

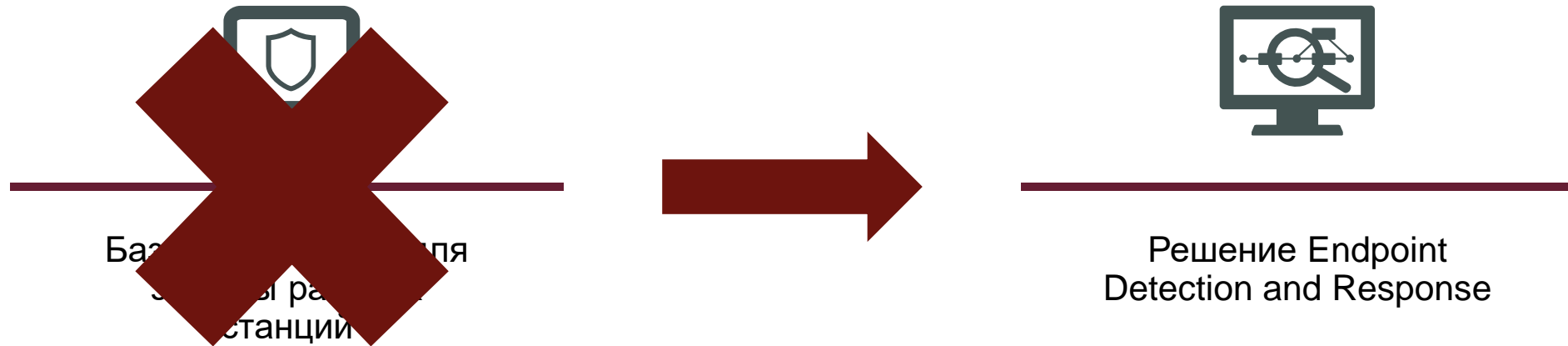


FortiEDR: инструмент автоматизации обнаружения и устранения атак на конечные узлы сети

Кирилл Михайлов, Fortinet

Необходимость EDR

EDR замена EPP?



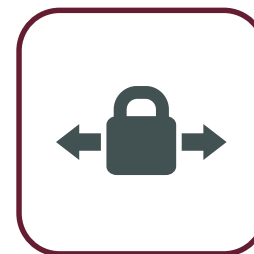
Функционал EPP



Базовое решение для
защиты рабочих
станций



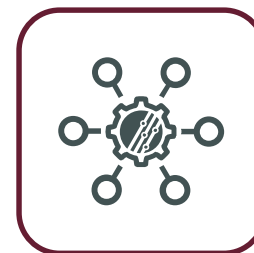
Антивирусный модуль



Модуль VPN



Модуль Compliance



Модуль интеграции со
сторонними системами

Функционал EDR



Решение Endpoint
Detection and Response



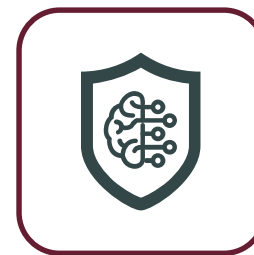
Антивирусный модуль



Модуль анализа
активности



Модуль реагирования и
восстановления
системы



Модуль анализа и
закрытия уязвимостей

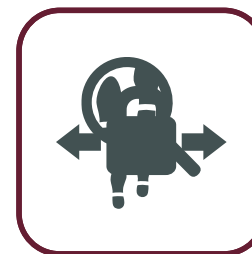
EDR – замена EPP?



Базовый EDR для
Detection and Response
станций



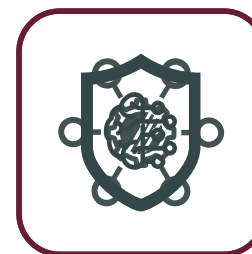
Антивирусный модуль



Модуль анализа
активности

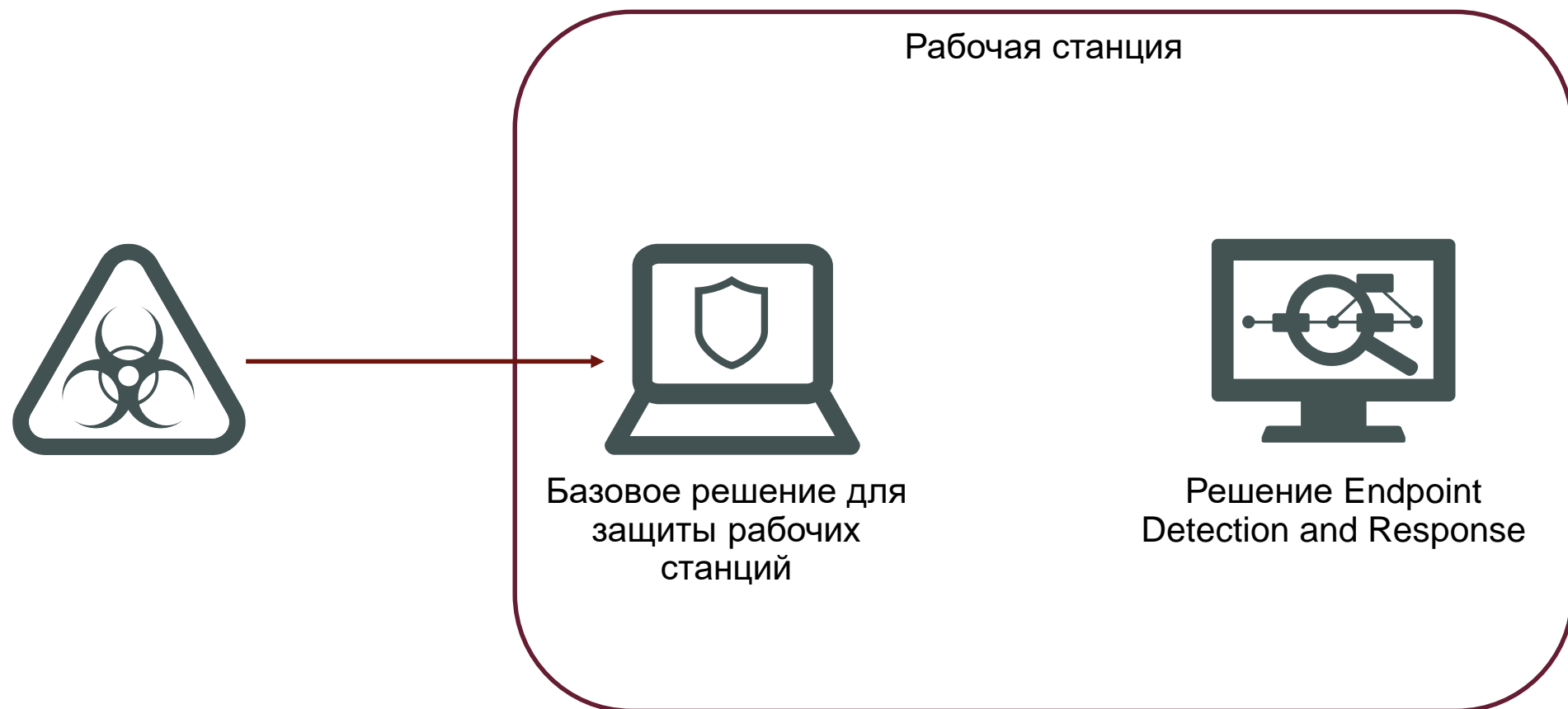


Модуль сопротивления и
восстановления
системы



Модуль хранения и
защиты информации

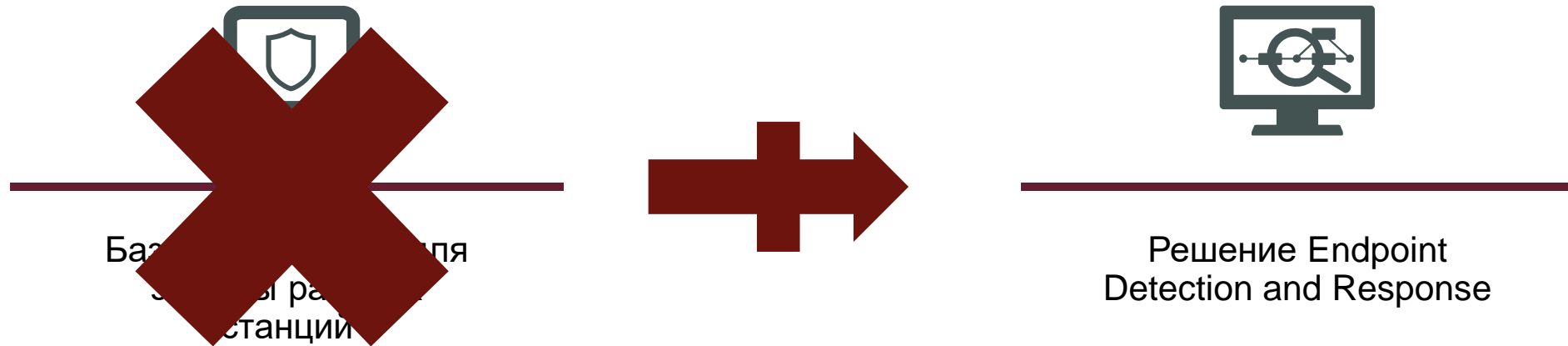
EDR: защита от известных угроз



EDR: обнаружение угроз

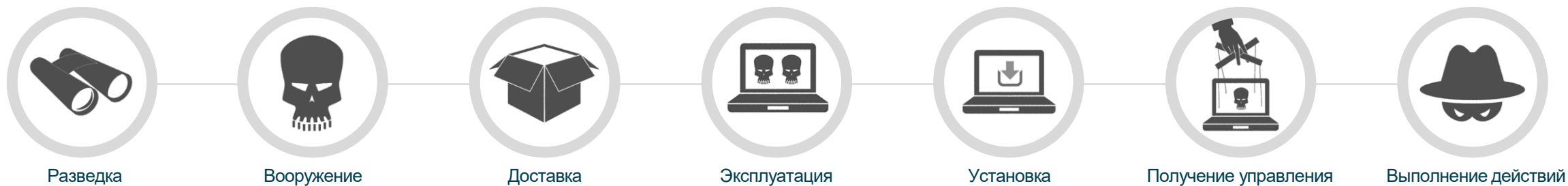


EDR замена EPP?



Автоматизация EDR

Снижение вреда от атаки



FortiEDR vs. неавтоматизированный EDR



Схема работы FortiEDR

Защита: pre-infection

Защита: post-infection

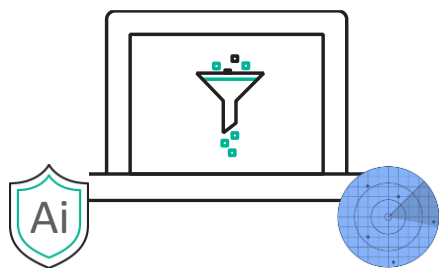
Реагирование

Префилترация

Запись

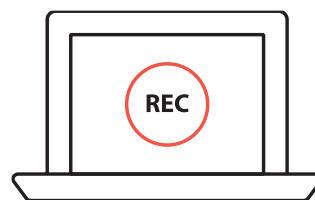
Сбор данных

Центральный компонент

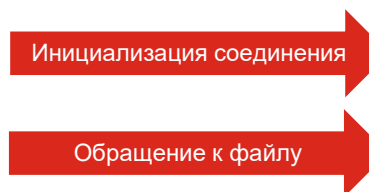


Шаг 1:
Коллектор блокирует известные угрозы

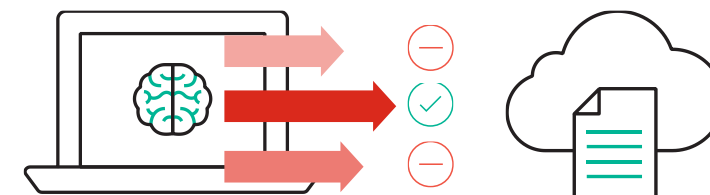
Шаг 2:
Коллектор реагирует на угрозы в соответствии с заранее заданными политиками



Шаг 3:
Коллектор собирает метаданные ОС



Шаг 4:
Коллектор передает снимок запроса и метаданные ОС центральному компоненту



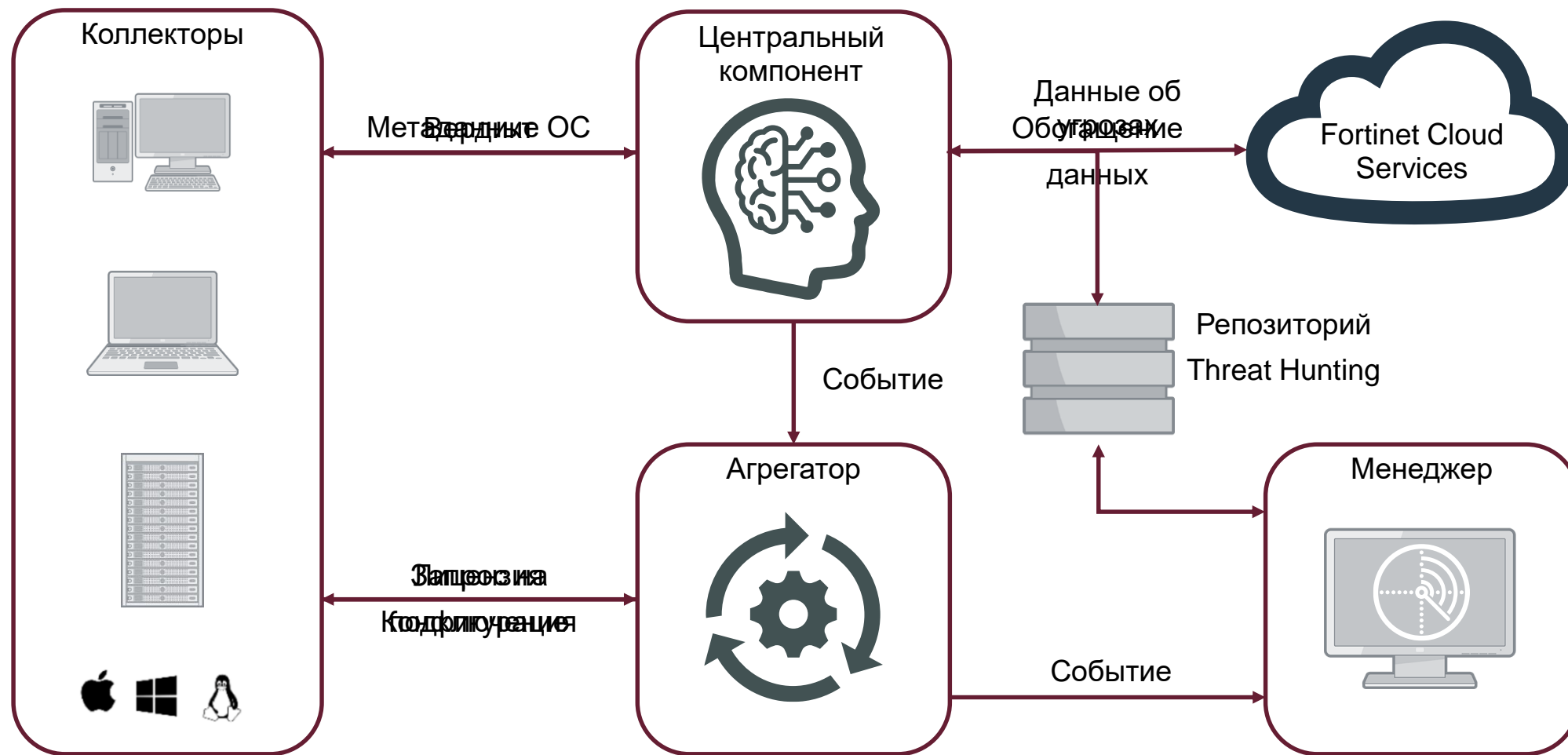
Шаг 5:
Центральный компонент анализирует данные, полученные от коллектора

Шаг 6:
Центральный компонент запускает плейбук для реагирования на обнаруженную нелегитимную активность

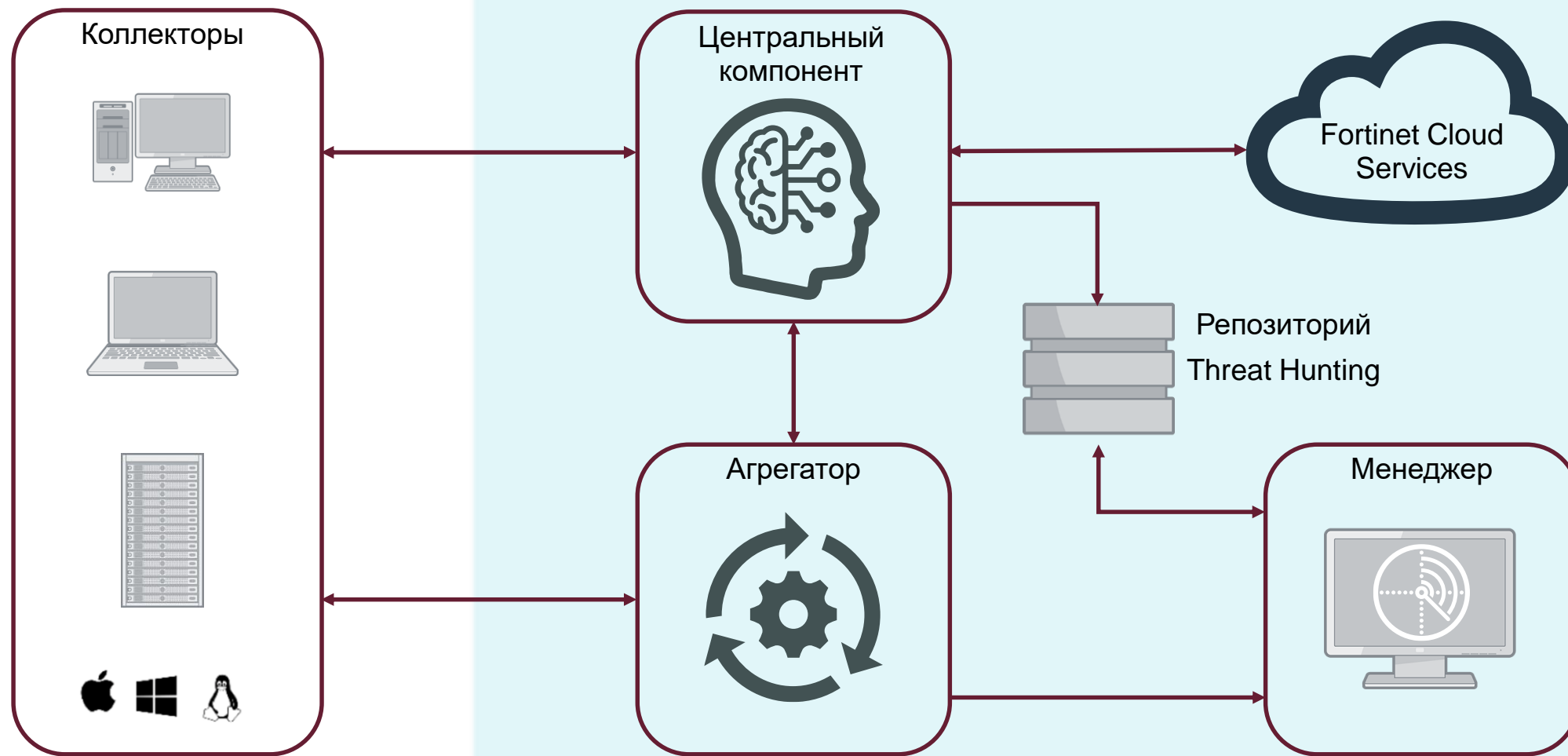
FortiEDR

Архитектура

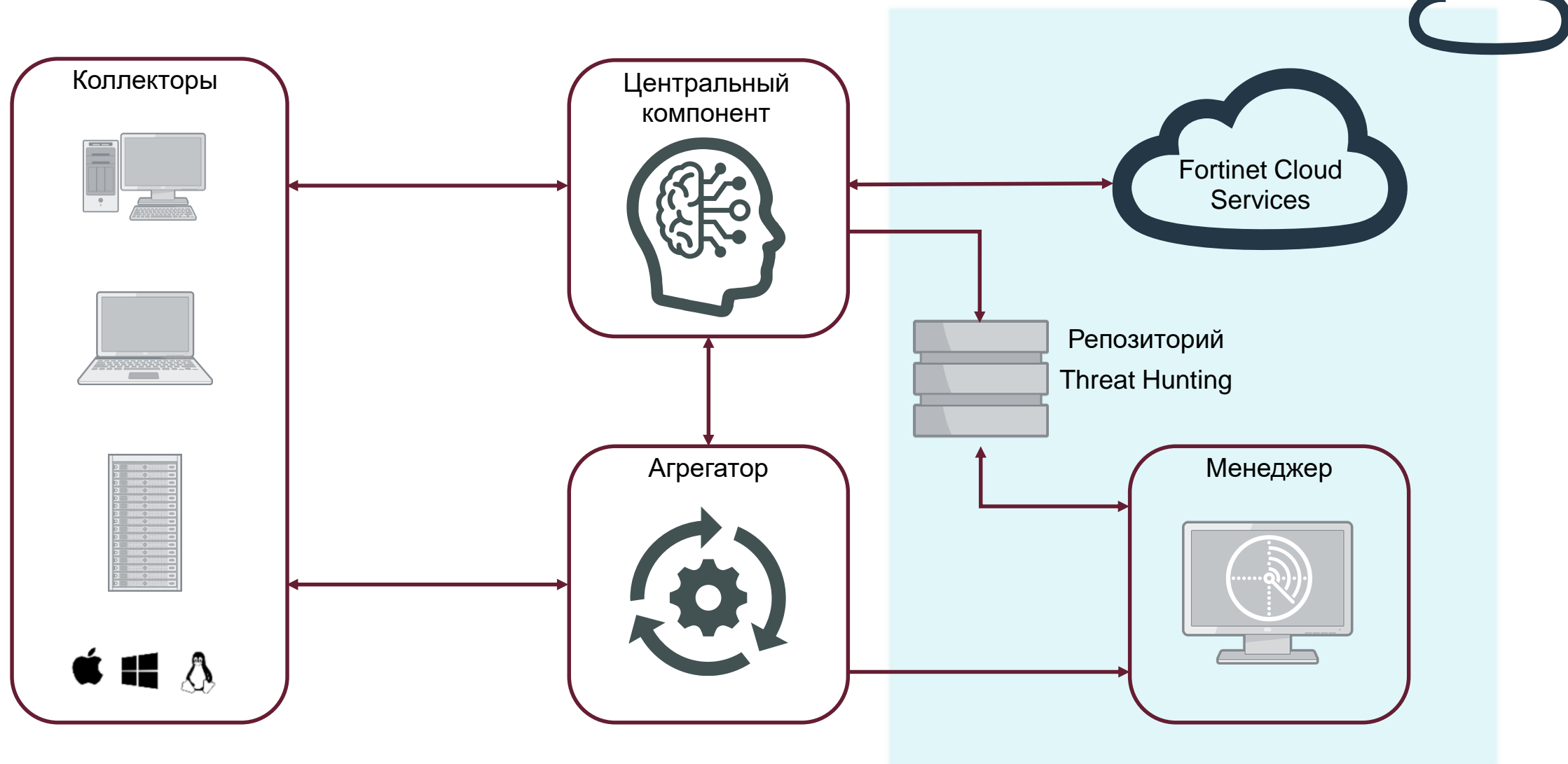
FortiEDR: компоненты



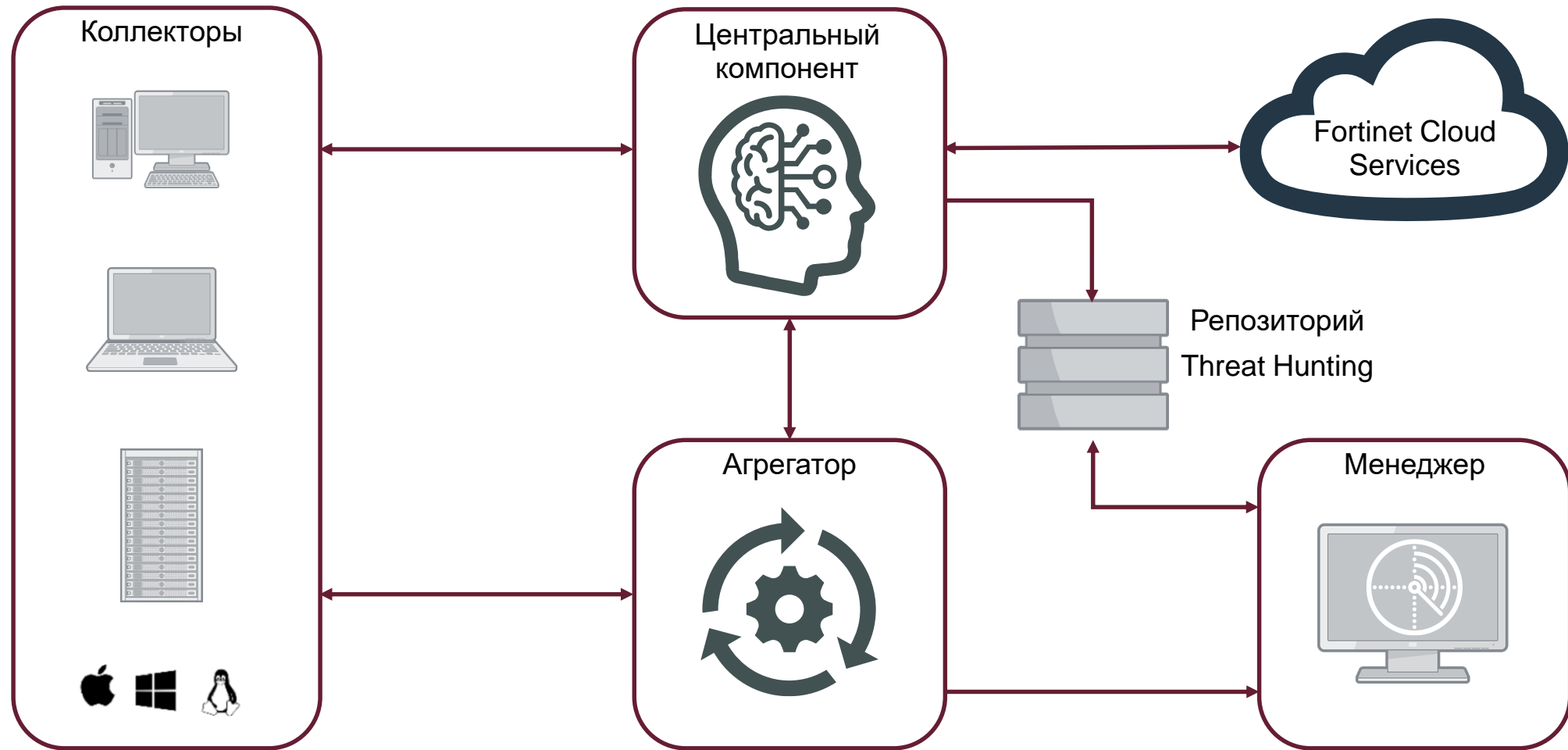
FortiEDR: варианты развертывания: облако



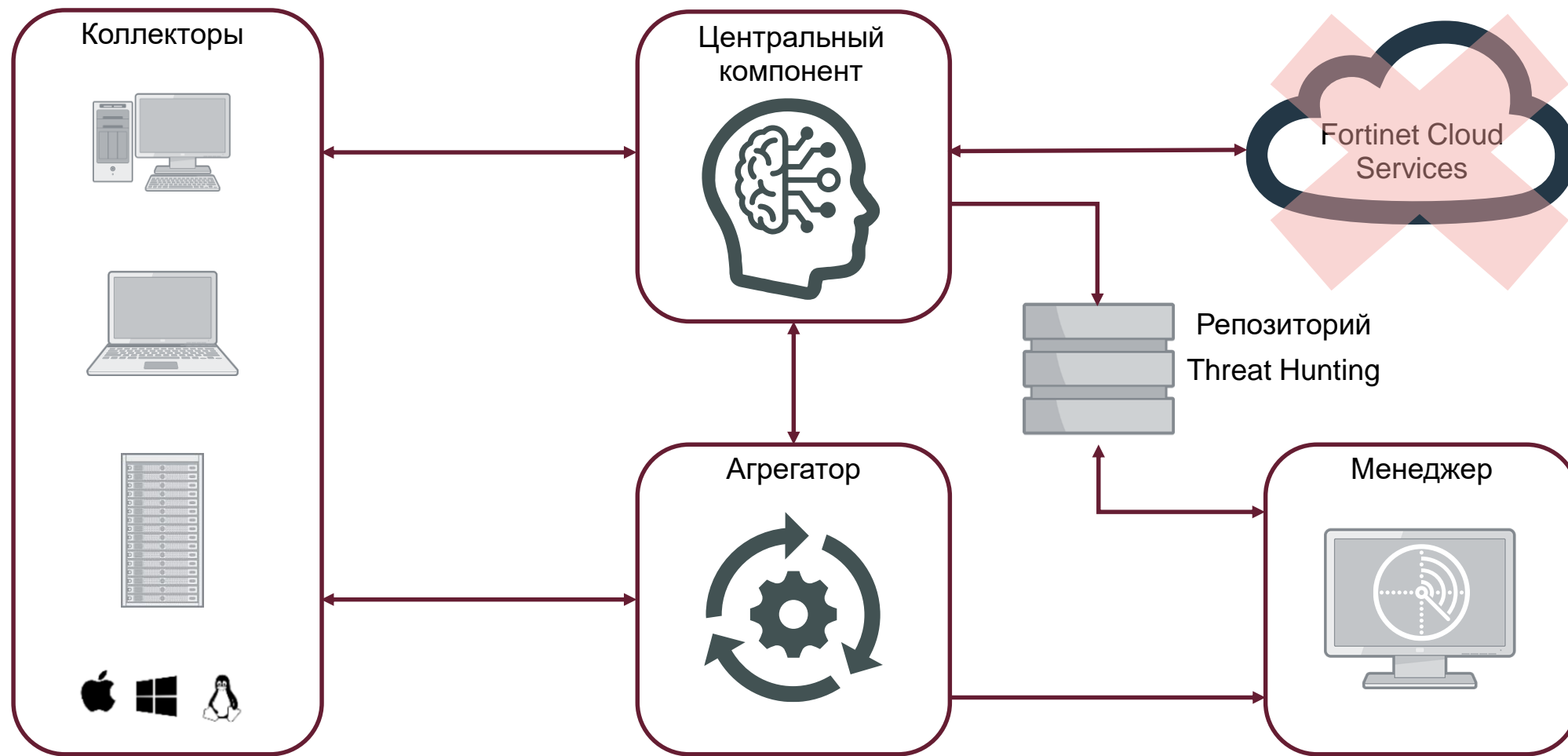
FortiEDR: варианты развертывания: гибрид



FortiEDR: варианты развертывания: локальный



FortiEDR: варианты развертывания: offline



FortiEDR: требования к системе (10к коллекторов)

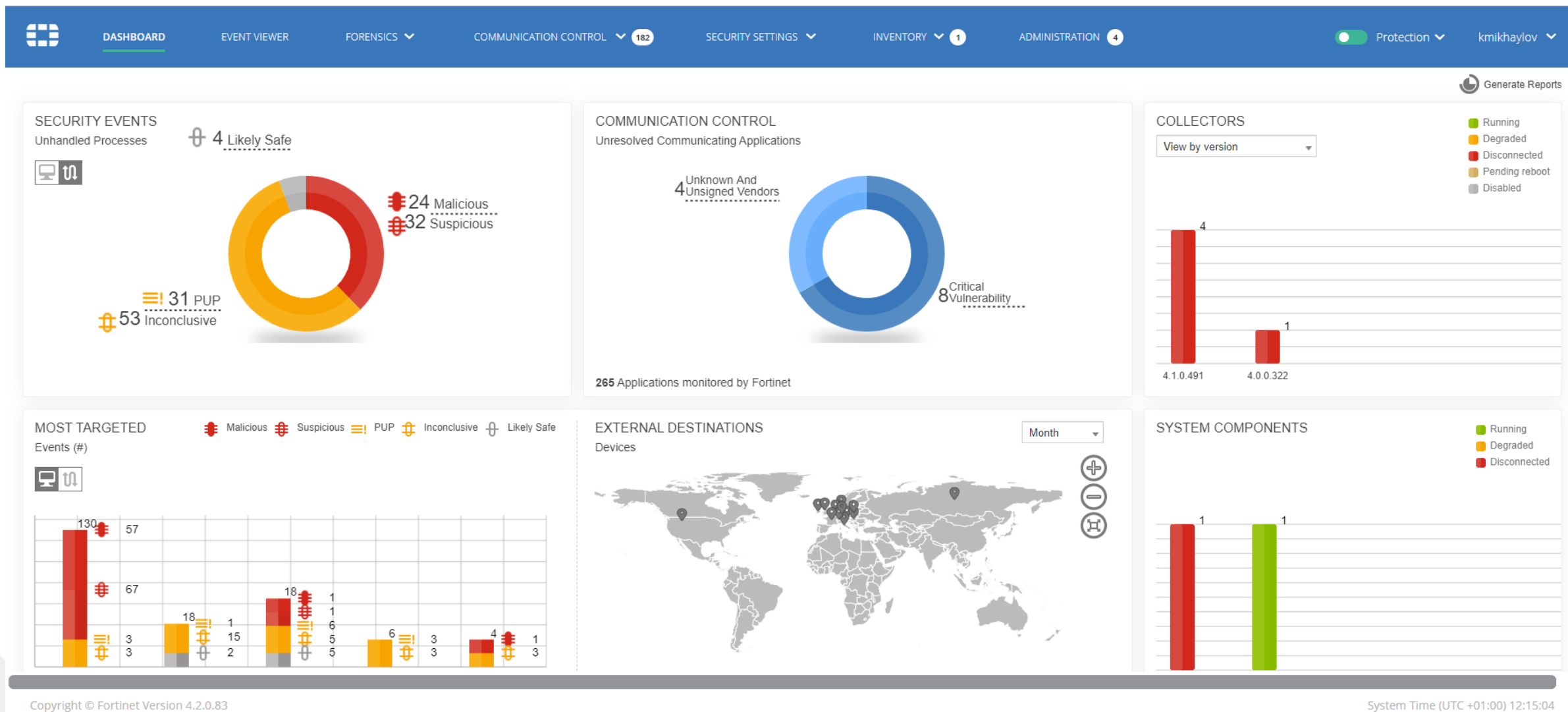
| Компонент | Поддерживаемая платформа | Требования |
|------------------------------|--------------------------|--|
| Коллектор | Windows, MacOS, Linux | < 1% cpu; 60MB memory; 20MB Disk usage |
| Центральный компонент (Core) | VM/Bare metal | 2 CPUs; 8GB RAM; 60GB* Disk size |
| Агрегатор | | 2 CPUs; 16GB RAM; 80GB* Disk size |
| Менеджер | | 2 CPUs; 16GB RAM; 150GB* Disk size |
| Репозиторий Threat Hunting | | 4 CPUs; 16GB* RAM 200GB* Disk size and up |
| Требования к каналу связи | 10000 коллекторов | ~ 50 Mbps |

* как минимум

FortiEDR

Функциональные возможности и управление

FortiEDR: главный экран



FortiEDR: политики безопасности

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL

13

SECURITY SETTINGS

INVENTORY

ADMINISTRATION

6

Simulation

kirill

SECURITY POLICIES

Clone Policy

Set Mode

Assign Collector Group

Exception Manager

Delete

All

| POLICY NAME | RULE NAME | ACTION | STATE |
|--|--|--------|---------|
| <div><div></div><div>IRansomware Prevention</div><div></div></div> | Debugged Process - Connection from a Debugged Process | Log | Enabled |
| | Dynamic Code - Malicious Runtime Generated Code Detected | Block | Enabled |
| | Executable Format - Bad Executable File Format | Block | Enabled |
| | Executable Stack - A Stack with Executable Code | Block | Enabled |
| | Executed Program has no installer | Block | Enabled |
| | Fake Critical Program - Program Attempted to Hide as a Service | Block | Enabled |
| | Fake Packer - A Fake Known Packer Detected | Block | Enabled |
| | File Encoder - Suspicious file modification | Block | Enabled |

Assigned Collector Groups

Unassign Group

test (1 collector included)

ADVANCED POLICY & RULE DATA

Rule Details

RULE NAME: Fake Critical Program - Program Attempted to Hide as a Service

RULE DETAILS

Many malware try to hide by looking like a critical system process, such as a service. This alert is a very strong indicator of malicious activity as it is rare for a legitimate software to do this.

FORENSICS RECOMMENDATIONS

Retrieve the executable file from the targeted device according to its Path by using the Forensics Tab in order to perform deeper analysis.

Copyright © Fortinet Version 4.1.0.78

System Time (UTC +02:00) 15:56:56

FORTINET

© Fortinet Inc. All Rights Reserved.

23

FortiEDR: автоматизация реагирования

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL

13

SECURITY SETTINGS

INVENTORY

ADMINISTRATION

6

Simulation

kirill

AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

Clone Playbook

Set Mode

Assign Collector Group

Delete

| | | | MALICIOUS | SUSPICIOUS | PUP | INCONCLUSIVE | LIKELY SAFE |
|---|--------------------------|--|--|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | NAME | | | | | | |
| <input type="checkbox"/> | Default Playbook | <div><div></div><div>Fortinet</div><div></div></div> | | | | | |
| <input checked="" type="checkbox"/> | my_playbook | <div><div></div><div></div><div></div></div> | | | | | |
| NOTIFICATIONS (sent in protection and simulation modes) | | | | | | | |
| | Send mail notification | | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Send syslog notification | | Syslog must be defined. Please contact Administrator. | | | | |
| | Open ticket | | Open ticket must be defined. Please contact Administrator. | | | | |
| INVESTIGATION | | | | | | | |
| | Isolate device | | ✓ | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

ASSIGNED COLLECTOR GROUPS

Unassign Group

☐ test (1 collector included)

ADVANCED PLAYBOOKS DATA

ACTION NAME: Isolate device

ACTION DETAILS

This option enables you to isolate a device and prevent its application and process from communicating externally, based on an event-specific classification. The definition that specifies which application can and cannot communicate is defined using the Communication Control Manager. This mechanism enables you to define which application should be allowed to communicate for debug or other purposes. This feature is supported by Collectors 3.1 and up.

Copyright © Fortinet Version 4.1.0.78

System Time (UTC +02:00) 15:58:42

FortiEDR: события

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL

13

SECURITY SETTINGS

INVENTORY

ADMINISTRATION

6

Simulation

kirill

EVENTS

Showing 1-4/4

Multiple search

Archive

Mark As

Export

Handle Event

Delete

Forensics

Exception Manager

| | Unhandled | ID | DEVICE | PROCESS | CLASSIFICATION | DESTINATIONS | RECEIVED | LAST UPDATED |
|--------------------------|-----------|----------------|-------------|---------|----------------|--------------|-----------------------|--------------|
| <input type="checkbox"/> | | report.pdf.exe | (10 events) | | Malicious | | 01-Apr-2020, 13:22:26 | |
| <input type="checkbox"/> | | cscript.exe | (3 events) | | Malicious | | 01-Apr-2020, 13:16:49 | |
| <input type="checkbox"/> | | dkINTpuA.dll | (1 event) | | Malicious | | 01-Apr-2020, 13:05:37 | |
| <input type="checkbox"/> | | rundll32.exe | (3 events) | | Malicious | | 25-Mar-2020, 10:59:45 | |

CLASSIFICATION DETAILS

History

▶ ADVANCED DATA

FortiEDR: события

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL

SECURITY SETTINGS

INVENTORY

ADMINISTRATION

Simulation

kill

EVENTS

Showing 1-4/4

Multiple search

Archive

Mark As

Export

Handle Event

Delete

Forensics

Exception Manager

| | Unhandled | ID | DEVICE | PROCESS | CLASSIFICATION | DESTINATIONS | RECEIVED | LAST UPDATED |
|--|-----------|----------------------------|-----------------|---------|----------------|---------------|-----------------------|-----------------------|
| <input type="checkbox"/> | | report.pdf.exe (10 events) | | | Malicious | | 01-Apr-2020, 13:22:26 | |
| <input type="checkbox"/> | | cscript.exe (3 events) | | | Malicious | | 01-Apr-2020, 13:16:49 | |
| <input type="checkbox"/> | | 428807 | DESKTOP-CLLEKQ2 | 3.vbs | Malicious | 192.168.163.4 | 01-Apr-2020, 13:16:49 | 01-Apr-2020, 13:16:49 |
| User: DESKTOP-CLLEKQ2\kmikhaylov Certificate: Signed Process path: C:\Windows\System32\cscript.exe Raw data items: 1 | | | | | | | | |
| <input type="checkbox"/> | | 428768 | DESKTOP-CLLEKQ2 | 2.vbs | Malicious | 192.168.163.4 | 01-Apr-2020, 13:16:44 | 01-Apr-2020, 13:16:44 |
| <input type="checkbox"/> | | 428730 | DESKTOP-CLLEKQ2 | 1.vbs | Malicious | 192.168.163.4 | 01-Apr-2020, 13:16:36 | 01-Apr-2020, 13:16:36 |
| <input type="checkbox"/> | | dkINTpuA.dll (1 event) | | | Malicious | | 01-Apr-2020, 13:05:37 | |
| <input type="checkbox"/> | | rundll32.exe (3 events) | | | Malicious | | 25-Mar-2020, 10:59:45 | |

CLASSIFICATION DETAILS

Threat name: Unknown

Threat family: Unknown

Threat type: Unknown

History

Malicious, by FortinetCloudServices , on 01-Apr-2020, 13:16:55

Simulation

Process ...oads\report.pdf.exe\ with PID 4348 was terminated at device DESKTOP-CLLEKQ2 once

Simulation

Device DESKTOP-CLLEKQ2 was isolated once

Triggered Rules

IExfiltration Prevention

Suspicious Application - Connection Attempt from a Suspiciou...

Unmapped Executable - Executable File Without a Correspon...

ADVANCED DATA

Copyright © Fortinet Version 4.1.0.78

System Time (UTC +02:00) 14:28:11

FORTINET

© Fortinet Inc. All Rights Reserved.

26

FortiEDR: события

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL

SECURITY SETTINGS

INVENTORY

ADMINISTRATION

Simulation

kill

EVENTS

Archive Mark As

Unhandled ID

report.pdf.exe (10 events)

cscript.exe (3 events)

dkINTpuA.dll (1 event)

rundll32.exe (3 events)

Suspicious Application - Connection Attempt from a Suspiciou...

Some applications do not initiate connections to the network on their own, but are still commonly used by threat-actors to ex-filtrate data from the network. Communication from such applications is blocked by default.

MITRE Techniques:

- T1064 - Scripting
- T1086 - PowerShell
- T1170 - Mshta
- T1047 - Windows Management Instrumentation
- T1121 - Regsvcs/Regasm
- T1117 - Regsvr32
- T1118 - InstallUtil
- T1191 - CMSTP

Unmapped Executable - Executable File Without a Correspon...

An executable running in memory does not have a corresponding file in the file system. Malware can therefore hide in process memory without being listed by the operating system. Commonly, this technique is used by both Advanced Persistent Threat (APT) and Volatile Persistent Threat (VPT). It may also be used by application installers or very aggressive application protectors, though this scenario is rare.

Go to the Forensics Tab. Get the Base Address and End Address, as specified in the relevant stack entry. Retrieve the memory from the targeted device according to these memory addresses by using the Forensics Tab and perform a deeper analysis.

Showing 1-4/4

Multiple search

CEIVED LAST UPDATED

01-Apr-2020, 13:22:26

01-Apr-2020, 13:16:49

01-Apr-2020, 13:16:49 01-Apr-2020, 13:16:49

32\cscript.exe Raw data items: 1

01-Apr-2020, 13:16:44 01-Apr-2020, 13:16:44

01-Apr-2020, 13:16:36 01-Apr-2020, 13:16:36

01-Apr-2020, 13:05:37

25-Mar-2020, 10:59:45

CLASSIFICATION DETAILS

Threat name: Unknown

Threat family: Unknown

Threat type: Unknown

History

Malicious, by FortinetCloudServices, on 01-Apr-2020, 13:16:55

- Simulation Process ...oads\report.pdf.exe with PID 4348 was terminated at device DESKTOP-CLLEKQ2 once
- Simulation Device DESKTOP-CLLEKQ2 was isolated once

Triggered Rules

IExfiltration Prevention

- Suspicious Application - Connection Attempt from a Suspiciou...
- Unmapped Executable - Executable File Without a Correspon...

ADVANCED

Copyright © Fortinet Version 4.1.0.78

System Time (UTC +02:00) 14:28:11

FORTINET

© Fortinet Inc. All Rights Reserved.

27

FortiEDR: анализ в песочнице

DASHBOARD

EVENT VIEWER 2

FORENSICS ▼

COMMUNICATION CONTROL ▼ 40

SECURITY SETTINGS ▼

INVENTORY ▼

ADMINISTRATION 65

Simulation ▼

kirill ▼

EVENTS

Archive

Mark As...

Export

Handle Event

Delete

Forensics

Exception Manager

☐

All

ID

DEVICE

PROCESS

CLASSIFICATION

DESTINATIONS

RECEIVED

LAST UPDATED

☐

updater_0520.exe (3 events)

Malicious

20-May-2020, 17:00:02

☐

☐

934599

DESKTOP-CLLEKQ2

updater_0520.exe

Malicious

Service Access

20-May-2020, 17:00:02

20-May-2020, 17:00:02

☐

☐

934583

DESKTOP-CLLEKQ2

updater_0520.exe

Suspicious

192.168.163.21

20-May-2020, 17:00:00

20-May-2020, 17:00:00

☐

☐

934567

DESKTOP-CLLEKQ2

updater_0520.exe

Malicious

20-May-2020, 16:59:52

20-May-2020, 17:00:00

☐

☐

Certificate: Unsigned

Process path: C:\Users\ipetrov\Downloads\updater_0520.exe

Raw data items: 2

☐

112.exe (1 event)

Malicious

20-May-2020, 16:24:54

☐

check.exe (2 events)

Malicious

20-May-2020, 16:19:45

☐

test_file.exe (2 events)

Malicious

20-May-2020, 16:19:45

☐

payload.exe (3 events)

Malicious

20-May-2020, 16:17:04

☐

1rans.exe (1 event)

Malicious

06-May-2020, 16:04:11

☐

hdtunepro.exe (1 event)

Malicious

06-May-2020, 15:34:29

☐

LittleCrypt.exe (1 event)

PUP

06-May-2020, 15:21:40

☐

locky.exe (2 events)

Malicious

06-May-2020, 15:14:56

☐

test.exe (3 events)

Malicious

15-Apr-2020, 16:02:12

☐

ssh (1 event)

Inconclusive

14-Apr-2020, 11:02:22

☐

end (3 events)

Inconclusive

14-Apr-2020, 11:02:22

ADVANCED DATA

CLASSIFICATION DETAILS

Threat name: Unknown

Threat family: Unknown

Threat type: Unknown

History

Malicious, by FortinetCloudServices , on 20-May-2020, 17:08:38

Simulation

Process ...slupdater_0520.exe\ with PID 9223372036854775807 was terminated at device DESKTOP-CLLEKQ2 once

Simulation

Device DESKTOP-CLLEKQ2 was isolated once

Suspicious, by FortinetCloudServices , on 20-May-2020, 17:00:17

Triggered Rules

IExecution Prevention

Sandbox Analysis - File was sent to the sandbox for analysis

A suspicious file was sent to the sandbox for analysis and inspection. After the analysis completes, the file will either be classified as malicious, in which case its future executions will be blocked, or it will be classified as benign, in which case its execution will continue.

Check the event classification. If cloud classification was not set, sandbox

Copyright © Fortinet Version 4.1.1.110

System Time (UTC +02:00) 17:12:07

FORTINET

© Fortinet Inc. All Rights Reserved.

28

FortiEDR: анализ в песочнице

DASHBOARD

EVENT VIEWER 2

FORENSICS

COMMUNICATION CONTROL 40

SECURITY SETTINGS

INVENTORY

ADMINISTRATION 65

Simulation

kirill

EVENTS

Archive

Mark As...

Export

Handle Event

Delete

Forensics

Exception Manager

All

ID

DEVICE

PROCESS

CLASSIFICATION

DESTINATIONS

RECEIVED

LAST UPDATED

updater_0520.exe

History

Malicious, by FortinetCloudServices , on 20-May-2020, 17:08:38

Simulation Process ...slupdater_0520.exe\ with PID 9223372036854775807 was terminated at device DESKTOP-CLLEKQ2 once

Simulation Device DESKTOP-CLLEKQ2 was isolated once

112.exe (1 event)

check.exe

test_file.exe

payload.exe

1rans.exe

hdtunepro...

LittleCrypt...

locky.exe (2 events)

test.exe (3 events)

ssh (1 event)

...

20-May-2020, 17:00:02

20-May-2020, 17:00:02

20-May-2020, 17:00:02

20-May-2020, 17:00:00

20-May-2020, 16:59:52

20-May-2020, 16:24:54

20-May-2020, 16:19:45

20-May-2020, 16:19:45

20-May-2020, 16:17:04

06-May-2020, 16:04:11

06-May-2020, 15:34:29

06-May-2020, 15:21:40

06-May-2020, 15:14:56

15-Apr-2020, 16:02:12

14-Apr-2020, 11:02:22

14-Apr-2020, 11:02:22

Malicious

Malicious

Inconclusive

Inconclusive

ADVANCED DATA

CLASSIFICATION DETAILS

Threat name: Unknown

Threat family: Unknown

Threat type: Unknown

History

Malicious, by FortinetCloudServices , on 20-May-2020, 17:08:38

Simulation Process ...slupdater_0520.exe\ with PID 9223372036854775807 was terminated at device DESKTOP-CLLEKQ2 once

Simulation Device DESKTOP-CLLEKQ2 was isolated once

Suspicious, by FortinetCloudServices , on 20-May-2020, 17:00:17

Triggered Rules

Execution Prevention

Sandbox Analysis - File was sent to the sandbox for analysis

A suspicious file was sent to the sandbox for analysis and inspection. After the analysis completes, the file will either be classified as malicious, in which case its future executions will be blocked, or it will be classified as benign, in which case its execution will continue.

Check the event classification. If cloud classification was not set, sandbox

Copyright © Fortinet Version 4.1.1.110

System Time (UTC +02:00) 17:12:07

FORTINET

© Fortinet Inc. All Rights Reserved.

29

FortiEDR: работа с событиями

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL

SECURITY SETTINGS

INVENTORY

ADMINISTRATION

Simulation

kirill

EVENTS

Archive

Mark As...

Export

Handle Event

Delete

Forensics

Exception

| | Unhandled | ID | DEVICE | PROCESS | CLASSIFICATION |
|--|-----------|----------------------------|-----------------|---------|----------------|
| <input type="checkbox"/> | | report.pdf.exe (10 events) | | | Malicious |
| <input type="checkbox"/> | | cscript.exe (3 events) | | | Malicious |
| <input checked="" type="checkbox"/> | | 428807 | DESKTOP-CLLEKQ2 | 3.vbs | Malicious |
| ▶ User: DESKTOP-CLLEKQ2\kmikhaylov Certificate: Signed | | | | | |
| <input type="checkbox"/> | | 428768 | DESKTOP-CLLEKQ2 | 2.vbs | Malicious |
| <input type="checkbox"/> | | 428730 | DESKTOP-CLLEKQ2 | 1.vbs | Malicious |
| <input type="checkbox"/> | | dkINTpuA.dll (1 event) | | | Malicious |
| <input type="checkbox"/> | | rundll32.exe (3 events) | | | Malicious |

EVENT HANDLING

Unhandled event 428807 for process cscript.exe

Classification

Malicious

Type comment

Malicious **FORTINET**
PUP
Safe

☐ Archive When Handled

Advanced

☐ Mute Event Notifications (🔊) for 1 week

Save and Handled

Save

Cancel

CLASSIFICATION DETAILS

Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

Malicious, by FortinetCloudServices , on 01-Apr-2020, 13:16:55

- Simulation Process ...oads\report.pdf.exe\ with PID 4348 was terminated at device DESKTOP-CLLEKQ2 once
- Simulation Device DESKTOP-CLLEKQ2 was isolated once

Triggered Rules

▶ IExfiltration Prevention

▶ ADVANCED DATA

Copyright © Fortinet Version 4.1.0.78

System Time (UTC +02:00) 14:49:47

FortiEDR: расследование инцидентов

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL

13

SECURITY SETTINGS

INVENTORY

ADMINISTRATION

6

Simulation

kirill

EVENTS

Archive

Mark As...

Export

Handle Event

Delete

Forensics

Exception Manager

Showing 1-4/4

Multiple search

| | ID | DEVICE | PROCESS | CLASSIFICATION | DESTINATIONS | RECEIVED | LAST UPDATED |
|---|-------------------------|-----------------|----------------|----------------|---------------------|-----------------------|-----------------------|
| report.pdf.exe (11 events) | | | | Malicious | | 01-Apr-2020, 15:09:05 | 1-10/11 |
| <input type="checkbox"/> | 429955 | DESKTOP-CLLEKQ2 | report.pdf.exe | Malicious | 192.168.163.21 | 01-Apr-2020, 15:09:05 | 01-Apr-2020, 15:15:27 |
| <input type="checkbox"/> | 428920 | DESKTOP-CLLEKQ2 | report.pdf.exe | Malicious | Sensitive Inform... | 01-Apr-2020, 13:22:26 | 01-Apr-2020, 13:22:26 |
| <input type="checkbox"/> | 428782 | DESKTOP-CLLEKQ2 | report.pdf.exe | Malicious | File Delete Attempt | 01-Apr-2020, 13:16:44 | 01-Apr-2020, 13:16:44 |
| <input type="checkbox"/> | 428712 | DESKTOP-CLLEKQ2 | report.pdf.exe | Malicious | 3 destinations | 01-Apr-2020, 13:16:36 | 01-Apr-2020, 13:16:49 |
| <input type="checkbox"/> | 428432 | DESKTOP-CLLEKQ2 | report.pdf.exe | Malicious | File Delete Attempt | 01-Apr-2020, 13:05:39 | 01-Apr-2020, 13:05:39 |
| <input type="checkbox"/> | 428381 | DESKTOP-CLLEKQ2 | report.pdf.exe | Malicious | 2 destinations | 01-Apr-2020, 13:05:37 | 01-Apr-2020, 13:05:38 |
| <input checked="" type="checkbox"/> | 428333 | DESKTOP-CLLEKQ2 | report.pdf.exe | Malicious | Modify OS Settings | 01-Apr-2020, 13:05:33 | 01-Apr-2020, 13:05:33 |
| User: DESKTOP-CLLEKQ2\kmikhaylov Certificate: Unsigned Process path: C:\Users\kmikhaylov\Downloads\report.pdf.exe Raw data items: 1 | | | | | | | |
| <input type="checkbox"/> | 428352 | DESKTOP-CLLEKQ2 | report.pdf.exe | Malicious | File Creation | 25-Mar-2020, 10:51:38 | 01-Apr-2020, 13:05:33 |
| <input type="checkbox"/> | 428256 | DESKTOP-CLLEKQ2 | report.pdf.exe | Malicious | Service Access | 25-Mar-2020, 10:28:15 | 01-Apr-2020, 13:01:39 |
| <input type="checkbox"/> | 428241 | DESKTOP-CLLEKQ2 | report.pdf.exe | Malicious | 192.168.163.21 | 25-Mar-2020, 10:28:13 | 01-Apr-2020, 13:01:38 |
| cscript.exe (3 events) | | | | | | | |
| <input type="checkbox"/> | dkINTpuA.dll (1 event) | | | Malicious | | 01-Apr-2020, 13:05:37 | |
| <input type="checkbox"/> | rundll32.exe (3 events) | | | Malicious | | 25-Mar-2020, 10:59:45 | |

CLASSIFICATION DETAILS

Malicious

By ReversingLabs

Threat name: Unknown

Threat family: Unknown

Threat type: Unknown

History

Malicious, by FortinetCloudServices , on 01-Apr-2020, 13:05:45

Simulation Process ...oads\report.pdf.exe\ with PID 4348 was terminated at device DESKTOP-CLLEKQ2 once

Simulation Device DESKTOP-CLLEKQ2 was isolated once

Triggered Rules

Invalid Checksum - Connection Attempt from Application with I...

Unconfirmed Executable - Executable File Failed Verification T...

Unmapped Executable - Executable File Without a Correspon...

ADVANCED DATA

Copyright © Fortinet Version 4.1.0.78

System Time (UTC +02:00) 15:15:38

FORTINET

© Fortinet Inc. All Rights Reserved.

33

FortiEDR: расследование инцидентов

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL 13

SECURITY SETTINGS

INVENTORY

ADMINISTRATION 6

Simulation

kill

Clear All

Event 428333
report.pdf.exe

Add Exception

Retrieve

Remediate

Isolate

Export

Raw Data Items: All

Selected 1/1

| DEVICE | OS | PROCESS | CLASSIFICATION | DESTINATION | RECEIVED | LAST SEEN |
|--------------------|-----------------------|-----------------------|--|----------------------------------|-----------------------|-----------------------|
| DESKTOP-CLLEKQ2 | Windows 10 Enterprise | report.pdf.exe | Malicious | Modify OS Settings | 01-Apr-2020, 13:05:33 | 01-Apr-2020, 13:05:33 |
| RAW ID: 1698076220 | Process Type: 64 bit | Certificate: Unsigned | Process Path: C:\Users\kmikhaylov\Downloads\report.pdf.exe | User: DESKTOP-CLLEKQ2\kmikhaylov | Count: 1 | |

Process winlogon.exe

1 Create

Process userinit.exe

2 Create

Process explorer.exe

3 Create

Process report.pdf.exe

4 Create Unconfirmed Executable

5 Open Unconfirmed Executable

6 Create Writable Code Unmapped Executable

7 Change Unconfirmed Executable

Block FORTINET

System configuration
Key: \REGISTRY\USER\1-5-21-5
40891490-233696972-510918550-
1000_CLASSES\CLSID\{0A29FF9E-7
F9C-4437-8B11-F424491E3931}\In
ProcServer02
Value: (default)

FortiEDR: расследование инцидентов

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL 13

SECURITY SETTINGS

INVENTORY

ADMINISTRATION 6

Simulation

kill

Clear All

Event 428333
report.pdf.exe

Add Exception

Retrieve

Remediate

Isolate

Export

Raw Data Items: All

Selected 1/1

| DEVICE | OS | PROCESS | CLASSIFICATION | DESTINATION | RECEIVED | LAST SEEN |
|--------------------|-----------------------|-----------------------|--|----------------------------------|-----------------------|-----------------------|
| DESKTOP-CLLEKQ2 | Windows 10 Enterprise | report.pdf.exe | Malicious | Modify OS Settings | 01-Apr-2020, 13:05:33 | 01-Apr-2020, 13:05:33 |
| RAW ID: 1698076220 | Process Type: 64 bit | Certificate: Unsigned | Process Path: C:\Users\kmikhaylov\Downloads\report.pdf.exe | User: DESKTOP-CLLEKQ2\kmikhaylov | Count: 1 | |

4 Create
Unconfirmed Executable
[more >](#)

6 Create
Writeable Code
Unmapped Executable

7 Change
Unconfirmed Executable
[more >](#)

Unconfirmed Executable
Invalid Checksum
Unmapped Executable

Block
FORTINET

System configuration
Key: \REGISTRY\USER\S-1-5-21-5
40891490-2836969672-510916650-
1000_CLASSES\CLSID\{0A29FF9E-7
F9C-4437-8B11-F424491E3931}\In
ProcServer32
Value: (default)

Process cmd.exe

Copyright © Fortinet Version 4.1.0.78

System Time (UTC +02:00) 15:18:47

FortiEDR: расследование инцидентов

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL 13

SECURITY SETTINGS

INVENTORY

ADMINISTRATION 6

Simulation

kirill

Event 428333
report.pdf.exe

Add Exception

Retrieve

Remediate

Isolate

Export

Raw Data Items: All

Selected 1/1

| DEVICE | OS | PROCESS | CLASSIFICATION | DESTINATION | RECEIVED | LAST SEEN | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|-----------------------|----------------|----------------|--------------------|-----------------------|----------------------------|--|----------------------|----------|-------------|-------------|--------------|-------------|------|---|----|----------|--|--|--|---------------------------|---|----|--------|---|----------------|----------------|---------------------------|------------------------|-----|----------|---|----------|----------|---------------------------|------------------------|-----|----------|---|----------|----------|----------------------------|---|----|--------|---|----------------|----------------|--------------------------|
| DESKTOP-CLLEKQ2 | Windows 10 Enterprise | report.pdf.exe | Malicious | Modify OS Settings | 01-Apr-2020, 13:05:33 | 01-Apr-2020, 13:05:33 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RAW ID: 1698076220 Process Type: 64 bit Certificate: Unsigned Process Path: C:\Users\kmikhaylov\Downloads\report.pdf.exe User: DESKTOP-CLLEKQ2\kmikhaylov Count: 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <div>PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION CREATE PROCESS OPEN PROCESS THREAD CREATION <u>SYSTEM CONFIGURATION</u></div> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <div><div>SYSTEM CONFIGURATION</div><div>Process ID: 4348 Company: Product: Process Hash (SHA-1): 208982E88ABA811BD5AA307A664ED55473B4D2BE</div><div>Source Process: ...skVolume3\Users\kmikhaylov\Downloads\report.pdf.exe Description: Comments: Process Owner: DESKTOP-CLLEKQ2\kmikhaylov</div><div>Target: ...D\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InProcServer32 Version: Command Line:</div><table><thead><tr><th>EXECUTABLE FILE NAME</th><th>WRITABLE</th><th>CERTIFICATE</th><th>REPETITIONS</th><th>BASE ADDRESS</th><th>END ADDRESS</th><th>HASH</th></tr></thead><tbody><tr><td>Main -IDevice\HarddiskVolume3\Users\kmikhaylov\Downloads\report.pdf.exe</td><td>No</td><td>Unsigned</td><td></td><td></td><td></td><td>208982E88ABA811BD5AA30...</td></tr><tr><td>\Device\HarddiskVolume3\Windows\System32\KernelBase.dll</td><td>No</td><td>Signed</td><td>2</td><td>0x7ff92c270000</td><td>0x7ff92c458000</td><td>3A0D965CED62D33A830A41...</td></tr><tr><td>Runtime Generated Code</td><td>Yes</td><td>Unsigned</td><td>2</td><td>0x510000</td><td>0x57d000</td><td>B64978FE52B04A841A7ADD...</td></tr><tr><td>Runtime Generated Code</td><td>Yes</td><td>Unsigned</td><td>3</td><td>0x4c0000</td><td>0x4fa000</td><td>27F027309612871D237AE17...</td></tr><tr><td>\Device\HarddiskVolume3\Windows\System32\kernel32.dll</td><td>No</td><td>Signed</td><td>1</td><td>0x7ff92cd80000</td><td>0x7ff92cd2d000</td><td>AD3E678DB0413EEDD9AAF...</td></tr></tbody></table></div> | | | | | | | | EXECUTABLE FILE NAME | WRITABLE | CERTIFICATE | REPETITIONS | BASE ADDRESS | END ADDRESS | HASH | Main -IDevice\HarddiskVolume3\Users\kmikhaylov\Downloads\report.pdf.exe | No | Unsigned | | | | 208982E88ABA811BD5AA30... | \Device\HarddiskVolume3\Windows\System32\KernelBase.dll | No | Signed | 2 | 0x7ff92c270000 | 0x7ff92c458000 | 3A0D965CED62D33A830A41... | Runtime Generated Code | Yes | Unsigned | 2 | 0x510000 | 0x57d000 | B64978FE52B04A841A7ADD... | Runtime Generated Code | Yes | Unsigned | 3 | 0x4c0000 | 0x4fa000 | 27F027309612871D237AE17... | \Device\HarddiskVolume3\Windows\System32\kernel32.dll | No | Signed | 1 | 0x7ff92cd80000 | 0x7ff92cd2d000 | AD3E678DB0413EEDD9AAF... |
| EXECUTABLE FILE NAME | WRITABLE | CERTIFICATE | REPETITIONS | BASE ADDRESS | END ADDRESS | HASH | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Main -IDevice\HarddiskVolume3\Users\kmikhaylov\Downloads\report.pdf.exe | No | Unsigned | | | | 208982E88ABA811BD5AA30... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| \Device\HarddiskVolume3\Windows\System32\KernelBase.dll | No | Signed | 2 | 0x7ff92c270000 | 0x7ff92c458000 | 3A0D965CED62D33A830A41... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Runtime Generated Code | Yes | Unsigned | 2 | 0x510000 | 0x57d000 | B64978FE52B04A841A7ADD... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Runtime Generated Code | Yes | Unsigned | 3 | 0x4c0000 | 0x4fa000 | 27F027309612871D237AE17... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| \Device\HarddiskVolume3\Windows\System32\kernel32.dll | No | Signed | 1 | 0x7ff92cd80000 | 0x7ff92cd2d000 | AD3E678DB0413EEDD9AAF... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Copyright © Fortinet Version 4.1.0.78 System Time (UTC +02:00) 15:22:30

FortiEDR: исключения

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL

13

SECURITY SETTINGS

INVENTORY

ADMINISTRATION

6

Simulation

kill

Event 428333
report.pdf.exe

Add Exception

Retrieve

Remediate

Isolate

Export

| DEVICE | OS | PROCESS |
|-------------------------|-----------------------|----------------------|
| DESKTOP-CLLEKQ2 | Windows 10 Enterprise | report.pdf.exe |
| RAW ID: 1698076220 | | Process Type: 64 bit |
| PARENT PROCESS CREATION | | |

SYSTEM CONFIGURATION

Process ID: 4348

Source Process: ...skVolume3\Users\kmikhaylov\Downloads\report.pdf.exe

Target: ...D\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InProcServer32

Version:

EXECUTABLE FILE NAME

Main -\Device\HarddiskVolume3\Users\kmikhaylov\Downloads\report.pdf.exe

\Device\HarddiskVolume3\Windows\System32\KernelBase.dll

Runtime Generated Code

Runtime Generated Code

\Device\HarddiskVolume3\Windows\System32\kernel32.dll

EXCEPTION CREATION

Unmapped Executable - Apply exception on:

Memory unique identifier: J/AnMJYShx0jeuF4EqJaypWEWok=

report.pdf.exe (Unsigned)

Current Path: \Users\kmikhaylov\Downloads

Any Path

Invalid Checksum - Apply exception on:

report.pdf.exe (Unsigned)

Current Path: \Users\kmikhaylov\Downloads

Any Path

Writeable Code - Apply exception on:

report.pdf.exe (Unsigned)

Current Path: \Users\kmikhaylov\Downloads

Any Path

Unconfirmed Executable - Apply exception on:

report.pdf.exe (Unsigned)

Current Path: \Users\kmikhaylov\Downloads

Any Path

Create Exception

Cancel

Raw Data Items: All

Selected

1/1

LAST SEEN

3:05:33

01-Apr-2020, 13:05:33

User: DESKTOP-CLLEKQ2\kmikhaylov

Count: 1

HEAD CREATION

SYSTEM CONFIGURATION

Process Hash (SHA-1): 208982E88ABA811BD5AA307A664ED55473B4D2BE

Process Owner: DESKTOP-CLLEKQ2\kmikhaylov

| ADDRESS | END ADDRESS | HASH |
|---------|---------------|----------------------------|
| | | 208982E88ABA811BD5AA30... |
| 00 | 0x7f92c458000 | 3A0D965CED62D33A830A41... |
| | 0x57d000 | B64978FE52B04A841A7ADD... |
| | 0x4fa000 | 27F027309612871D237AE17... |
| 00 | 0x7f92cd2d000 | AD3E678DB0413EEDD9AAF... |

Copyright © Fortinet Version 4.1.0.78

System Time (UTC +02:00) 15:26:54

FortiEDR: дамп памяти процесса

Event 428333
report.pdf.exe

Add Exception

Retrieve

Remediate

Isolate

Export

| DEVICE | OS | PROCESS |
|---|-----------------------|----------------|
| DESKTOP-CLLEKQ2 | Windows 10 Enterprise | report.pdf.exe |
| RAW ID: 1698076220 Process Type: 64 bit | | |
| PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PRO... | | |

SYSTEM CONFIGURATION

Process ID: 4348 Company: Product: Process Hash (SHA-1): 208982E88ABA811BD5AA307A664ED55473B4D2BE

Source Process: ...skVolume3\Users\kmikhaylov\Downloads\report.pdf.exe Description: Comments: Process Owner: DESKTOP-CLLEKQ2\kmikhaylov

Target: ...D\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InProcServer32 Version: Command Line:

| EXECUTABLE FILE NAME | WRITABLE | CERTIFICATE | REPETITIONS | BASE ADDRESS | END ADDRESS | HASH |
|---|----------|-------------|-------------|----------------|----------------|----------------------------|
| Main -IDevice\HarddiskVolume3\Users\kmikhaylov\Downloads\report.pdf.exe | No | Unsigned | | | | 208982E88ABA811BD5AA30... |
| \Device\HarddiskVolume3\Windows\System32\KernelBase.dll | No | Signed | 2 | 0x7ff92c270000 | 0x7ff92c458000 | 3A0D965CED62D33A830A41... |
| Runtime Generated Code | Yes | Unsigned | 2 | 0x510000 | 0x57d000 | B64978FE52B04A841A7ADD... |
| Runtime Generated Code | Yes | Unsigned | 3 | 0x4c0000 | 0x4fa000 | 27F027309612871D237AE17... |
| \Device\HarddiskVolume3\Windows\System32\kernel32.dll | No | Signed | 1 | 0x7ff92cc80000 | 0x7ff92cd2d000 | AD3E678DB0413EEDD9AAF... |

Copyright © Fortinet Version 4.1.0.78 System Time (UTC +02:00) 15:28:00

Clear All

Raw Data Items: All

Selected 1/1

LAST SEEN

3:05:33 01-Apr-2020, 13:05:33 User: DESKTOP-CLLEKQ2\kmikhaylov Count: 1

HEAD CREATION SYSTEM CONFIGURATION

MEMORY RETRIEVAL

EVENT 428333, DESKTOP-CLLEKQ2
report.pdf.exe

Retrieve memory of selected stack entries - 6 entries selected

Retrieve from:
✓ Memory ✓ Disk

Retrieve memory region from address: Hex value (0x..)

to address: Hex value (0x..)

Retrieve the entire process memory

Estimated Memory Retrieval file size: 5.2 MB

Retrieve Cancel

FortiEDR: ручное реагирование

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL

13

SECURITY SETTINGS

INVENTORY

ADMINISTRATION

6

Simulation

kill

Event 428333
report.pdf.exe

Add Exception

Retrieve

Remediate

Isolate

Export

| DEVICE | OS | PROCESS |
|-------------------------|-----------------------|----------------------|
| DESKTOP-CLLEKQ2 | Windows 10 Enterprise | report.pdf.exe |
| RAW ID: 1698076220 | | Process Type: 64 bit |
| PARENT PROCESS CREATION | | |

SYSTEM CONFIGURATION

Process ID: 4348

Source Process: ...skVolume3\Users\kmikhaylov\Downloads\report.pdf.exe

Target: ...D\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InProcServer32

Version:

EXECUTABLE FILE NAME

| WRIT | |
|---|-----|
| Main -IDevice\HarddiskVolume3\Users\kmikhaylov\Downloads\report.pdf.exe | No |
| \Device\HarddiskVolume3\Windows\System32\KernelBase.dll | No |
| Runtime Generated Code | Yes |
| Runtime Generated Code | Yes |
| \Device\HarddiskVolume3\Windows\System32\kernel32.dll | No |

REMEDiate DEVICE DESKTOP-CLLEKQ2

report.pdf.exe
EVENT 428333
PROCESS ID 4348

☐ Terminate process report.pdf.exe

☐ Remove 6 selected executable files

☐ Delete file at path c:\temp\abcd.exe

☒ Handle persistent data (registry) \REGISTRY\USER\S-1-5-21-540891490-28369...

☒ Remove key

☒ Modify registry value (Default)

☒ Remove value

☐ Update value data to (A key or value that do not exist will automatically be created)

From C:\Users\KMIKHA~1\AppData\Local\Temp\dklINTpu... (REG_SZ)

Type

Remediate

Cancel

Raw Data Items: All

Selected 1/1

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998

999

1000

1001

1002

1003

1004

1005

1006

1007

1008

1009

1010

1011

1012

1013

1014

1015

1016

1017

1018

1019

1020

1021

1022

1023

1024

1025

1026

1027

1028

1029

1030

1031

1032

1033

1034

1035

1036

1037

1038

1039

1040

1041

1042

1043

1044

1045

1046

1047

1048

1049

1050

1051

1052

1053

1054

1055

1056

1057

1058

1059

1060

1061

1062

1063

1064

1065

1066

1067

1068

1069

1070

1071

1072

1073

1074

1075

1076

1077

1078

1079

1080

1081

1082

1083

1084

1085

1086

1087

1088

1089

1090

1091

1092

1093

1094

1095

1096

1097

1098

1099

1100

1101

1102

1103

1104

1105

1106

1107

1108

1109

1110

1111

1112

1113

1114

1115

1116

1117

1118

1119

1120

1121

1122

1123

1124

1125

1126

1127

1128

1129

1130

1131

1132

1133

1134

1135

1136

1137

1138

1139

1140

1141

1142

1143

1144

1145

1146

1147

1148

1149

1150

1151

1152

1153

1154

1155

1156

1157

1158

1159

1160

1161

1162

1163

1164

1165

1166

1167

1168

1169

1170

1171

1172

1173

1174

1175

1176

1177

1178

1179

1180

1181

1182

1183

1184

1185

1186

1187

1188

1189

1190

1191

1192

1193

1194

1195

1196

1197

1198

1199

1200

1201

1202

1203

1204

1205

1206

1207

1208

1209

1210

1211

1212

1213

1214

1215

1216

1217

1218

1219

1220

1221

1222

1223

1224

1225

1226

1227

1228

1229

1230

1231

1232

1233

1234

1235

1236

1237

1238

1239

1240

1241

1242

1243

1244

1245

1246

1247

1248

1249

1250

1251

1252

1253

1254

1255

1256

1257

1258

1259

1260

1261

1262

1263

1264

1265

1266

1267

1268

1269

1270

1271

1272

1273

1274

1275

1276

1277

1278

1279

1280

1281

1282

1283

1284

1285

1286

1287

1288

1289

1290

1291

1292

1293

1294

1295

1296

1297

1298

1299

1300

1301

1302

1303

1304

1305

1306

1307

1308

1309

1310

1311

1312

1313

1314

1315

1316

1317

1318

1319

1320

1321

1322

1323

1324

1325

1326

1327

1328

1329

1330

1331

1332

1333

1334

1335

1336

1337

1338

1339

1340

1341

1342

1343

1344

1345

1346

1347

1348

1349

1350

1351

1352

1353

1354

1355

1356

1357

1358

1359

1360

1361

1362

1363

1364

1365

1366

1367

1368

1369

1370

1371

1372

1373

1374

1375

1376

1377

1378

1379

1380

1381

1382

1383

1384

1385

1386

1387

1388

1389

139

FortiEDR: просмотр событий

DASHBOARD
EVENT VIEWER
FORENSICS
COMMUNICATION CONTROL
SECURITY SETTINGS
INVENTORY
ADMINISTRATION

Simulation
kirill

Clear All

Event 428333
report.pdf.exe

Add Exception
Retrieve
Remediate
Isolate
Export

1/1

Raw Data Items: All

Selected

| DEVICE | OS | PROCESS | DESTINATION | RECEIVED | LAST SEEN |
|----------------|-----------------|----------------|---------------|-----------------------|-----------------------|
| DESKTOP-CLL... | Windows 10 E... | report.pdf.exe | Modify OS ... | 01-Apr-2020, 13:05:33 | 01-Apr-2020, 13:05:33 |

RAW ID: 1698076220 Process Type: 64 bit Certificate: Unsigned Process Path: ...nloads\report.pdf.exe User: ...KQ2\kmikhaylov Count: 1

CREATE PROCESS

Process ID: 4348
 Source Process: ...ds\report.pdf.exe
 Target: ...indows\System32\cmd.exe

Company:
 Description:
 Version:

Product:
 Comments:
 Command Line:

Process Hash (SHA-1): 208982E...
 Process Owner: DESKTOP-CLLE...

| EXECUTABLE FILE NAME | WRITABL... | CERTIFICA... | REPETITIO... | BASE ADDRE... | END ADDRES... |
|---|------------|--------------|--------------|----------------|----------------|
| Main - ...ikhaylov\Downloads\report.pdf.exe | No | Unsigned | | | |
| ...lume3\Windows\System32\KernelBase.dll | No | Signed | 3 | 0x7ff92c270000 | 0x7ff92c458000 |
| ...Volume3\Windows\System32\kernel32.dll | No | Signed | 1 | 0x7ff92cc80000 | 0x7ff92cd2d000 |
| Runtime Generated Code | Yes | Unsigned | 1 | 0x510000 | 0x57d000 |
| Runtime Generated Code | Yes | Unsigned | 1 | 0x4c0000 | 0x4fa000 |

Event 428333
report.pdf.exe

Add Exception
Retrieve
Remediate
Isolate
Export

1/1

Raw Data Items: All

Selected

| DEVICE | OS | PROCESS | DESTINATION | RECEIVED | LAST SEEN |
|----------------|-----------------|----------------|---------------|-----------------------|-----------------------|
| DESKTOP-CLL... | Windows 10 E... | report.pdf.exe | Modify OS ... | 01-Apr-2020, 13:05:33 | 01-Apr-2020, 13:05:33 |

RAW ID: 1698076220 Process Type: 64 bit Certificate: Unsigned Process Path: ...nloads\report.pdf.exe User: ...KQ2\kmikhaylov Count: 1

SYSTEM CONFIGURATION

Process ID: 4348
 Source Process: ...ds\report.pdf.exe
 Target: ...91E3931}\InProcServer32

Company:
 Description:
 Version:

Product:
 Comments:
 Command Line:

Process Hash (SHA-1): 208982E...
 Process Owner: DESKTOP-CLLE...

| EXECUTABLE FILE NAME | WRITABL... | CERTIFICA... | REPETITIO... | BASE ADDRES... | END ADDRES... |
|---|------------|--------------|--------------|----------------|----------------|
| Main - ...ikhaylov\Downloads\report.pdf.exe | No | Unsigned | | | |
| ...lume3\Windows\System32\KernelBase.dll | No | Signed | 2 | 0x7ff92c270000 | 0x7ff92c458000 |
| Runtime Generated Code | Yes | Unsigned | 2 | 0x510000 | 0x57d000 |
| Runtime Generated Code | Yes | Unsigned | 3 | 0x4c0000 | 0x4fa000 |
| ...Volume3\Windows\System32\kernel32.dll | No | Signed | 1 | 0x7ff92cc80000 | 0x7ff92cd2d000 |

Copyright © Fortinet Version 4.1.0.78
System Time (UTC +02:00) 15:32:55

FortiEDR: threat hunting

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL

13

SECURITY SETTINGS

INVENTORY

ADMINISTRATION

6

Simulation

kirill

Remediate

01

02

03

Hash

File Name

208982E88ABA811BD5AA307A664ED55473B4D2BE

Max

Last month

Last week

Last day

Custom

SEARCH

CLEAR

SHA-1: 208982E88ABA... BIT: 64 SIZE: 7168 IS SIGNED: No VENDOR: PRODUCT: VERSION:

1 DEVICES 3 PATHS 1 WEEKS

Showing 1-10/10

Copyright © Fortinet Version 4.1.0.78

System Time (UTC +02:00) 15:35:33

FortiEDR: контроль сетевых соединений

DASHBOARD

EVENT VIEWER 3

FORENSICS

COMMUNICATION CONTROL 40

SECURITY SETTINGS

INVENTORY

ADMINISTRATION 65

Simulation

kirill

APPLICATIONS

Showing 1-10/45

Search Application

All

Mark As...

Delete

Modify Action

Advanced Filter

Export

| APPLICATION | Signed | VENDOR | REPUTATION | VULNERABILITY | FIRST SEEN | LAST SEEN |
|---|--------|-----------------------|---|---------------|-------------|--------------|
| <input type="checkbox"/> Windows Explorer | Signed | Microsoft Corporation | <div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div> | Unknown | 03-Apr-2020 | 20-May-20... |
| <input type="checkbox"/> Search and Cortana application | Signed | Microsoft Corporation | <div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div> | Unknown | 03-Apr-2020 | 20-May-20... |
| <input type="checkbox"/> Background Task Host | Signed | Microsoft Corporation | <div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div> | Unknown | 03-Apr-2020 | 20-May-20... |
| <input checked="" type="checkbox"/> Microsoft OneDrive | Signed | Microsoft Corporation | <div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div> | Medium | 03-Apr-2020 | 20-May-20... |
| <input type="checkbox"/> 19.232.1124.0010 | | | <div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div> | Medium | 03-Apr-2020 | 13-May-20... |
| <input type="checkbox"/> 17.3.5892.0626 | | | <div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div> | Medium | 03-Apr-2020 | 06-Apr-2020 |
| <input type="checkbox"/> 19.232.1124.0012 | | | <div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div> | Medium | 28-Apr-2020 | 07-May-20... |
| <input type="checkbox"/> 20.052.0311.0011 | | | <div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div> | Medium | 13-May-2020 | 20-May-2020 |
| <input type="checkbox"/> Thunderbird | Signed | Mozilla Corporation | <div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div> | Critical | 03-Apr-2020 | 10-Apr-2020 |

VERSION DETAILS

Microsoft OneDrive, v. 20.052.0311.0011

Policies

| Policy | Action |
|-----------------------------------|---------------------------|
| Default Communication Control ... | Allow According to policy |
| Servers Policy | Allow According to policy |
| my_policy | Allow According to policy |
| Isolation Policy | Deny According to policy |

Vulnerabilities

Total 1 CVEs

CVE-2020-0935 - Medium (CVSS 3.0: 5.5, CVSS 2.0: 2.1)

ADVANCED DATA

APPLICATION INFO

Application Description: Microsoft OneDrive

First Connection Time: 13-May-2020, 16:47:12

Last Connection Time: 20-May-2020, 16:09:09

Process Names:
\\Device\\HarddiskVolume3\\Users\\ipetrov\\AppData\\Local\\Microsoft\\OneDriv...
\\Device\\HarddiskVolume3\\Users\\ipetrov\\AppData\\Local\\Microsoft\\OneDriv...
And 1 more...

APPLICATION USAGE

Total System: 27 connections / day

test 27 connections / day

More...

DESTINATIONS

| IP | CONNECTION TIME | COUNTRY |
|---------------|-----------------------|---------------|
| 40.90.137.120 | 20-May-2020, 16:07:36 | United States |
| 52.114.128.43 | 20-May-2020, 16:07:33 | United States |
| 2.21.109.198 | 20-May-2020, 16:07:33 | Austria |

More...

Copyright © Fortinet Version 4.1.1.110

System Time (UTC +02:00) 16:42:24

FORTINET

© Fortinet Inc. All Rights Reserved.

42

FortiEDR: обнаружение устройств

DASHBOARD

EVENT VIEWER 15

FORENSICS

COMMUNICATION CONTROL 125

SECURITY SETTINGS

INVENTORY 13

ADMINISTRATION 21

Simulation

kmikhaylov

COLLECTORS (7/7)

Search Devices or Groups

Unmanaged

Create Group

Move to Group

Delete

Enable/Disable

Isolate


Export

Uninstall

7 Unmanaged devices were found

| COLLECTOR GROUP NAME | DEVICE NAME | LAST LOGGED | OS | IP | MAC ADDRESS | VERSION | STATE | LAST SEEN |
|-------------------------|----------------------------------|-------------|------------|----------------|-------------------|---------|-----------|-----------|
| Unmanaged devices (7/7) | | | | | | | | |
| | VMware | | Windows | 192.168.7.2 | 4C-1D-96-49-78-CF | | Unmanaged | Today |
| | OpenVPN Web CA 2020.06.... | | Linux (VM) | 192.168.7.11 | 00-0C-29-71-05-B0 | | Unmanaged | Today |
| | dc.internal.net | | Windows | 192.168.7.12 | 00-0C-29-89-C9-1D | | Unmanaged | Today |
| | Default-Server-Certificate-91... | | Linux (VM) | 192.168.7.20 | 00-0C-29-4E-D5-74 | | Unmanaged | Today |
| | N/A | | Windows | 192.168.31.90 | 10-63-C8-50-FD-B3 | | Unmanaged | Today |
| | WIN-F3PK6B5S90C | | Windows | 192.168.31.207 | 30-E3-7A-6E-76-16 | | Unmanaged | Today |
| | N/A | | Windows | 192.168.31.251 | 00-1F-D0-1E-D5-53 | | Unmanaged | Today |

FortiEDR: обнаружение устройств



DASHBOARD

EVENT VIEWER 14

FORENSICS ▾

COMMUNICATION CONTROL 124

SECURITY SETTINGS ▾

INVENTORY 9

ADMINISTRATION 20

Protection ▾

kmikhaylov ▾

IOT DEVICES (7/7)

a ▾✕

All ▾

Create Group

Move to Group

Delete ▾

Device Details

Export ▾

| <input type="checkbox"/> | DEVICE GROUP NAME | DEVICE NAME | CATEGORY | MODEL | INTERNAL IP | MAC ADDRESS | LOCATION | FIRST SEEN | LAST SEEN |
|----------------------------|-------------------------|----------------------------------|--|-------------------------|-----------------------------|-------------------|-------------------|------------|-----------|
| ▶ <input type="checkbox"/> | Almaty IoT (0/0) | | | | | | | | |
| ▶ <input type="checkbox"/> | Default IOT Group (0/0) | | | | | | | | |
| ▼ <input type="checkbox"/> | Other (7/7) | | | | | | | | |
| | | <input type="checkbox"/> N/A | New | Media device | 192.168.7.8 | 90-A2-5B-24-CA-DA | Russia | Today | Today |
| | | <input type="checkbox"/> N/A | New | Other | Apple | 192.168.7.6 | 1C-36-BB-25-AB-C0 | Russia | Today |
| | | <input type="checkbox"/> TP-Link | New | Other | Linux 2.6.32 - 3.10 | 74-DA-88-4A-14-28 | Russia | Today | Today |
| | | <input type="checkbox"/> N/A | New | Network device | Murata Manufacturing, D-... | DC-EF-CA-1D-CE-43 | Russia | Today | Today |
| | | <input type="checkbox"/> N/A | New | Other | Fortinet, Linux 3.2 - 3.8 | 70-4C-A5-BB-6C-11 | Russia | Today | Today |
| | | <input type="checkbox"/> N/A | New | Other | Apple | 38-F9-D3-6A-89-A5 | Russia | Today | Today |
| | | <input type="checkbox"/> N/A | New | <div><div></div>▼</div> | 192.168.7.7 | 58-6B-14-9C-37-B4 | Russia | Today | Today |
| | | | <div><div>Storage</div><div>Terminal</div><div>VoIP adapter</div><div>VoIP phone</div><div>Webcam</div><div>Video Device</div></div> | | | | | | |

Fortinet Security Fabric

FortiEDR: интеграция с FortiGate

The screenshot displays the FortiGate VM64 web interface. The left sidebar shows the navigation menu with 'Addresses' selected. The main panel is titled 'Edit Address Group' and shows the configuration for a group named 'fedr'. The group is of type 'Group' and contains two members: 'dummy.address.com' and 'FortiEDR_195.201.72.6'. A tooltip is visible over the 'FortiEDR_195.201.72.6' member, showing details such as Address, Type (IP Range), IP Range (195.201.72.6 - 195.201.72.6), Interface (any), Comments (FortiEDR Event ID - 6400479), and References (1). The interface also includes fields for Group name, Color, Type, Members, Static route configuration, and Comments. The bottom of the panel has 'OK' and 'Cancel' buttons.

FortiGate VM64 fg1

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shapers

Traffic Shaping Policy

Traffic Shaping Profile

Security Profiles

VPN

User & Authentication

WiFi & Switch Controller

Log & Report

Edit Address Group

Group name fedr

Color Change

Type Group Folder

Members

dummy.address.com

FortiEDR_195.201.72.6

Static route configuration

Comments Write a comment... 0/255

Documentation

Online Help

Video Tutorials

Address FortiEDR_195.201.72.6

Type IP Range

IP Range 195.201.72.6 - 195.201.72.6

Interface any

Comments FortiEDR Event ID - 6400479

References 1

Edit

OK Cancel

FortiEDR: интеграция с FortiSandbox

DASHBOARD

EVENT VIEWER 2

FORENSICS

COMMUNICATION CONTROL 40

SECURITY SETTINGS

INVENTORY

ADMINISTRATION 65

Simulation

kirill

EVENTS

Archive

Mark As...

Export

Handle Event

Delete

Forensics

Exception Manager

All

ID

DEVICE

PROCESS

CLASSIFICATION

DESTINATIONS

RECEIVED

LAST UPDATED

updater_0520.exe

History

Malicious, by FortinetCloudServices , on 20-May-2020, 17:08:38

Simulation Process ...slupdater_0520.exe\ with PID 9223372036854775807 was terminated at device DESKTOP-CLLEKQ2 once

Simulation Device DESKTOP-CLLEKQ2 was isolated once

112.exe (1 event)

check.exe

test_file.exe

payload.exe

1rans.exe

hdtunepro...

LittleCrypt...

locky.exe (2 events)

test.exe (3 events)

ssh (1 event)

...

20-May-2020, 17:00:02

20-May-2020, 17:00:02

20-May-2020, 17:00:02

20-May-2020, 17:00:00

20-May-2020, 16:59:52

20-May-2020, 16:24:54

20-May-2020, 16:19:45

20-May-2020, 16:19:45

20-May-2020, 16:17:04

06-May-2020, 16:04:11

06-May-2020, 15:34:29

06-May-2020, 15:21:40

06-May-2020, 15:14:56

15-Apr-2020, 16:02:12

14-Apr-2020, 11:02:22

14-Apr-2020, 11:02:22

Malicious

Malicious

Inconclusive

Inconclusive

ADVANCED DATA

CLASSIFICATION DETAILS

Threat name: Unknown

Threat family: Unknown

Threat type: Unknown

History

Malicious, by FortinetCloudServices , on 20-May-2020, 17:08:38

Simulation Process ...slupdater_0520.exe\ with PID 9223372036854775807 was terminated at device DESKTOP-CLLEKQ2 once

Simulation Device DESKTOP-CLLEKQ2 was isolated once

Suspicious, by FortinetCloudServices , on 20-May-2020, 17:00:17

Triggered Rules

Execution Prevention

Sandbox Analysis - File was sent to the sandbox for analysis

A suspicious file was sent to the sandbox for analysis and inspection. After the analysis completes, the file will either be classified as malicious, in which case its future executions will be blocked, or it will be classified as benign, in which case its execution will continue.

Check the event classification. If cloud classification was not set, sandbox

Copyright © Fortinet Version 4.1.1.110


System Time (UTC +02:00) 17:12:07

FORTINET

© Fortinet Inc. All Rights Reserved.

47

FortiEDR: интеграция с FortiNAC



DASHBOARD

EVENT VIEWER 518

FORENSICS ▾

COMMUNICATION CONTROL ▾ 1224

SECURITY SETTINGS ▾

INVENTORY ▾

ADMINISTRATION 545

Protection ▾

Einat ▾

LICENSING

ORGANIZATIONS

USERS

DISTRIBUTION
LISTS

[EXPORT
SETTINGS](#)

TOOLS

SYSTEM
EVENTS

IP SETS

SMTP

Server Name *

Email address *

support@ensilo.com

Port *

587

Encryption type

TLS ▾

Sender Name

User name *

Password *

Use SMTP authentication

✓

Test

Save

Clear

OPEN TICKET

System name

Email address *

Save

Clear

SYSLOG

Define New Syslog

Name: *

FortiNAC

Host: *

10.0.1.34

Port: *

10514

Protocol:

TCP ▾

Use SSL:

✓

Test

NOTIFICATIONS

Security Events

Enabled

System Events

Disabled

Audit trail

Disabled

FORTINET

© Fortinet Inc. All Rights Reserved.

48

Лицензирование

Лицензирование



Количество узлов сети



Сервисы и подписки



Вопросы?

Кирилл Михайлов, kmikhaylov@fortinet.com
cis@fortinet.com