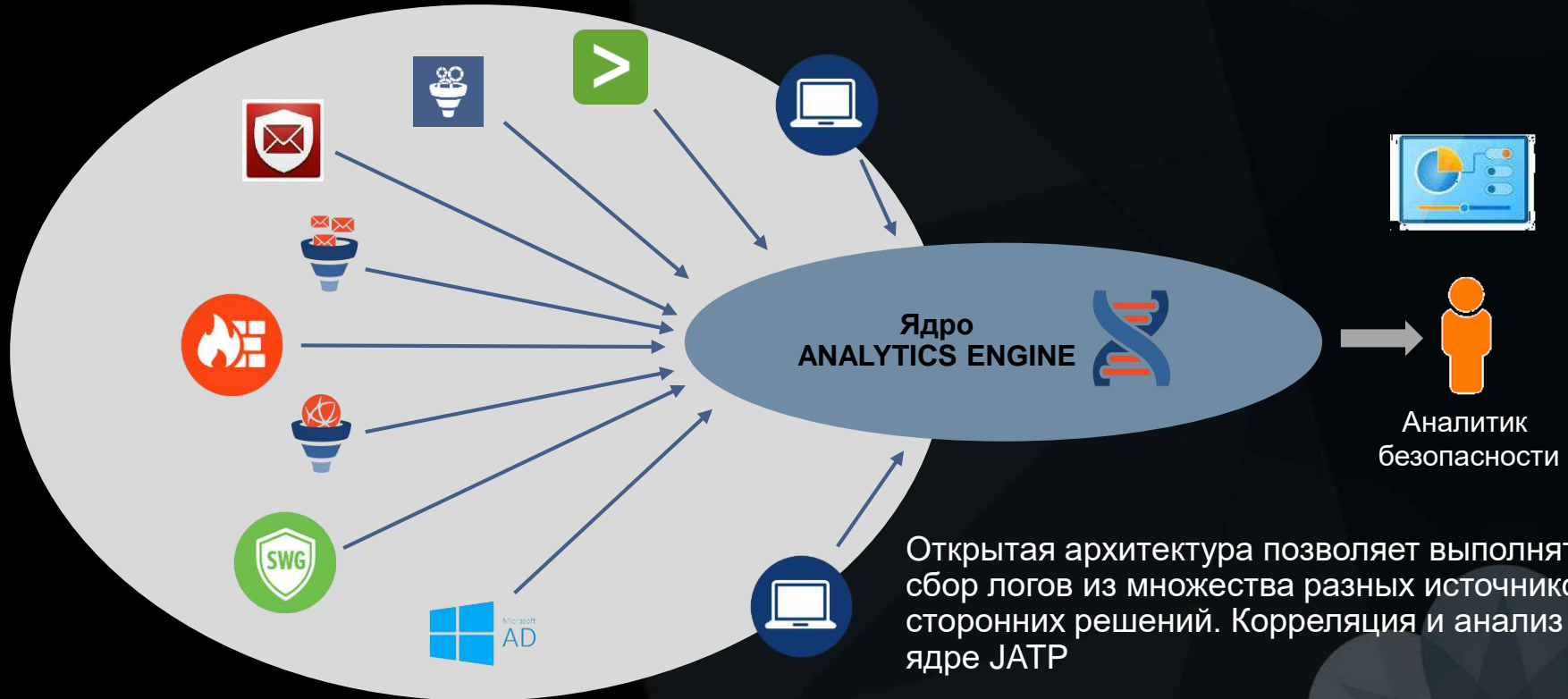
Модель безопасности с несколькими уровнями контроля



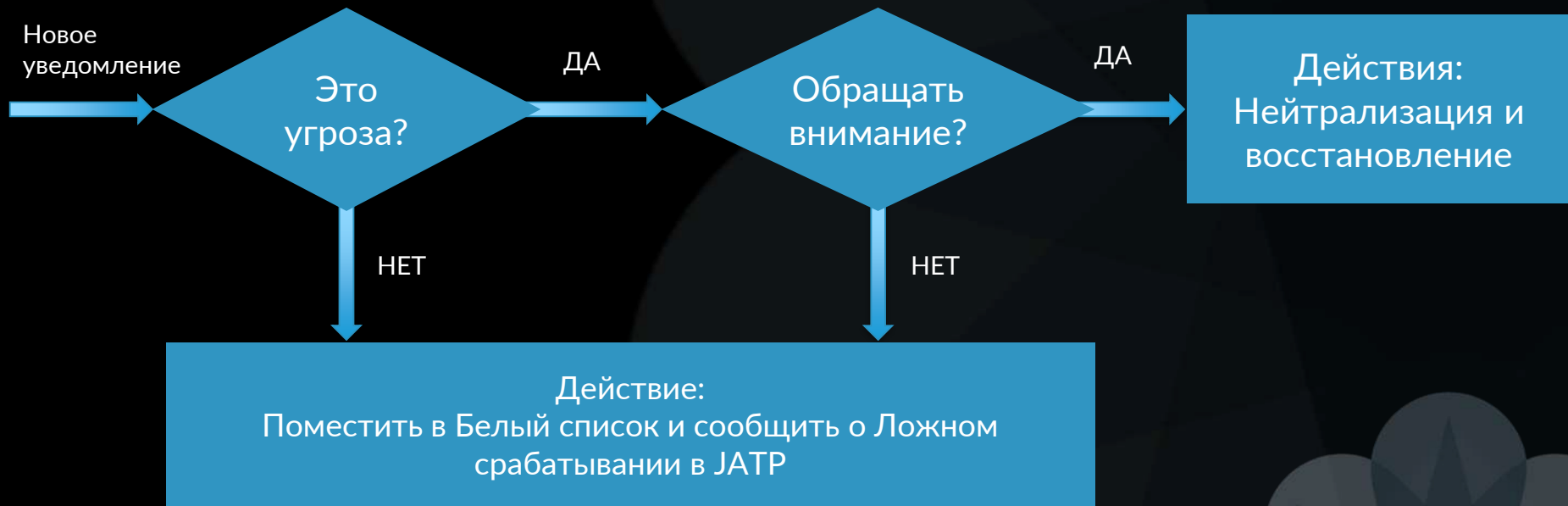
Модель безопасности с несколькими уровнями контроля



Продвинутая аналитика: консолидация и корреляция событий

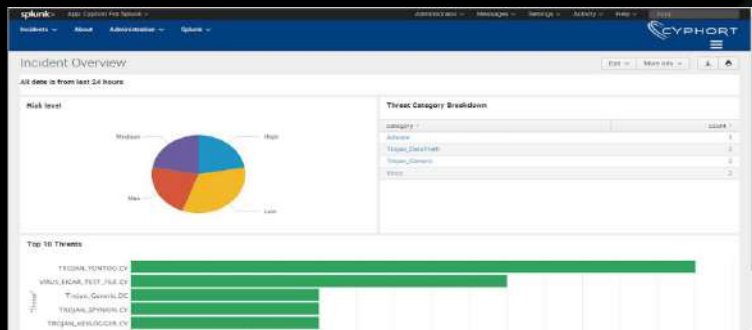


Упрощенный алгоритм IR



1. Идентификация

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



Severity: **High**

Threat: [TROJAN_BOXER.CY](#)

Threat Hash: 021182305c88973380f63160ab629ab

Threat Type: Download (Zip archive data, at least v1.0 to extract ((.JAR) Java Archive))

Time: Tue, 16 Feb 2016 11:44:37 -0800

URL Link: https://10.2.20.61/rvadmin/index.html?incident_id=112495

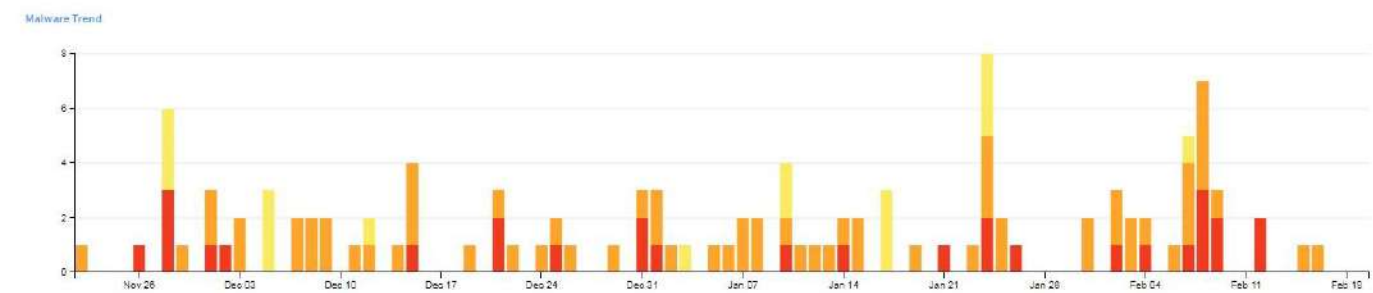
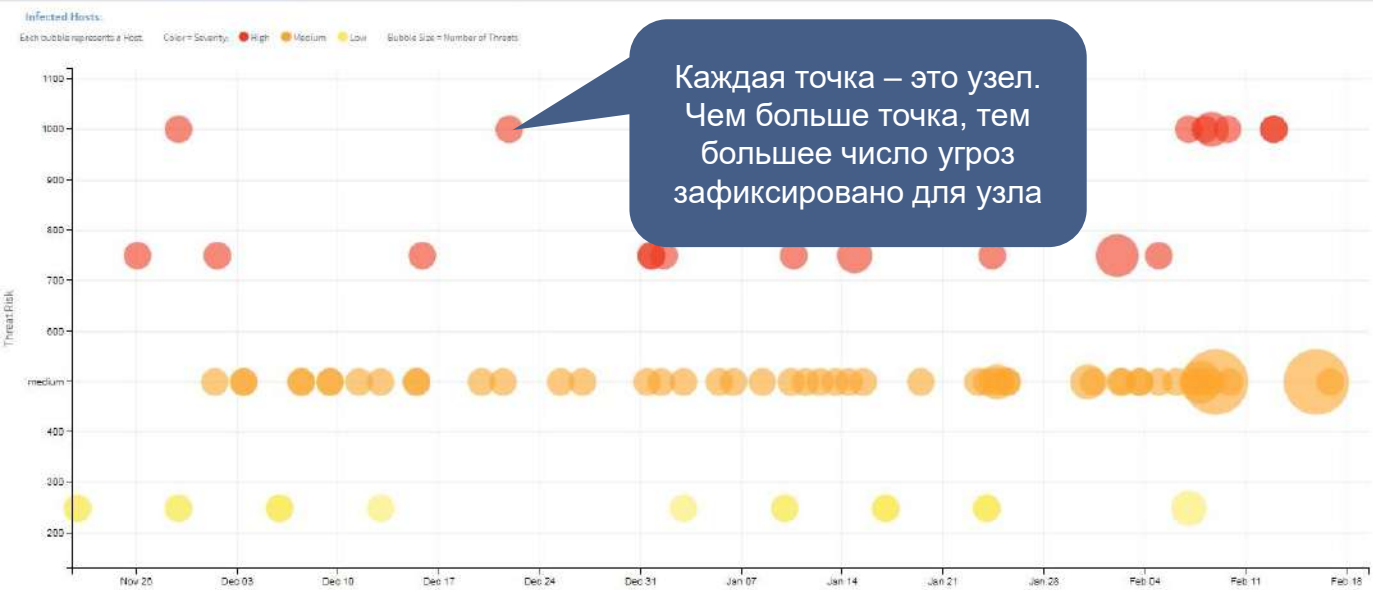
Threat Source: 74.190.126.37([infospace.com](#))

Threat Target: 172.61.53.78(172.61.53.78)

Collector: 10.2.20.61

Cyphort Version: 3.3.1.29

[view alert](#)



Host Details

Target Actions

Hostname: - Username: -
IP Address: 10.1.2.16 FQDN: 10.1.2.16
Source Email ID: - Destination Email ID: -

Asset Value: Medium Anti-Virus: Not Conf
Time: Jan 24, 2018 09:51:21 RTZ 2 OS: igard Windows x7

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

Top Compromised Endpoints

Status	Risk	Host	Threat
New	Max	JOSH-DESKTOP	Trojan_Waldeh
Acknowledged	Max	192.168.50.18	Trojan_Malref
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_Fincov
New	High	ny_demo_11	Trojan_Gloperc
New	High	10.1.2.10	Trojan_Gloperc

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.pfvevqqj.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	phdkegkt.oktrr.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	dntpr.eombqoe.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	ppeupmfoh.qxpold.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	yulvlyssaqujuqvm.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

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




2. Расследование

Details for TROJAN_ASKTOOLBAR.CY

Summary

Actions

Target:

Zone:	Customer-1
Hostname:	-
Username:	-
IP Address:	10.1.2.187
FQDN:	10.1.2.187
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

Exploits

Downloads

Infections

Lateral Spread

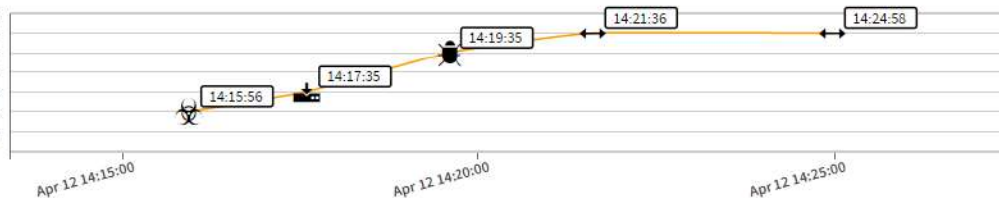
Progression:



Triggers:



Custom Rules
Lateral Spread
Infection
Execution
Downloads
Exploit
Phishing

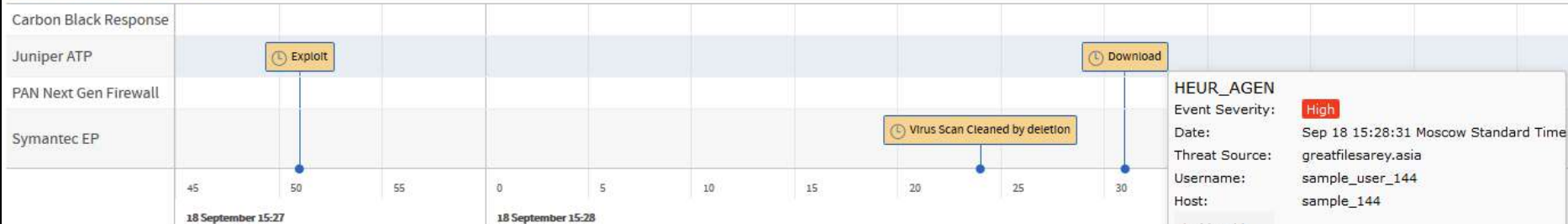


Golden Images: Not Configured



Select Vendor(s) Hostname sample_144

Timeline for Hostname : sample_144



HEUR_AGEN
 Event Severity: High
 Date: Sep 18 15:28:31 Moscow Standard Time
 Threat Source: greatfilesarey.asia
 Username: sample_user_144
 Host: sample_144
 Incident Id : 3125
 Event Id : 5523

Details for HEUR_AGEN

SUMMARY EXPLOITS DOWNLOADS EXTERNAL SOURCES

Actions

Target:

Zone:	Default Zone	Risk:	High
Incident Id:	3125	Threat Category:	Trojan_Generic
Hostname:	sample_144	Asset Value:	Max
Username:	sample_user_144	Target OS:	Windows 7
IP Address:	10.1.1.144	Relevance:	Max
FQDN:	10.1.1.144	Progression:	Exploit + Download
Source Email ID:	--	Protocol:	LOG,HTTP
Destination Email ID:	--	OS Matched:	No
		Summary:	High Risk Threat: downloaded HEUR_AGEN
		Collectors:	Core External Event Collector,web collector JCL
		Source:	greatfilesarey.asia (172.16.0.1)

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  Symantec. **BLUE COAT**

• 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)

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

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

Notifications System Profiles Environmental Settings Email Mitigation Settings Firewall Mitigation Settings Asset Value Anti-Virus Configuration Endpoint Integration Settings BlueCoat Configuration Whitelist Rules YARA Rule Upload SNORT Rule Upload Identity Configuration Splunk Configuration External Event Collectors Custom External Collectors

Source Type:
 Firewall
 Web Gateway
 Endpoint AV
 Endpoint Response

Vendor Name:
 pan-new
 PAN Next Gen Firewall

Transport:
 Log Collector
Log Source Identifier: PA-TEST
SSL:
 Enabled
 Disabled

Default Severity:
 Max
 High
 Med
 Low
 Benign

Create Incident:
 Enabled
 Disabled

Save

Cancel

Current Third Party Sources

Category	Vendor	Transport	Details	Actions
Firewall	pan-new	Log Collector	Log Source Identifier: PA-TEST	Delete Edit Counters Delete Events
Endpoint AV	ESET	Log Collector	Log Source Identifier: ESETAVENT01.AD.SANNET.GOV	Delete Edit Counters Delete Events
Endpoint AV	Symantec EP	Log Collector	Log Source Identifier: ATA-SYMANTEC-MANAGER	Delete Edit Counters Delete Events
Firewall	PAN Next Gen Firewall	Log Collector	Log Source Identifier: PA-200	Delete Edit Counters Delete Events

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

А если нужно понимать еще какие-то логи?

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

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

Notifications
System Profiles
Environmental Settings
Email Mitigation Settings
Firewall Mitigation Settings
Asset Value
Anti-Virus Configuration
Endpoint Integration Settings
BlueCoat Configuration
Whitelist Rules
YARA Rule Upload
SNORT Rule Upload
Identity Configuration
Splunk Configuration
External Event Collectors
Custom External Collectors

Edit Custom Event Source: CB-custom

Create New Source Parse Log File Field Mapping Date Format Log Filtering Severity Assignments

Create New Source

Name* CB-custom

Description

Type*

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

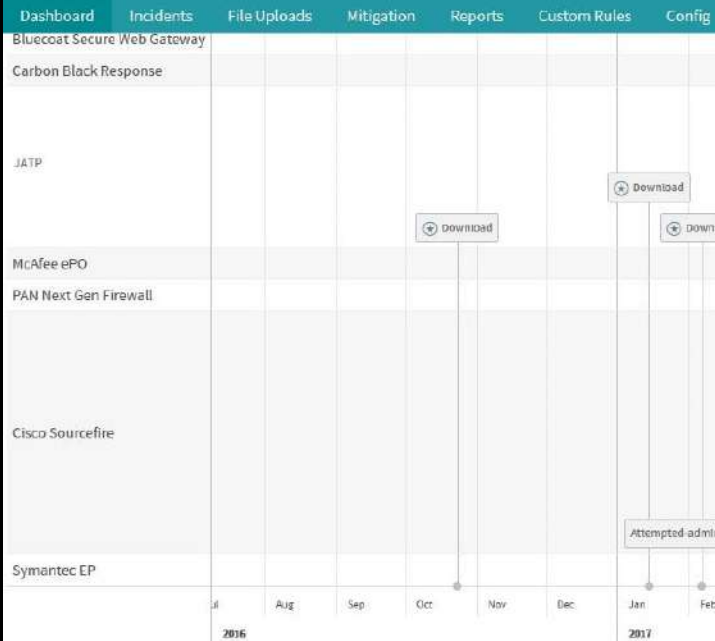
Cancel Next

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

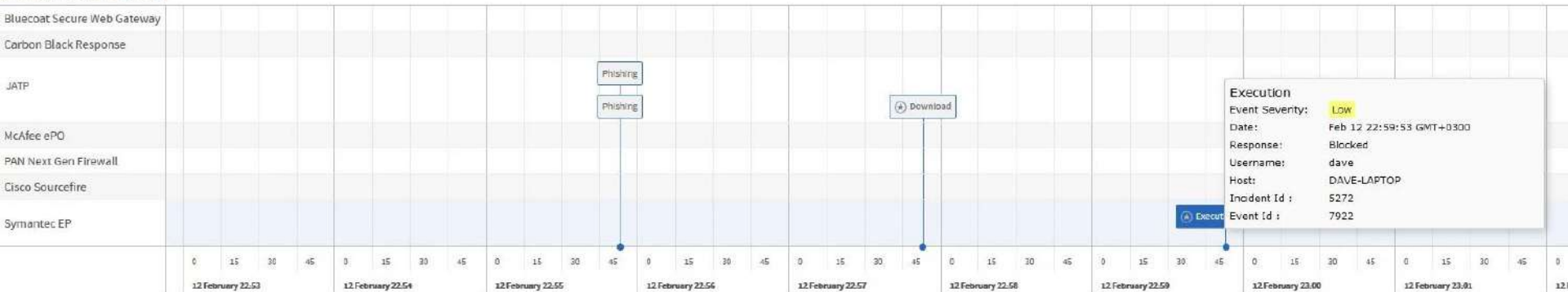
Search:

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=899189 sensor=10.0.0.1 http://10.0.0.1 event_id=11836 msg='EXPLOIT dclient subnet mask option buffer overflow attempt' sid=15700 gid=3 rev=2 class_desc='Attempted Adminis trator 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_bits=7 impact=2 blocked=No impls_label=0 vlan_id=0 kds_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=slp1 iface_egress=slp2 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

Timeline for Endpoint IP: 10.1.1.190



Execution
 Event Severity: **Low**
 Date: Feb 12 22:59:53 GMT+0300
 Response: Blocked
 Username: dave
 Host: DAVE-LAPTOP
 Incident Id : 5272
 Event Id : 7922

Details for TROJAN_LMN.DC
 SUMMARY PHISHING DOWNLOADS EXTERNAL SOURCES

Vendor	Product	Host	Action	Response
Symantec EP		10.1.1.190	Execution	Blocked

Response: Blocked
 Event Action: Execution
 Severity: Low
 Vendor Product: Symantec EP
 Category: Trojan
 File Name: WL-fab8fb28b5d7d04ce51dc9b995d5e21-0
 File Hash: 256ea793b46e9ac3e6e36c459256876c
 Device Host: 10.1.1.190
 Signature: Trojan.Gen
 Raw Log: 2017-03-13 11:56:53-07;VirusFound;IP Address: 10.1.1.190, Computer name: DAVE-LAPTOP, Source: Real Time Scan, Risk name: Trojan.Gen, Occurrences: 1, /Users/dave/Downloads/WL-fab8fb28b5d7d04ce51dc9b995d5e21-0, Actual action: Deleted, Requested action: Deleted, Secondary action: Deleted, Event time: 2017-03-13 11:57:53-07, End: 2017-03-13 11:57:53-07, Last update time: 2017-03-13 11:57:53-07, Domain: -, Server: sepxxxx, User: dave, Source computer: DAVE-LAPTOP, Source IP: 10.1.1.190, Disposition: Good, Download site: null, Web domain: null, Downloaded by: null, Prevalence: Reputation was not used in this detection., Confidence: Reputation was not used in this detection., URL Tracking Status: Off, First Seen: Reputation was not used in this detection., Sensitivity: Low, MDS, Application hash: 256ea793b46e9ac3e6e36c459256876c, Hash type: md5, Company name: HHHHH, Application name: , Application version: , Application type: -1, File size (bytes): 345088, Category set: Security risk, Category type: UNKNOWN

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 сосредоточиться 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

Threat Name:	Trojan_Generic.DC
Threat Category:	Trojan_Generic
Captured From:	HTTP Traffic
Source:	18.23.92.114
Source Address:	vibmdyap.lidlima.com (18.23.92.114) USA
Source URL:	http://vibmdyap.lidlima.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

- Find on VirusTotal
- Download Sample
- Download Behavior Log
- Generate IVP
- Add to Whitelist
- Report False Positive



History

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

Behavior Information	
Top Indicators:	<ul style="list-style-type: none">+ 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 timeHighest total committed memory for a process in a cook
VM Network Callbacks:	None
Anti-Debugging:	None

Search:

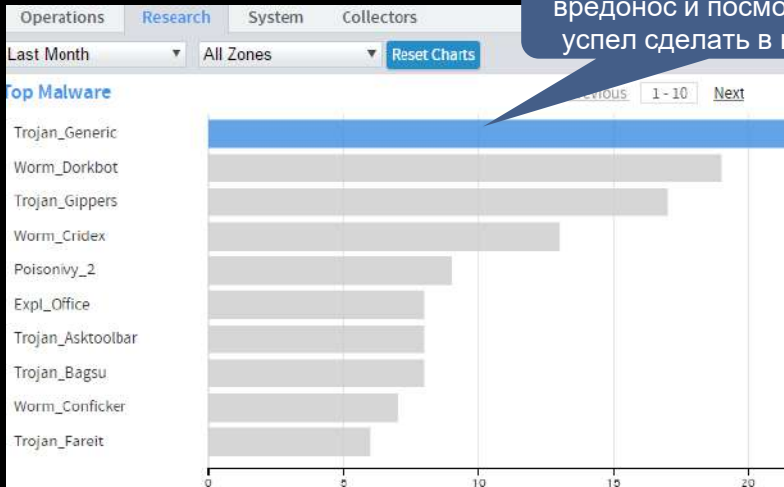
	Severity	Threat Name	File Type	Collector
--	----------	-------------	-----------	-----------

Malware Indicators

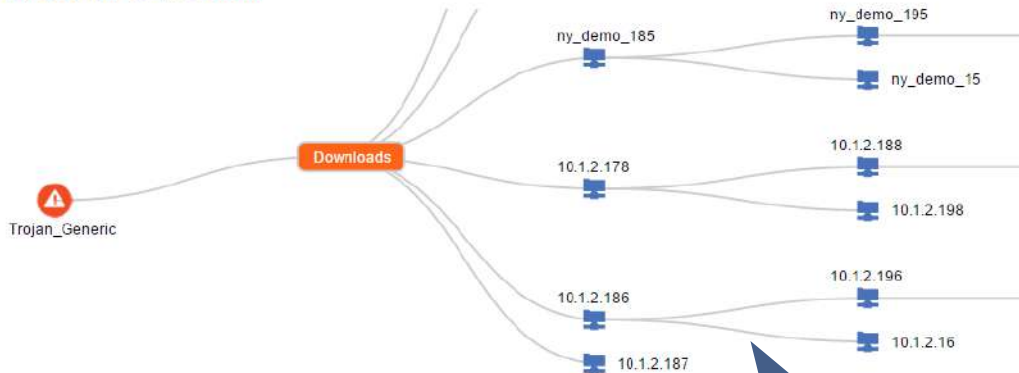
Malicious Trait	Behavior	Details
Anti Sandbox	Checks the System BIOS/Processor registry key to see if it contains virtual, vmware, vbox, qemu, etc.	\\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0
	Checks the System BIOS/Processor registry key to see if it contains virtual, vmware, vbox, qemu, etc.	\\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\~MHz*
Suspicious Processes	Creates a process that runs in a suspicious path	C:\WINDOWS\Temp\sqlserver.exe
Suspicious File Drops	Creates a suspicious file	c:\WINDOWS\Temp\sqlserver.exe c:\WINDOWS\Temp\USBServers32.exe c:\WINDOWS\Temp\ttdelLzz.bat c:\WINDOWS\Temp\ttotozzz.bat C:\Program Files\Microsoft Office\HelpLib\Agnt\CL_TMPCgi\UT5.exe c:\WINDOWS\Temp\Server32\History.dat
Persistence	Drops file in the startup folder so it run automatically at togon	C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\Update.bat
Suspicious Registry Modifications	Some malwares like to set these key values	\\REGISTRY\USER\S-1-5-21-842925246-484763869-117609710-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{dc3e8586-365a-11e1-9c6d-e06d6172696f}\BaseClass* \\REGISTRY\USER\S-1-5-21-842925246-484763869-117609710-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{59dfa098-9b09-11e2-9897-806d6172696f}\BaseClass* \\REGISTRY\USER\S-1-5-21-842925246-484763869-117609710-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{9cd0cdd9-900f-11e2-ba02-525400123456}\BaseClass*
Suspicious File Accesses	Sample opens itself	C:\Program Files\Microsoft Office\HelpLib\Agnt\CL_TMPCgi\UT5.exe
Suspicious Registry Accesses	Key that usually gets exploited by DDos attack malware which exploits known Microsoft RPC flaw	\\REGISTRY\MACHINE\SOFTWARE\Microsoft\Rpc \\REGISTRY\USER\S-1-5-21-842925246-484763869-117609710-500\Software\Microsoft\Internet Explorer\Security \\REGISTRY\MACHINE\SOFTWARE\Microsoft\Internet Explorer\Security
	Locks at key that deals with Internet Explorer authentication support settings	\\REGISTRY\USER\S-1-5-21-842925246-484763869-117609710-500\Software\Microsoft\Internet Explorer\Security\DisableSecuritySettingsCheck* \\REGISTRY\MACHINE\SOFTWARE\Microsoft\Internet Explorer\Security\DisableSecuritySettingsCheck*
Makes Network/Internet connection	Makes a TCP connection	87.106.20.192:80
Other Suspicious Behaviors	Sends an io control code to an unknown device in the kernel	device-0x22_function-0x51_method-0x0_access-0x2 device-0x22_function-0x53_method-0x0_access-0x1
	Sends an io control code to a known device in the kernel	device-0x12_function-0x0_method-0x3_access-0x0 device-0x39_function-0x2_method-0x0_access-0x0

Подробные данные о поведении ВПО на каждой зафиксированной стадии

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



Threat Progression - Trojan_Generic



Узлы, для которых были зафиксированы свидетельства заражения

Total Malware Found

Top Malware Countries

- High
- Low
- Med



Threat Details

Threat Name: Trojan_Generic.DC
File Type: PE32 executable (console) Intel 00386, for MS Windows
File Size: 159,744 (156KB)

File Hashes: 6 hashes total

Most Recent: Mar 16 14:17:04 Pacific Daylight Time
MD5: 18ccf42cc51f02a59803bc995ac16fdb
SHA1: 7fab7695a10b101ae240c5f4e87553fcc0cf06d5
SHA256: 9ee2d976ff311c47311396508f0fcbafee2298361dce78e54eb8a5e1e8d1dd5

[View all File Hashes](#)

Top Indicators:

- Creates a process in some suspicious paths which are temporary in nature
- Sets a page of memory to EXECUTE
- Masquerades as standard Windows component
- Sleeps for an excessive amount of time
- Highest total committed memory for a process in a cook



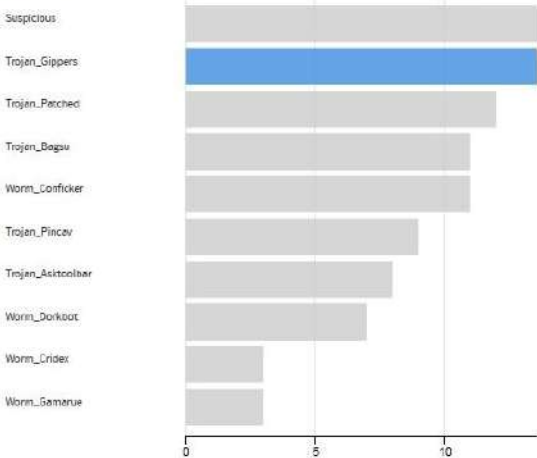
Last 3 Months

All Zones

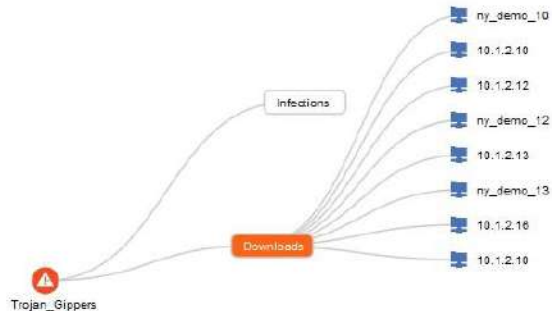
Reset Charts

Top Malware

Previous 1-10 Next



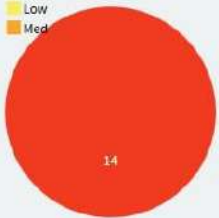
Threat Progression - Trojan_Gippers



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

Total Malware Found

High
Low
Med



Top Malware Countries



Threat Details

Threat Name: TROJAN_GIPPERS.DC
File Type: PE32 executable (GUI) Intel 60386, for MS Windows
File Size: 1 205 788 (1MB)

File Hashes : 8 hashes total

Most Recent: Nov 26 02:05:03 GMT+0300
MD5: bf1b44a20430e597c16b9680b8e417fc
SHA1: e33cd5839729947a38b4a12b19fa8d4679c1502
SHA256: b1242375d516e06844c58724567b00f4754de942efde65cfc465a07d0edc74ef
[View all File Hashes](#)

Malware Indicators:

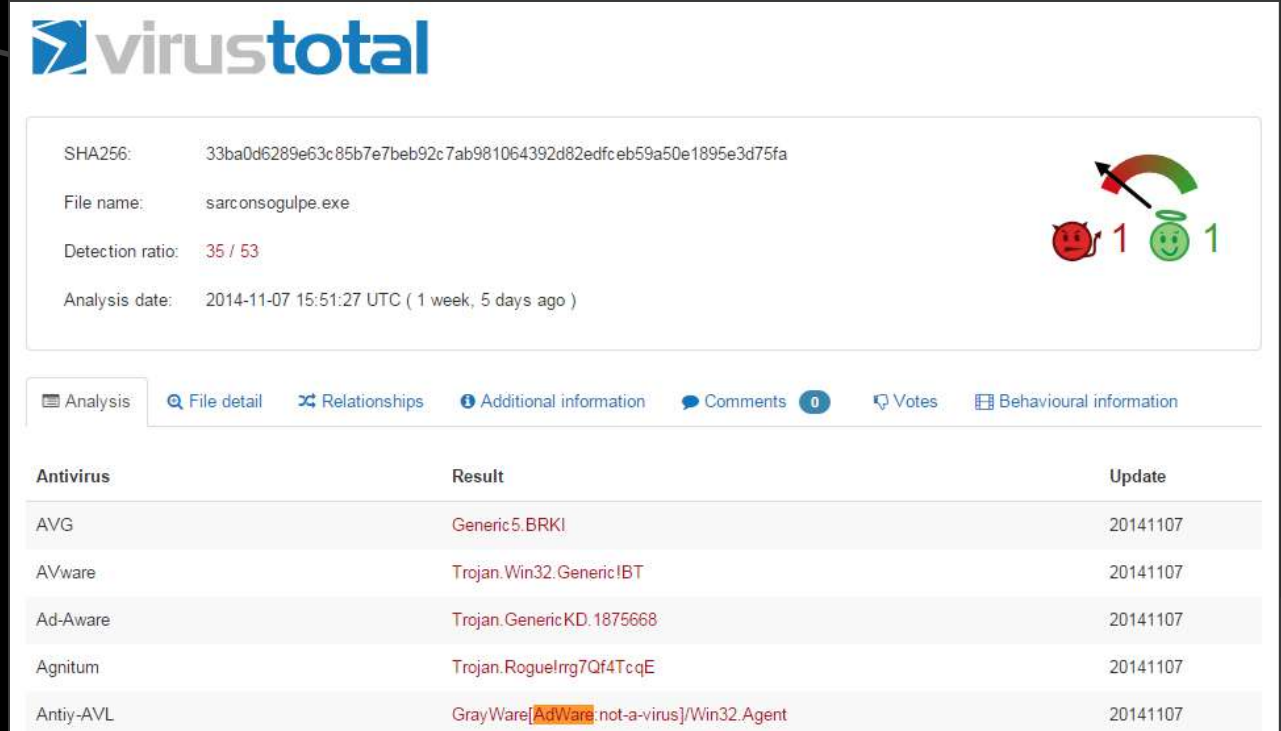
- Creates suspicious file with intention to overwrite on system paths
- Creates a process that runs in a suspicious path
- Opens suspicious registry key
- Sample opens itself
- Copies malicious file to system paths

File Hashes related to TROJAN_GIPPERS.DC

Date	MD5	SHA1	SHA256
Nov 26 02:05:03 GMT+0300 Show Incident	bf1b44a20430e597c16b9680b8e417fc	e33cd5839729947a38b4a12b19fa8d4679c1502	b1242375d516e06844c58724567b00f4754de942efde65cfc465a07d0edc74ef
Dec 2 02:05:03 GMT+0300 Show Incident	bf1b44a20430e597c16b9680b8e417fc	e33cd5839729947a38b4a12b19fa8d4679c1502	b1242375d516e06844c58724567b00f4754de942efde65cfc465a07d0edc74ef
Dec 15 20:39:48 GMT+0300 Show Incident	bf1b44a20430e597c16b9680b8e417fc	e33cd5839729947a38b4a12b19fa8d4679c1502	b1242375d516e06844c58724567b00f4754de942efde65cfc465a07d0edc74ef

3. Подтверждение: VirusTotal

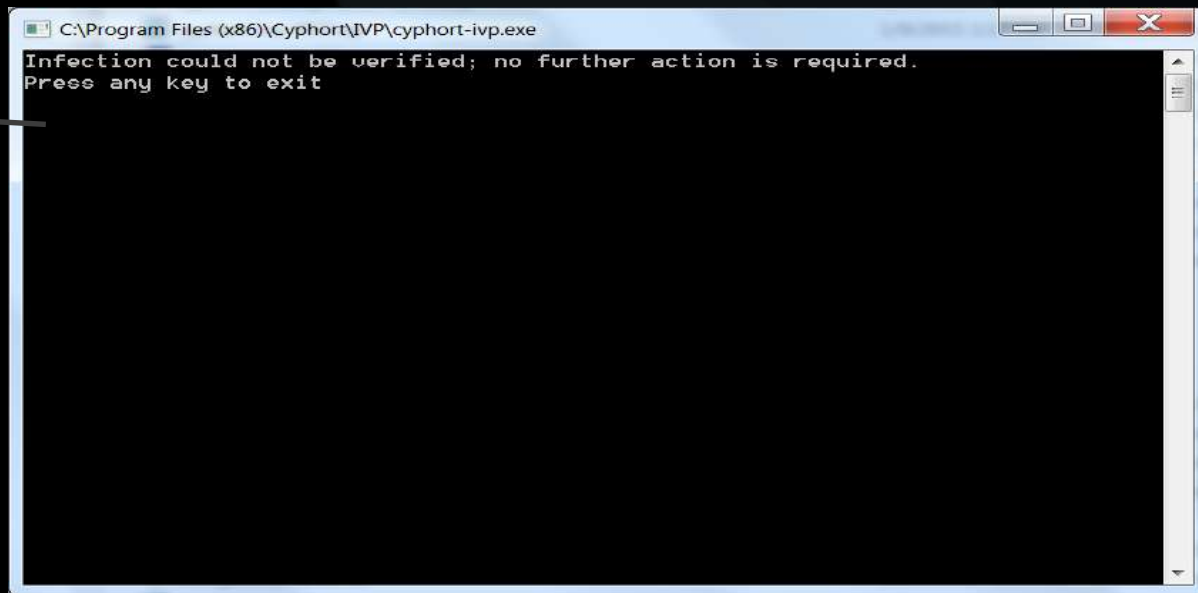
- Find on VirusTotal
- Download PCAP Trace
- Download Sample
- Download Behavior Log
- Generate IVP
- Add to Whitelist
- Report False Positive



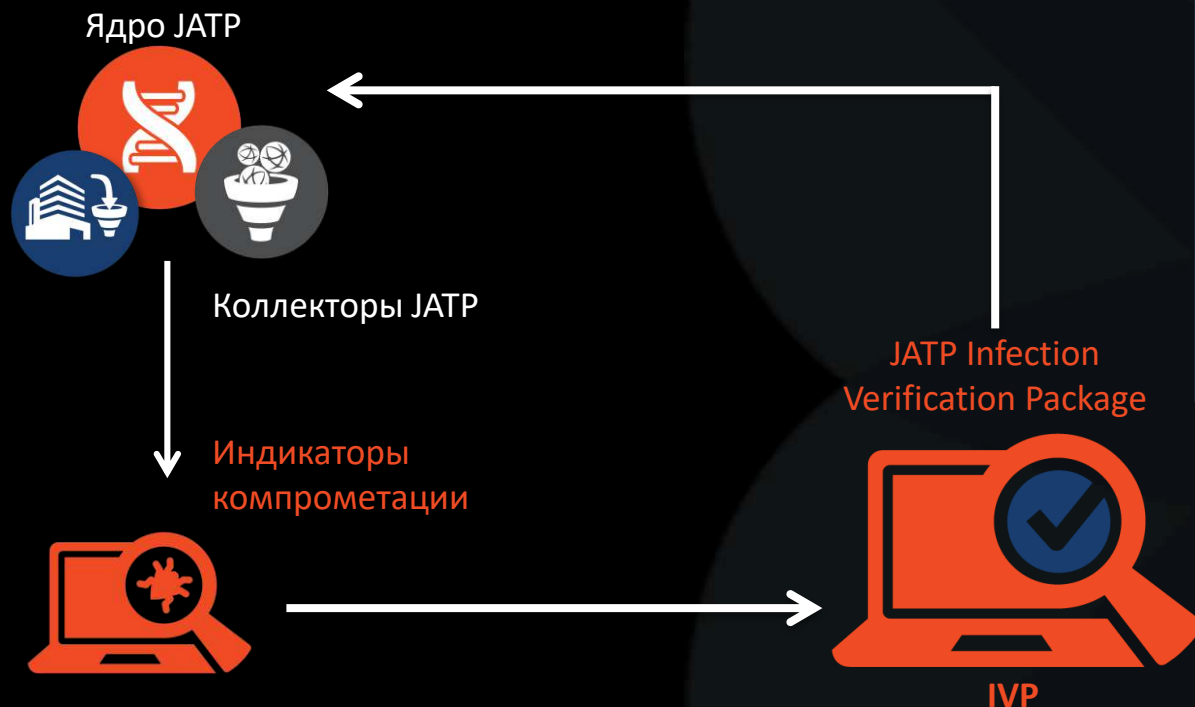
The screenshot shows the VirusTotal analysis page for the file `sarconsogulpe.exe`. The page displays the SHA256 hash, file name, detection ratio (35/53), and analysis date. A navigation bar includes tabs for Analysis, File detail, Relationships, Additional information, Comments (0), Votes, and Behavioural information. Below the navigation bar is a table of antivirus results.

Antivirus	Result	Update
AVG	Generic5.BRKL	20141107
AVware	Trojan.Win32.Generic!BT	20141107
Ad-Aware	Trojan.GenericKD.1875668	20141107
Agnitum	Trojan.RogueIrg7Qf4TcqE	20141107
Antiy-AVL	GrayWare[AdWare:not-a-virus]/Win32.Agent	20141107

3. Подтверждение: Infection Verification Pack (IVP)



Infection Verification Pack



Изменения в ОС:


Ключи реестра, созданные Mutex, запущенные процессы, загруженные файлы и т.д.

JATP позволяет создать пакет IVP для запуска на конечном 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

3. Подтверждение: проверка целевых узлов IVP

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

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

The screenshot shows the 'System Defaults' configuration page in a web interface. On the left is a dark blue sidebar with navigation items: Notifications, System Profiles, Password Reset, Roles, Zones, Users, SAML Settings, RADIUS Settings, System Settings (highlighted), Certificate Management, GSS Settings, Web Collectors, and Email Collectors. The main content area is titled 'System Defaults' and contains the following settings:

- Hostname: tap35
- Server fully-qualified domain name: tap35
- IVP format: MSI Self-extracting Zip file [Download MSI](#)
- Software Update enabled:
- Content Update enabled:
- Enable Cyphort support account:
- Restart services now:
- Reboot appliance now:
- Clear event database:
-

A 'System Settings' button with a wrench icon is located on the right side of the configuration area.

Интеграция с EDR

ADVANCED THREAT PREVENTION APPLIANCE

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications +

System Profiles +

Environmental Settings -

Email Mitigation Settings

Firewall Mitigation Settings

Asset Value

Anti-Virus Configuration

Endpoint Integration Settings

BlueCoat Configuration

Whitelist Rules

YARA Rule Upload

SNORT Rule Upload

Identity Configuration

Splunk Configuration

External Event Collectors

Endpoint Type:

CarbonBlack

CrowdStrike

Cancel

Current Endpoint Integration

Description	Actions
CarbonBlack : 172.19.100.25	Disable Delete Edit Test

All File Uploads (4 shown)

Search: Last Month CSV Upload File

Status	Incident Id	Risk	Threat	File Name	Uploaded By	Date & Time	Analysis Status	Zone
				archive manager.dmg	jperez	Feb 8 23:25:33 GMT+0300	Complete	Default Zone
				hmar6.jar	kanat	Jan 31 01:05:14 GMT+0300	Complete	Default Zone
New	620713	HIGH	TROJAN_AGENT.Rep	DFX-Patch-SiCarli.exe	kanat	Jan 31 00:33:30 GMT+0300	Complete	Default Zone
				hmar6.jar crossrat sample	kanat	Jan 30 14:57:10 GMT+0300	Complete	Default Zone

Details for TROJAN_AGENT.Rep

SUMMARY UPLOADS

Search:

Severity	Threat Name	File Type	Collector
	MD5: 97c0436e257d1cc22b36300966a2cdc		
	SHA1: 3aedb25f95dcfd9e997c2221f03a77e9bacb12f		
	SHA256: a95dd946acbe215a4b09e216e42829a515283da5c85884f0ca2004b4ee903bdf		

Signed by: N/A

History

Analysis Timestamps	Severity
Jan 31 00:42:41 GMT+0300	High
Jan 31 00:42:35 GMT+0300	Benign

Process graph

No sub-processes spawned.

Malware Indicators

Malicious Trait	Behavior	Details
Suspicious File Drops	Creates a suspicious file	C:\Users\John\AppData\Local\Temp\baasmod.dll C:\Users\John\AppData\Local\Temp\dup2patcher.exe
Other Suspicious Behaviors	Sends an Io control code to a known device in the kernel	device-0x39_function-0x2_method-0x0_access-0x0
	Opens a named mutex	C:\Load\WinSta\WinSta0 Local\MSCTF.Ctl\Monitor\Inst\MutexDefault1

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 fabien

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

All Incidents (185 shown, 185 total)

Search: Show Threat All Zones Last Month

Status	Incident ID	Risk	Threat	Progression	Collector Type	Threat Source	Threat Target	Zone	Target OS	Collector	Date & Time
New	647952	HIGH	WORM_CRIDEX.CY	DL	Web	greatfilesarey.asia	10.1.1.129	Default Zone	unknown	Security Analytics Demo	Mar 8 09:07:01 Pacific Standard Time
New	647951	MED	WORM_DORKBOT.DC	DL	Web	greatfilesarey.asia	10.2.1.128	Default Zone	unknown	Security Analytics Demo	Mar 8 04:56:28 Pacific Standard Time
New	647950	HIGH	WORM_CRIDEX.CY	DL	Web	greatfilesarey.asia	10.1.1.122	Default Zone	unknown	Security Analytics Demo	Mar 8 02:45:04 Pacific Standard Time
New	647949	MED	WORM_DORKBOT.DC	DL	Web	greatfilesarey.asia	10.2.1.127	Default Zone	unknown	Security Analytics Demo	Mar 7 23:03:48 Pacific Standard Time
New	647948	HIGH	WORM_CRIDEX.CY	DL	Web	greatfilesarey.asia	10.1.1.121	Default Zone	unknown	Security Analytics Demo	Mar 7 20:52:23 Pacific Standard Time
New	647947	MED	WORM_DORKBOT.DC	DL	Web	greatfilesarey.asia	10.2.1.130	Default Zone	unknown	Security Analytics Demo	Mar 7 16:41:50 Pacific Standard Time
New	647946	MED	WORM_DORKBOT.DC	DL	Web	greatfilesarey.asia	10.2.1.129	Default Zone	unknown	Security Analytics Demo	Mar 7 10:49:09 Pacific Standard Time
New	647945	MED	TROJAN_POISON.DC	DL	Web	die-tradlers.de	10.3.1.34	Default Zone	Windows 7	Security Analytics Demo	Mar 7 10:05:01 Pacific Standard Time
New	647944	HIGH	WORM_CRIDEX.CY	DL	Web	greatfilesarey.asia	10.1.1.123	Default Zone	unknown	Security Analytics Demo	Mar 7 08:37:44 Pacific Standard Time
New	647941	MED	WORM_DORKBOT.DC	DL	Web	greatfilesarey.asia	10.1.1.119	Default Zone	unknown	Security Analytics Demo	Mar 7 00:02:22 Pacific Standard Time
New	647943	MED	WORM_GAMARUE.DC	DL	Web	greatfilesarey.asia	10.1.5.142	Default Zone	unknown	Security Analytics Demo	Mar 7 00:00:06 Pacific Standard Time
New	647942	MED	WORM_CONFICKER.DC	DL	Web	greatfilesarey.asia	10.1.5.171	Default Zone	unknown	Security Analytics Demo	Mar 7 00:00:02 Pacific Standard Time

Details for WORM_CRIDEX.CY

SUMMARY DOWNLOADS CUSTOM RULES

Actions
Actions
Mitigate Incident
View Timeline

Incident ID: 647944
Host Name: -
User Name: -
IP Address: 10.1.1.123
FQDN: 10.1.1.123
Source Email ID: -
Destination Email ID: -
Risk: High
Threat Category: Trojan_Generic

Progression:

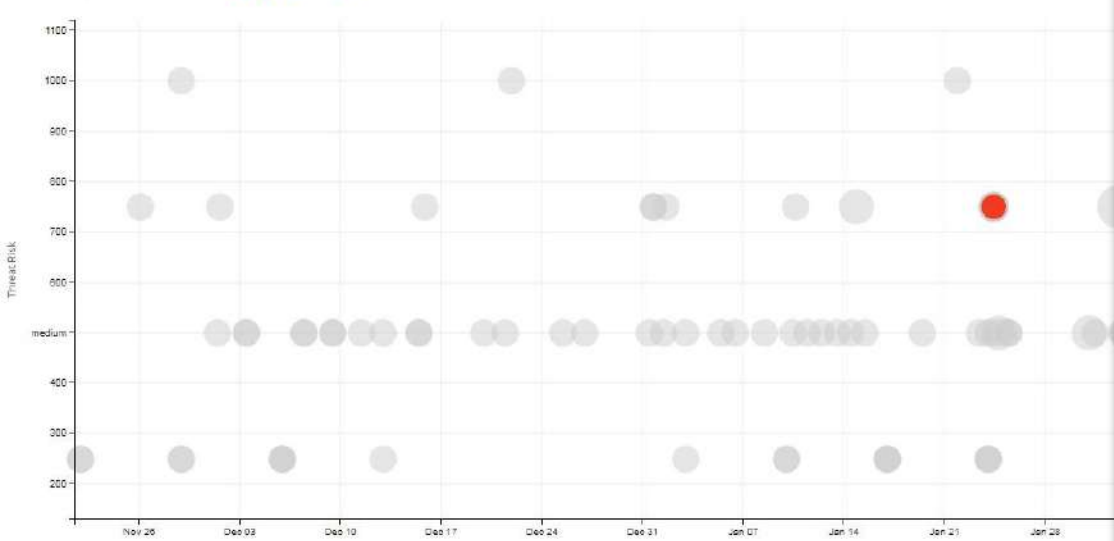
DELIVERY EXPLOITATION & INSTALLATION COMMAND & CONTROL ACTION ON TARGETS

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

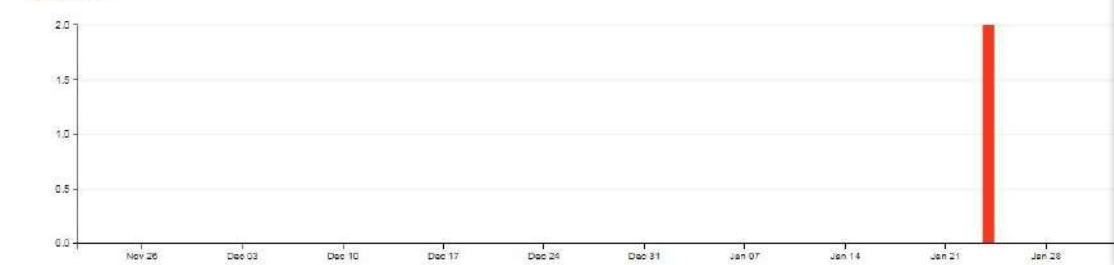
Triggers: Reputation Behavior Network Static

Custom Rules: Lateral Spread Infection Execution Downloads

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



Malware Trend



Host Details

Target

Hostname: -
 IP Address: 10.1.2.16
 Source Email ID: -

Asset Value: Medium
 Time: Jan 24, 2018 09:51:21 RTZ 2 (3MMA)

User: -
 FQDN: -
 Destination: -

Anti-Virus: Not Configured
 OS: Windows 7

Progression

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

Actions

- Actions
- View Incident
- View Timeline
- Mitigate Incident

Переход в раздел Mitigation

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

В разделе нейтрализации угроз можно выбрать действия для предотвращения заражения.

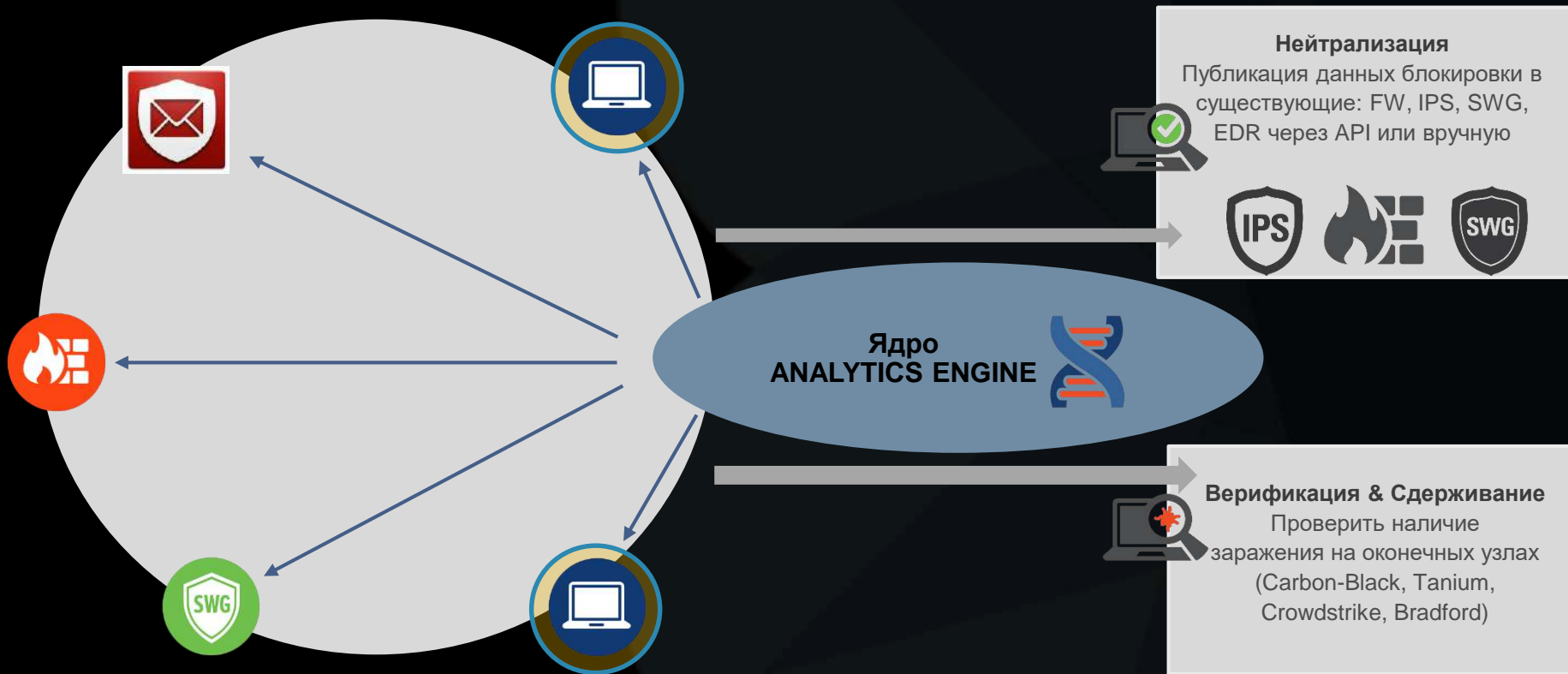
JATP умеет взаимодействовать со сторонними продуктами безопасности

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

IP Filtering URL Filtering IPS Signatures Endpoint Infection Verification Emails

App	Remove	Push to Device	Severity	Confidence	Owner	Threat	Threat Source	Mal
		Enabled	Medium	Max	cyad min	malvertising	Juniper Labs	23
		Disabled	Medium	Max	JATP	malvertising	Juniper Labs	89.44.4
		Enabled	Medium	High	cyad min	VIRUS:WIN32_SALITY_AU.CY	Local	109.179.219.135
		Enabled	Max	High	gsuzuki	TROJAN_Foreit.CY	Local	115.47.49.181
		Disabled	Medium	High	JATP	VIRUS:WIN32_SALITY_AU.CY	Local	122.155.166.149
		Enabled	Medium	High	cyad min	TROJAN_ZeroAccess.CY	Local	173.193.250.103
		Disabled	Medium	High	JATP	TROJAN_ASKTOOLBAR.CY	Local	18.23.92.114
		Enabled	Medium	High	USER	TROJAN_ASKTOOLBAR.CY	Local	183.44.23.12
		Enabled	High	High	cyad min	TROJAN_Trojan.CY	Local	193.106.172.140
		Disabled	Medium	High	JATP	VIRUS:WIN32_SALITY_AU.CY	Local	195.22.26.231
		Disabled	Medium	High	JATP	VIRUS:WIN32_SALITY_AU.CY	Local	195.22.26.253
		Enabled	High	High	USER	TROJAN_Pincav.CY	Local	199.59.243.106
		Disabled	Medium	High	JATP	VIRUS:WIN32_SALITY_AU.CY	Local	37.59.11.189
		Enabled	High	High	USER	TROJAN_Gippers.CY	Local	74.206.164.166
		Disabled	High	Medium	JATP	TROJAN_ROGUE.CY	Local	199.7.61.118
		Disabled	Low	Low	JATP	TROJAN_Generic.CY	Local	213.192.75.2
		Disabled	Low	Low	JATP	TROJAN_Generic.CY	Local	222.186.222.250
		Disabled	Low	Low	JATP	TROJAN_Generic.CY	Local	79.96.91.234
		Enabled	Low	Low	USER	SUSP_KRADDARE.CY	Local	115.66.58.5

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

Firewall/SWG



BLUE COAT



Check Point
SOFTWARE TECHNOLOGIES LTD.

JUNIPER
NETWORKS



FORTINET

Endpoint



CARBON CROWDSTRIKE
BLACK

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
<code>event_id</code> or <code>md5sum/sha1sum</code>	[Required] Unique identifier for this event. One of these parameters is a mandatory parameter. Get this from the output of the API <a href="https://<Host>/cyadmin/api.php?op=events">https://<Host>/cyadmin/api.php?op=events The <code>md5sum</code> & <code>sha1sum</code> are the hashes of the objects.
<code>get_components</code>	1 indicates components are available When the <code>get_components</code> 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 Surphort и признание в индустрии

Компания

Основана: 2011, Santa Clara, CA (HQ)

Решение: Обнаружение продвинутых угроз, аналитика и нейтрализация

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

Признание

2017



2016



2015

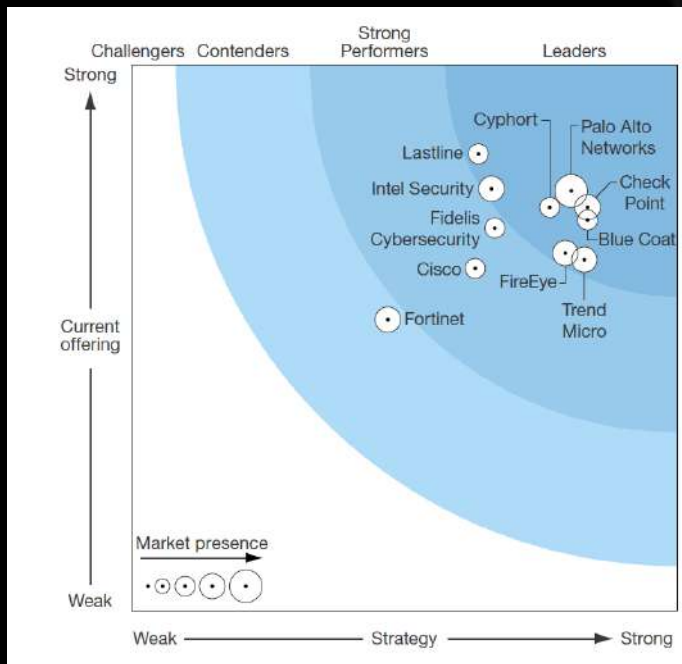


2014



Высокие результаты независимых тестов

FORRESTER®



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

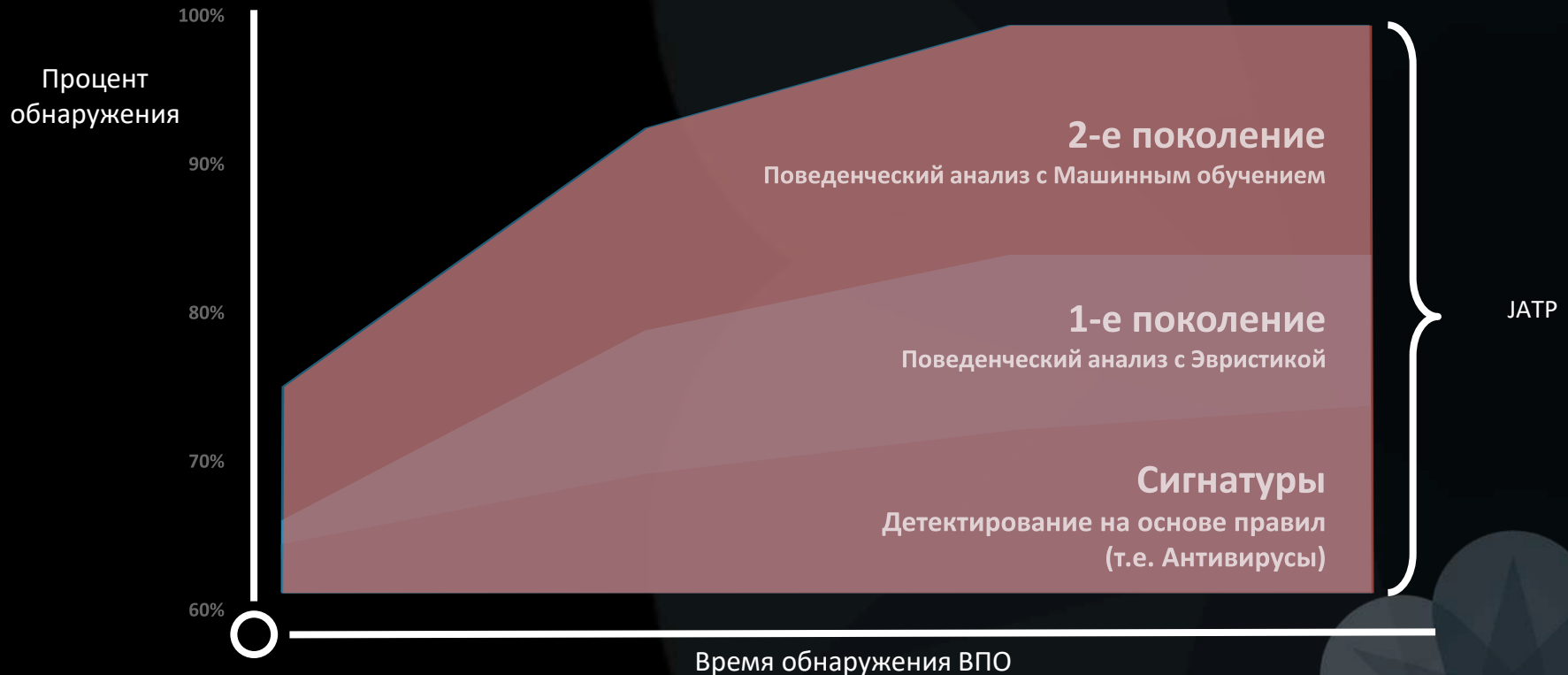


Как JATP работает

Ключевые компоненты JATP



Глубокий анализ JATP значительно эффективнее сигнатурного анализа



Продвижение угрозы по Cyber Kill Chain

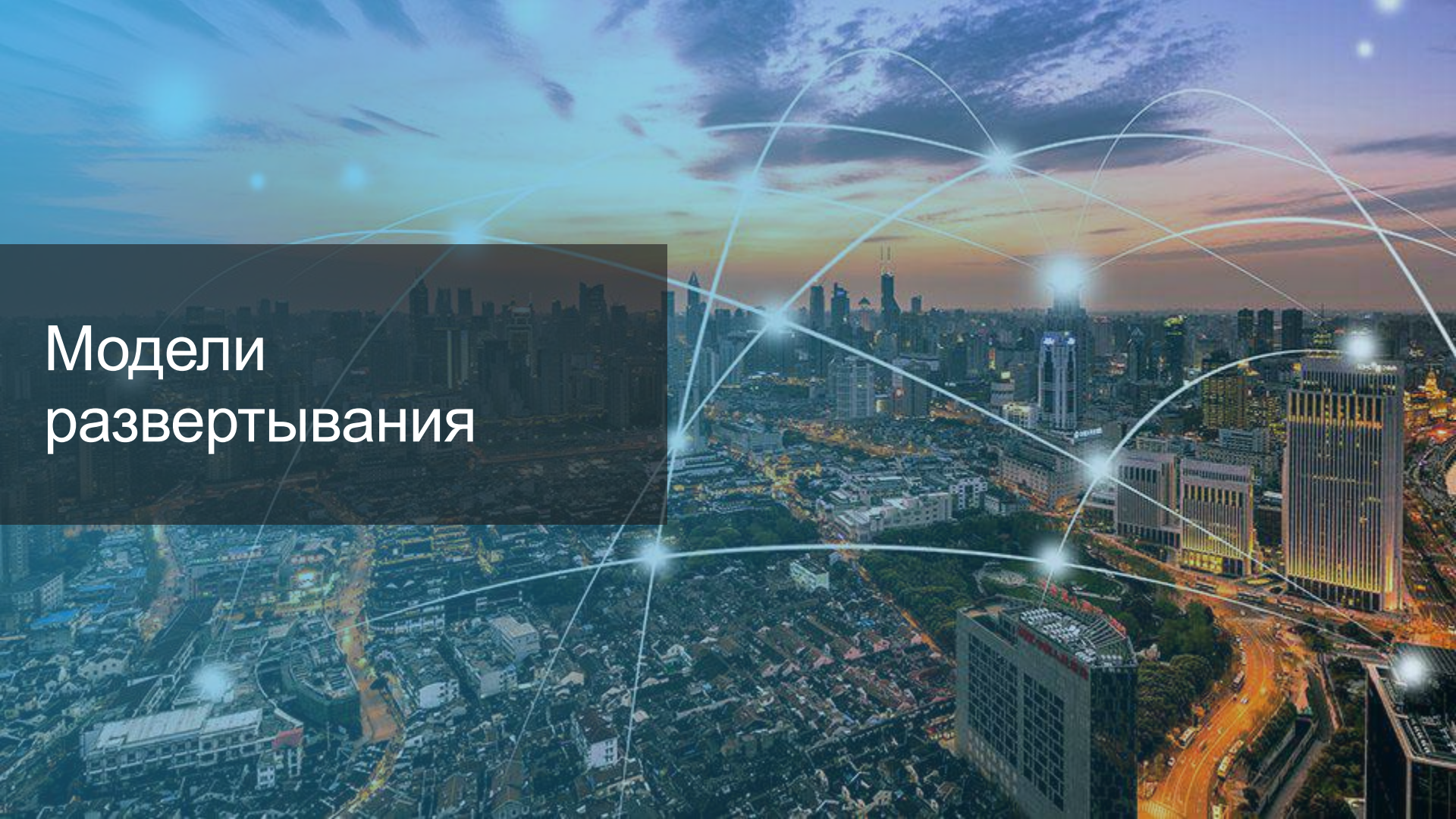


Juniper
Advanced
Threat
Prevention
Appliance
(JATP)

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

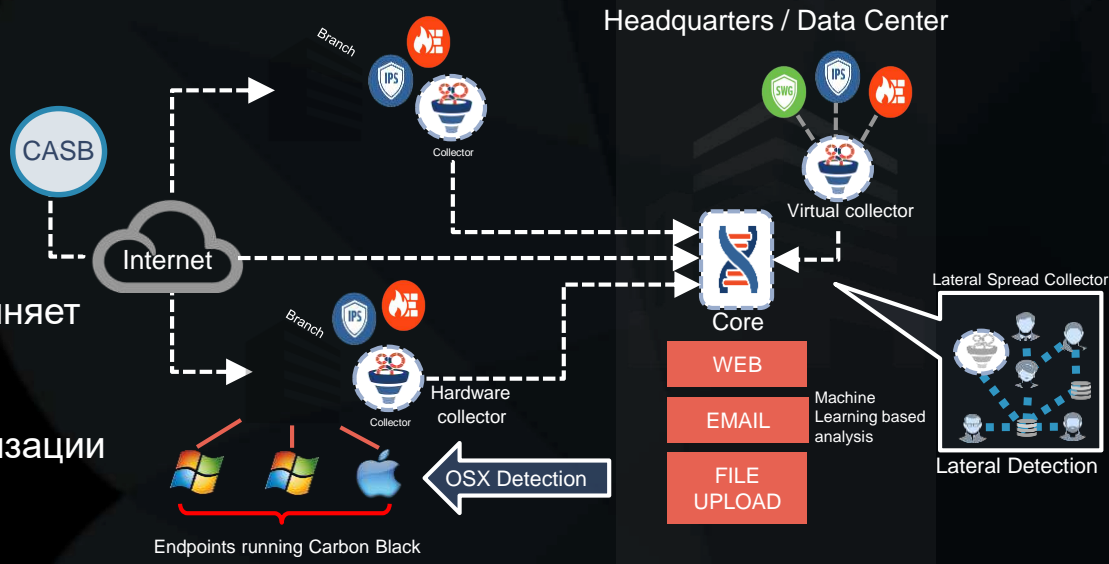


An aerial night view of a city, likely Shanghai, with a network of glowing white lines and nodes overlaid on the scene. The lines connect various points across the city, suggesting a network or data flow. The city lights are visible in the background, and the sky is a mix of blue and purple hues.

Модели развертывания

Развертывание

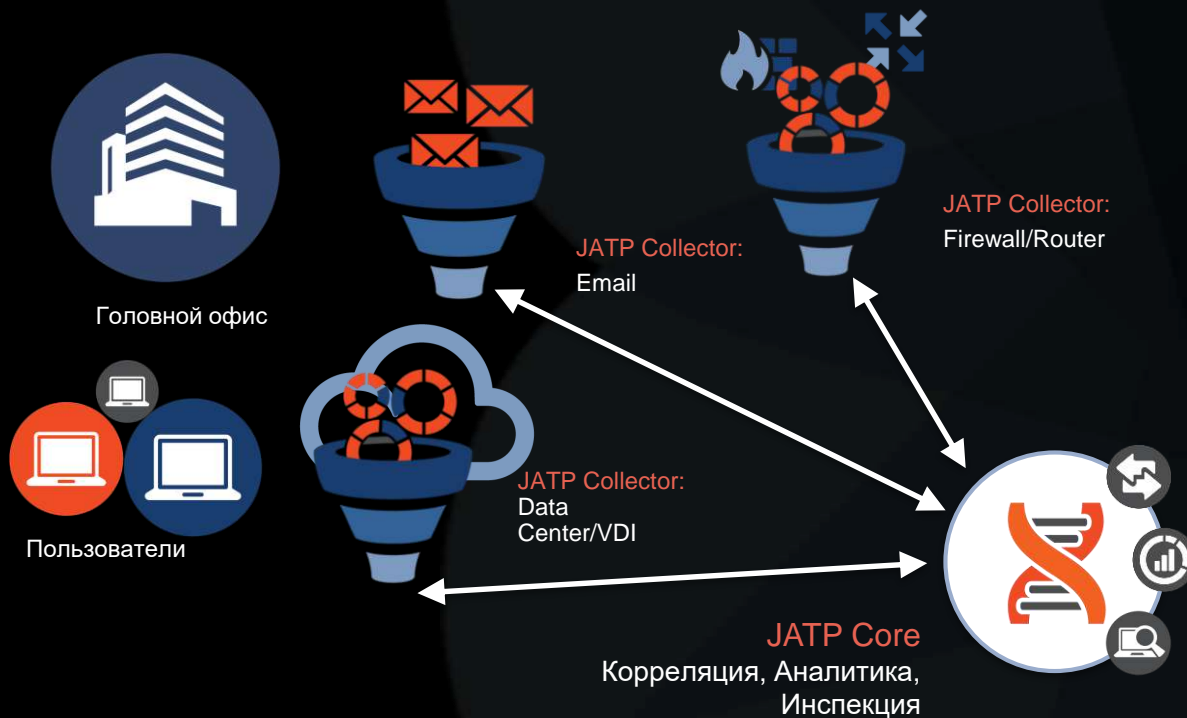
- Центральное Ядро JATP собирает информацию от коллекторов, выполняет детектирование и анализ;
- Компоненты управления и нейтрализации угроз входят в состав Ядра;
- Коллекторы собирают данные о Web и SMB трафике со SPAN/TAP портов сетевых устройств;
- Коллекторы почты собирают данные с почтовых серверов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



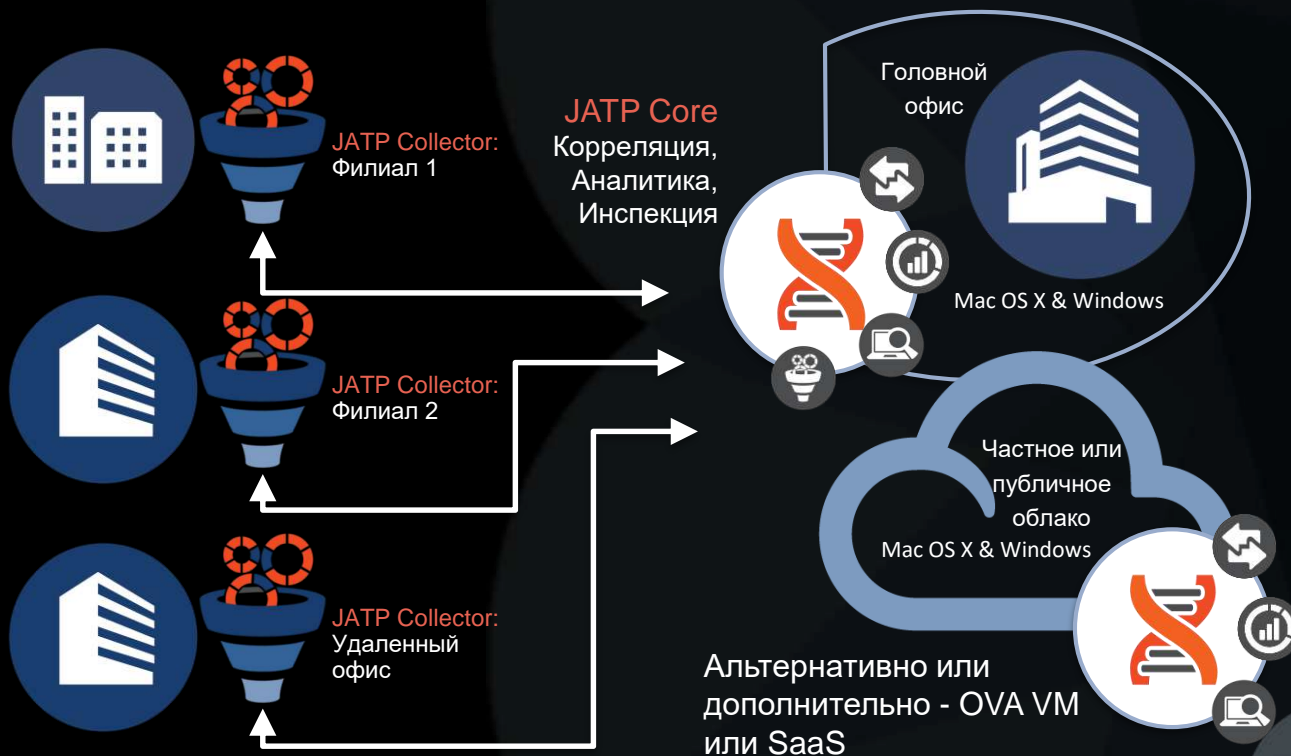
Опции для Ядра и Коллекторов:

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

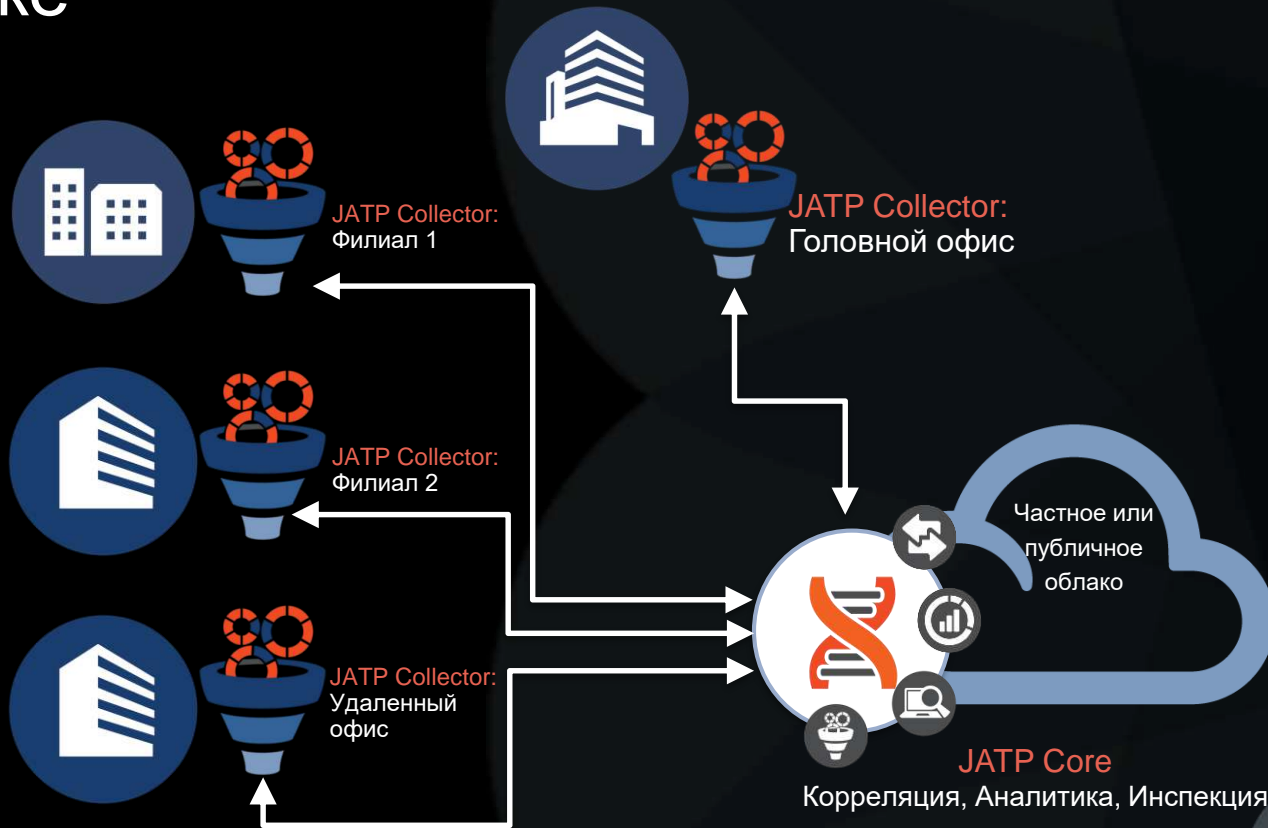
Развертывание в центральном офисе



Развертывание на нескольких площадках

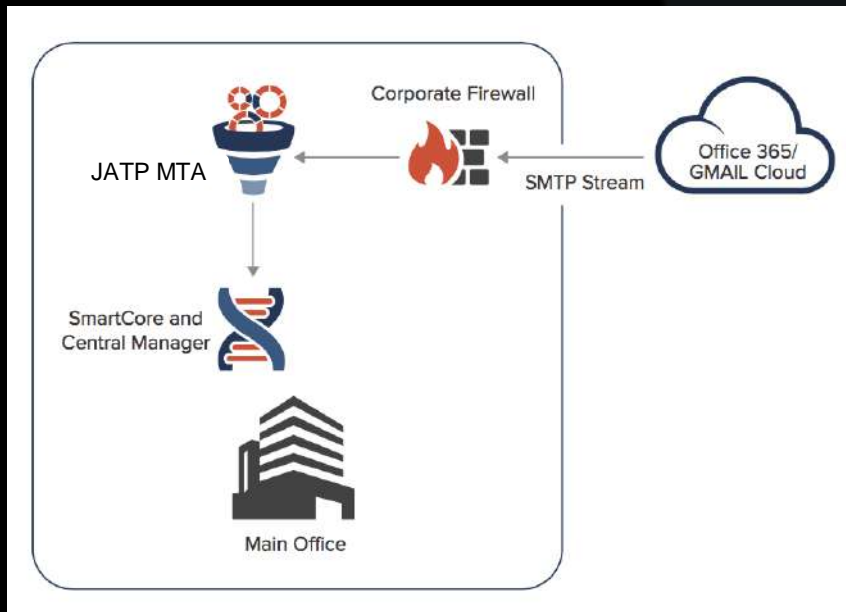


Развертывание в частном или публичном облаке



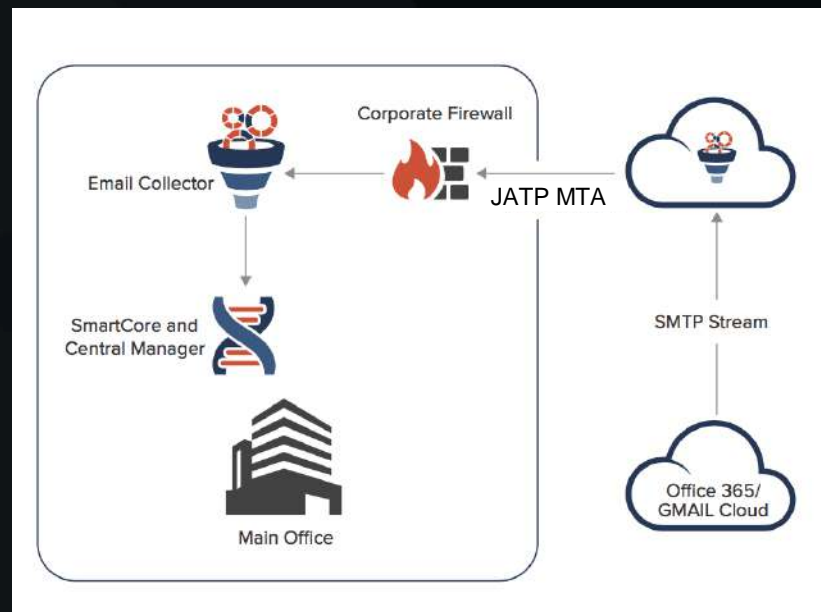
Развертывание – анализ почты

Сбор почты локальным коллектором



JATP MTA развернут локально

Сбор почты коллектором в облаке

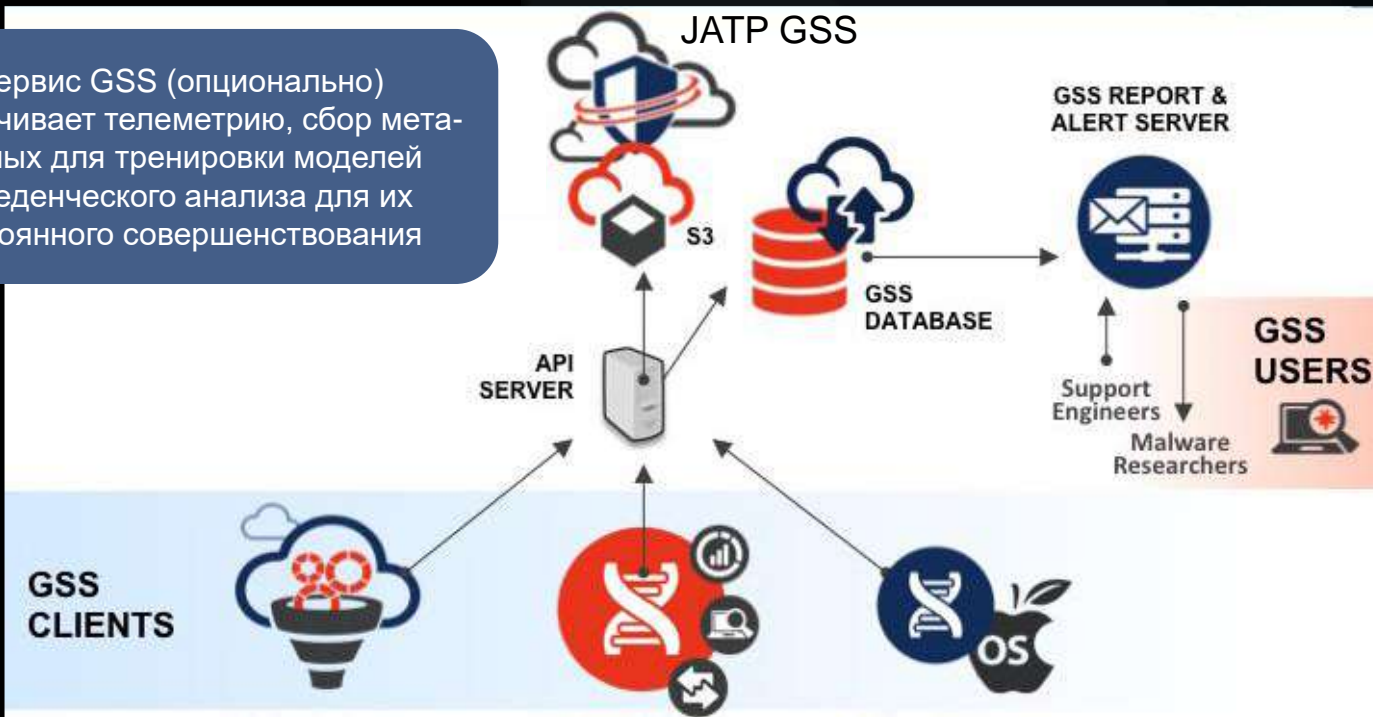


JATP MTA развернут в частном облаке

JATP MTA устанавливается out-of-band, не inline

Global Security Service

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



Коллектор

Основное ядро

Вторичное ядро

Juniper Threat Network

Однонаправленная и двунаправленная модели взаимодействия (опционально) :

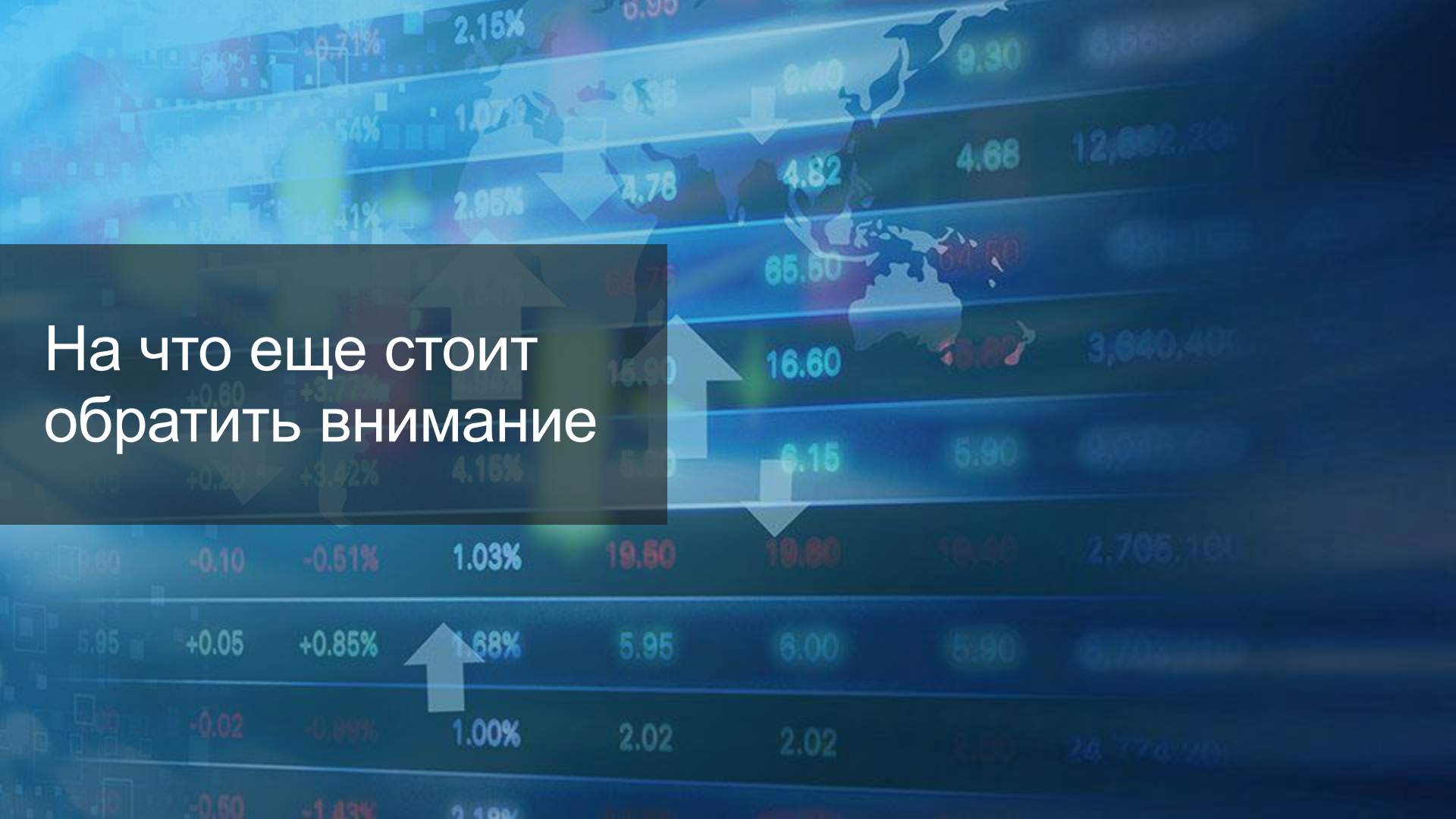
- Пользователь получает обновления, но сам ничего не отправляет;
- Пользователь получает обновления, отправляет мета-данные и телеметрию.



Обновления моделей машинного обучения

Обновления данных Threat intelligence

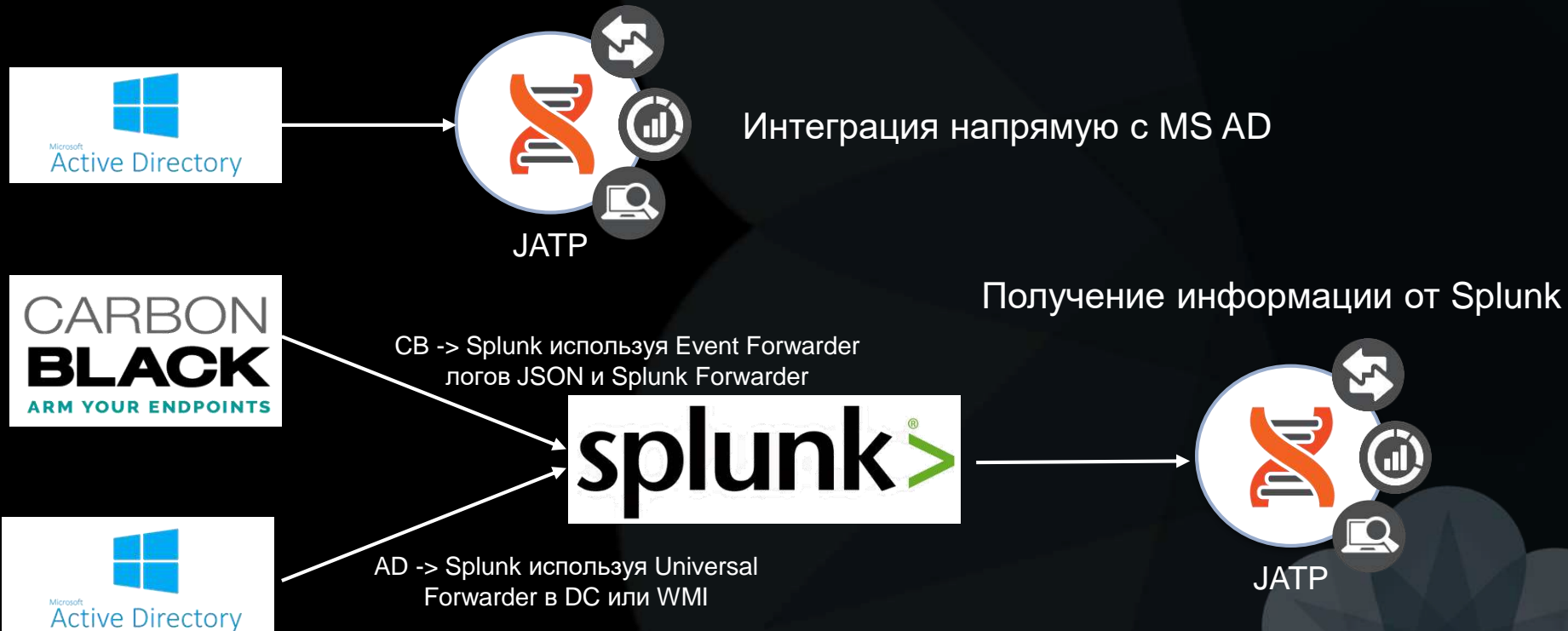
Обновление модулей репутационного и статического анализа



На что еще стоит
обратить внимание

Интеграция с Active Directory

Получение подробных данных о пользователях и машинах



Автоматическая нейтрализация ВПО

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

IP Filtering URL Filtering IPS Signatures Endpoint Infection Verification Emails Hosts

Endpoint Infections to be Verified

Search:

	Severity	Target	Threat	Exposure Date	Action
▶	HIGH	ny_demo_16	2 Downloads	Mar 23 14:00:30 Moscow Standard Time	
▶	HIGH	ny_demo_253	2 Downloads	Jul 25 01:34:16 Moscow Standard Time	
▶	HIGH	10.1.2.75	2 Downloads	Aug 12 22:42:11 Moscow Standard Time	
▶	HIGH	ny_demo_41	2 Downloads	Mar 25 17:42:01 Moscow Standard Time	
▶	HIGH	ny_demo_27	3 Downloads	Mar 24 12:45:10 Moscow Standard Time	
▼	HIGH	demo_11	3 Downloads	Mar 23 04:42:13 Moscow Standard Time	

Details for demo_11

HIGH	TROJAN_WITTHY	Fri Mar 23 2018 04:42:13 GMT+0300 (Moscow Standard Time)	Download IVP
HIGH	TROJAN_DROPPER	Sat May 04 2019 16:53:58 GMT+0300 (Moscow Standard Time)	Download IVP
HIGH	TROJAN_WITTHY	Wed Mar 28 2018 23:20:26 GMT+0300 (Moscow Standard Time)	Download IVP
LOW	demo_190	HEUR_AGEN	Aug 10 20:44:27 Moscow Standard Time Download IVP
LOW	demo_46	ADWARE_TARANIS	
LOW	10.1.3.125	HEUR_AGEN	
LOW	demo_51	ADWARE_TARANIS	
LOW	demo_125	ADWARE_TARANIS	
LOW	10.0.1.190	ADWARE_TARANIS	
LOW	10.1.3.227	ADWARE_TARANIS	

- ✓ 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

ADVANCED THREAT PREVENTION APPLIANCE

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

All Incidents (2 shown, 2 total)

Search: Show Threat Last Month

Status	Incident ID	Risk	Threat	Progression	Collector Type	Threat Source	Threat Target	Target
New	5	MED	Suspicious_SSH.HP	LS	LAN	Reg2-Collector-ssh-honeypot	172.16.1.175	
New	4	HIGH	TROJAN:WIN32_MALEX_GEN_E.CY	IN	LAN	nhatlinh98.net	host-1-11.private.cyphort.com.	

Details for TROJAN:WIN32_MALEX_GEN_E.CY

Summary	Severity	Threat	Source	Destination
	Medium	Suspicious_SSH.HP	Reg2-Collector-ssh-honeypot	host-1-11.private.cyphort.com.

Infections

Lateral Spread

Summary

Threat Name: Suspicious_SSH.HP

Description: SSH session attempted on Cyphort Honeypot

Username: root

Source: 172.16.1.200

Analysis Timestamp: Jan 18, 2017 23:48:41 PST

Incident ID: 4

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

Анализ горизонтального трафика

New	5224	HIGH	Trojan_Generic.DC	DL+LS	LAN	ny_demo_185	ny_demo_205	Default Zone	demo next x collector	Jul 16 10:21:24 PDT
-----	------	------	-------------------	-------	-----	-------------	-------------	--------------	-----------------------	---------------------

Details for Trojan_Generic.DC

SUMMARY DOWNLOADS LATERAL SPREAD

Severity	Threat	Source	Destination	Date & Time
High	Trojan_Generic.DC	ny_demo_205	ny_demo_215	Jul 16 10:24:46 PDT

Summary

Threat Name: Trojan_Generic.DC

Captured from: Windows File Transfer

Source: ny_demo_205

Analysis Timestamp: Jul 16, 2017 10:25:19 PDT

Incident ID: 5225

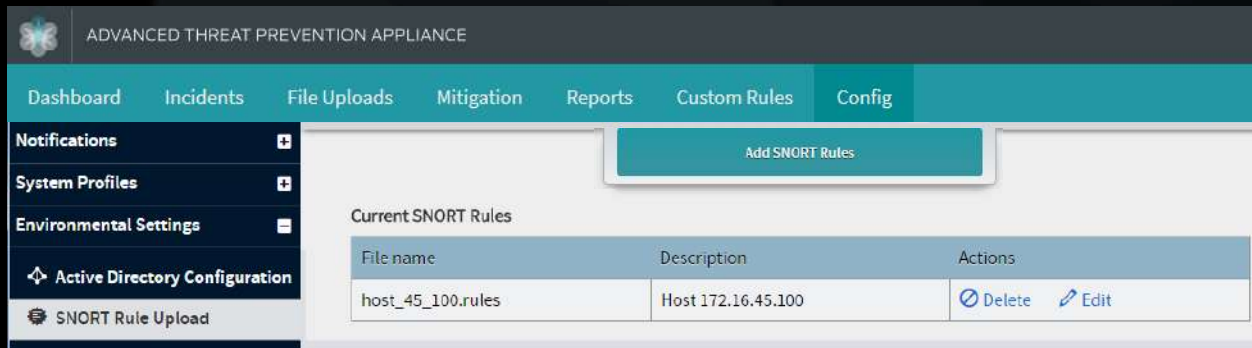
Add to Whitelist

Report False Positive

- 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



ADVANCED THREAT PREVENTION APPLIANCE

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

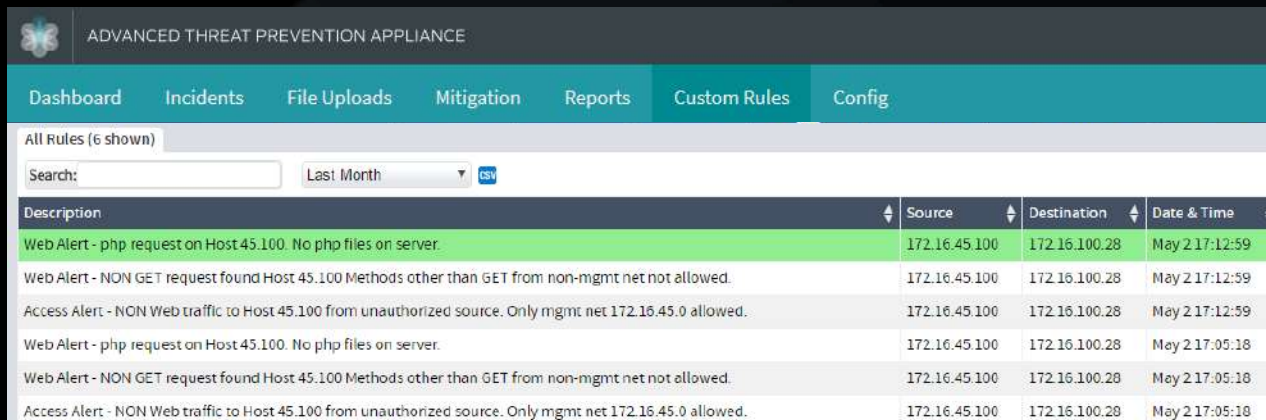
Notifications System Profiles Environmental Settings Active Directory Configuration SNORT Rule Upload

Add SNORT Rules

Current SNORT Rules

File name	Description	Actions
host_45_100.rules	Host 172.16.45.100	Delete Edit

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



ADVANCED THREAT PREVENTION APPLIANCE

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

All Rules (6 shown)

Search: Last Month CSV

Description	Source	Destination	Date & Time
Web Alert - php request on Host 45.100. No php files on server.	172.16.45.100	172.16.100.28	May 2 17:12:59
Web Alert - NON GET request found Host 45.100 Methods other than GET from non-mgmt net not allowed.	172.16.45.100	172.16.100.28	May 2 17:12:59
Access Alert - NON Web traffic to Host 45.100 from unauthorized source. Only mgmt net 172.16.45.0 allowed.	172.16.45.100	172.16.100.28	May 2 17:12:59
Web Alert - php request on Host 45.100. No php files on server.	172.16.45.100	172.16.100.28	May 2 17:05:18
Web Alert - NON GET request found Host 45.100 Methods other than GET from non-mgmt net not allowed.	172.16.45.100	172.16.100.28	May 2 17:05:18
Access Alert - NON Web traffic to Host 45.100 from unauthorized source. Only mgmt net 172.16.45.0 allowed.	172.16.45.100	172.16.100.28	May 2 17:05:18

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

The screenshot displays the 'ADVANCED THREAT PREVENTION APPLIANCE' interface. The top navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The left sidebar lists various settings, with 'YARA Rule Upload' highlighted. A context menu is open over the 'YARA Rule Upload' option, listing actions such as 'Find on VirusTotal', 'Download PCAP Trace', 'Download Sample', 'Download Behavior Log', 'Download Matched YARA Rules' (highlighted with a red box), 'Generate IVP', 'Add to Whitelist', and 'Report False Positive'.

The main configuration area for a YARA rule is shown below. It includes a 'File Type' list with 'exe' selected, a 'Choose Yara File:' section with a 'Choose File' button and 'No file chosen' text, a 'Description:' field containing 'HealthCheck Sample', and an 'Enabled:' section with 'Enabled' selected. A 'Save' button is visible. Below the configuration area, a 'Current YARA Rules' table is displayed:

File Suffix	Description
exe : healthcheck_sample_yara.txt	HealthCheck Sample

A 'Cancel' button is located at the bottom right of the configuration area.

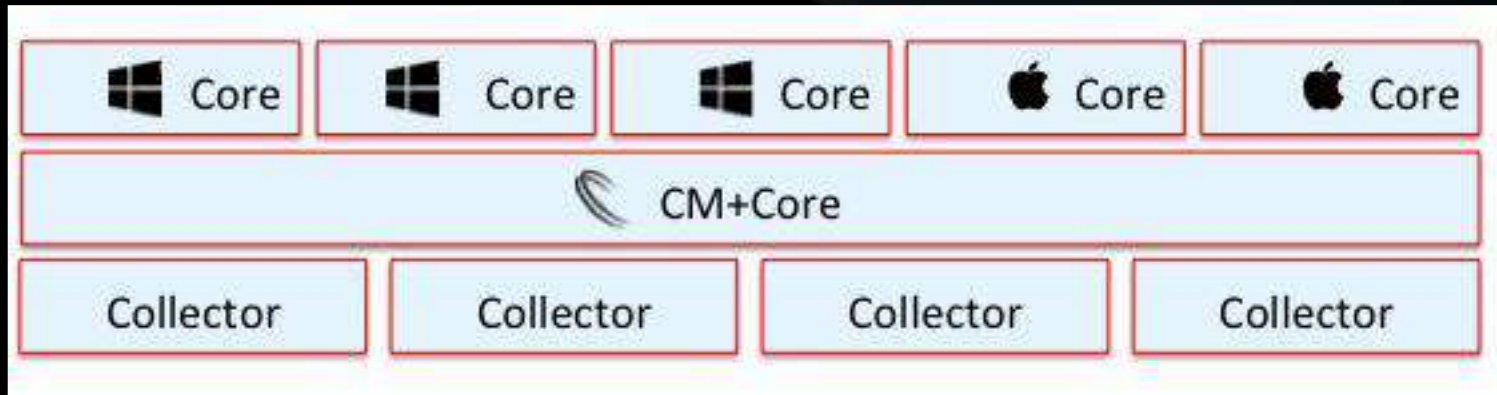
Собственный «Золотой образ» виртуальной машины

The screenshot displays the configuration page for 'Golden Image VMs' in the Juniper ATPA interface. The top navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The left sidebar lists various system settings such as 'Password Reset', 'Roles', 'Zones', 'Users', 'SAML Settings', 'RADIUS Settings', 'System Settings', 'Certificate Management', 'GSS Settings', 'Web Collectors', 'SRX Settings', 'Email Collectors', 'Secondary Cores', and 'Golden Image VMs'. The main content area contains several input fields: 'Image Name', 'Description', 'VNC ID', 'Architecture' (with radio buttons for 32-bit and 64-bit), 'Disk Size (GB)' (set to 20), 'Risk Reduction' (with radio buttons for Yes and No), and 'Network Segment' (set to default). A 'Cancel' button is visible at the bottom right of the configuration area. Below the configuration fields, there is a section titled 'Current VM Images' with a table containing columns for 'Description', 'Enabled', and 'Status'.

«Золотой» – Ваш собственный образ с требуемым Вам ПО и его версиями. JATP будет использовать использовал его при детонации образов 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



A photograph of a server room with rows of server racks on both sides and a central door. The room is lit with a cool blue light. A dark semi-transparent rectangle is overlaid on the left side of the image, containing the text 'Форм-фактор' in white.

Форм-фактор

Апплайнсы физические и виртуальные

JATP 400

- 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

JATP 700

- 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

vJATP Core, Mail & Web vCollector

- 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

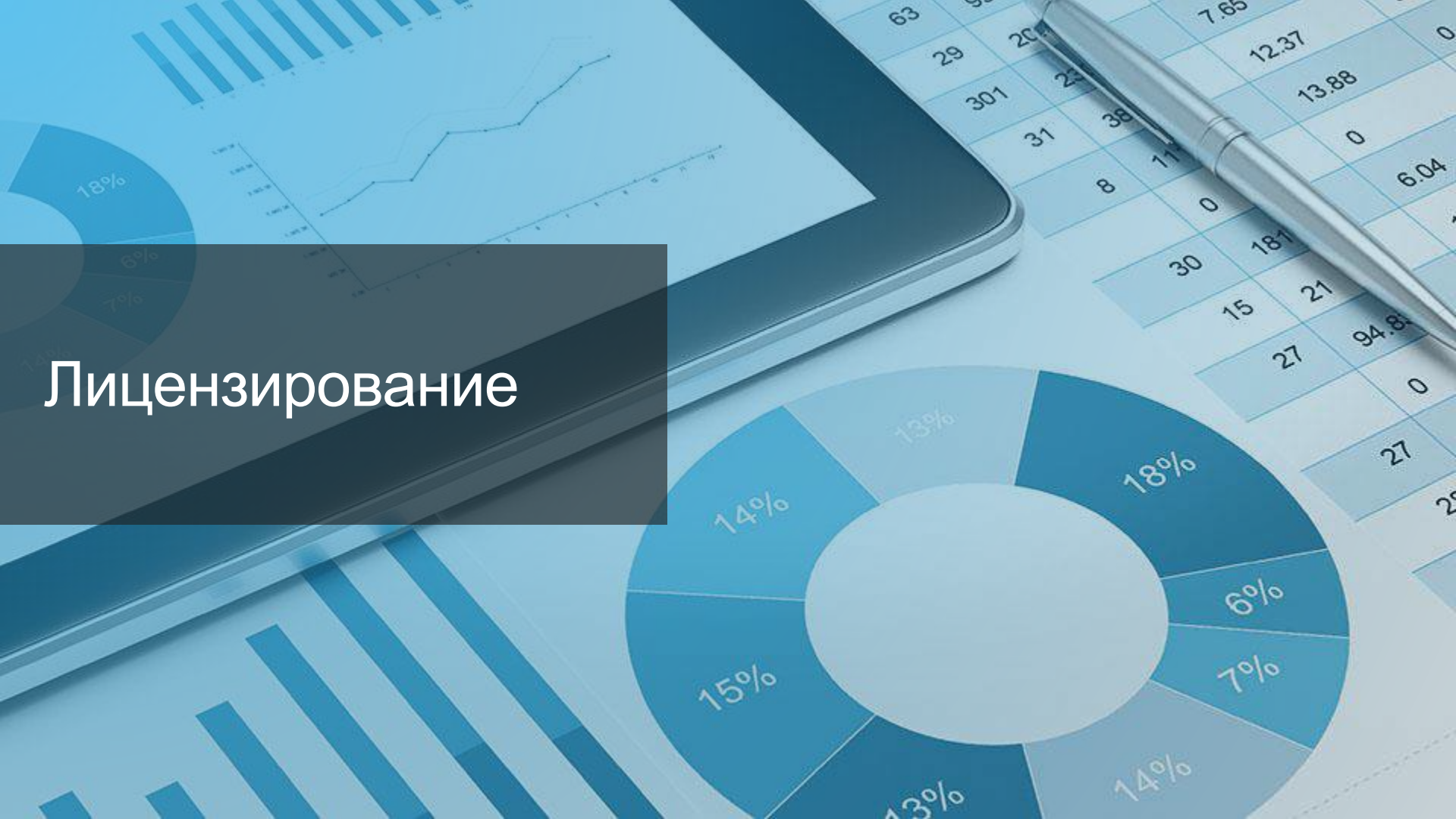
Virtual Web Collector

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



СПАСИБО!

JUNIPER
NETWORKS

Engineering
Simplicity



Наш канал на Youtube