

FORTINET®

FortiEDR: средство обнаружения комплексных атак на рабочие станции

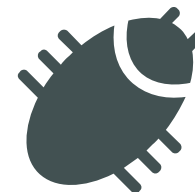
Кирилл Михайлов, Fortinet

Зачем?

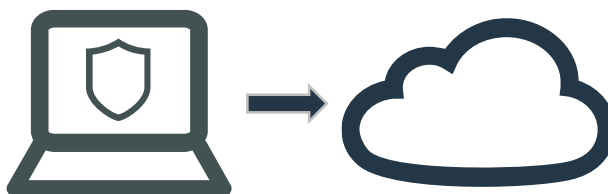
Зачем?



Эволюция атак



Управление уязвимостями



Размытие границ сети

Эволюция атак



Эволюция атак



Целевой фишинг



Вредоносное программное обеспечение



Атаки с использованием легитимного ПО

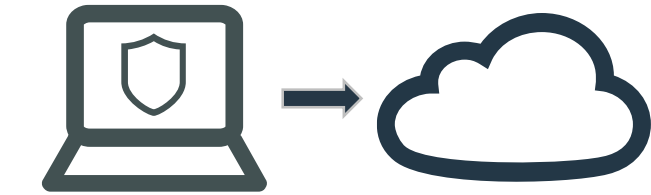


Угрозы нулевого дня

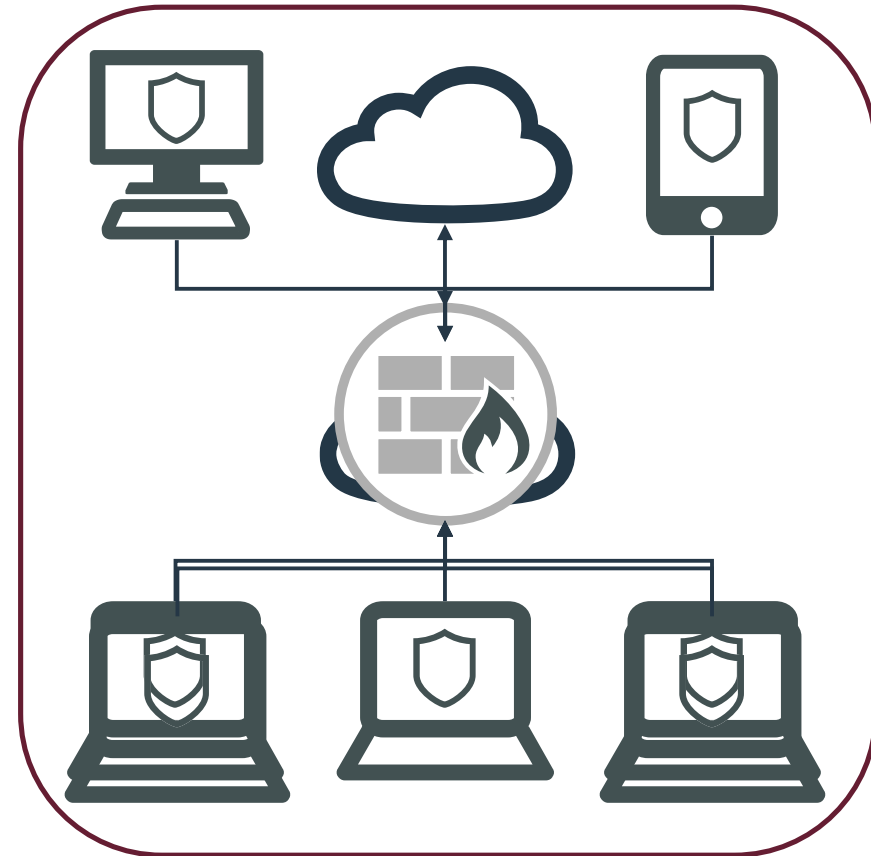


Вирусы-вымогатели

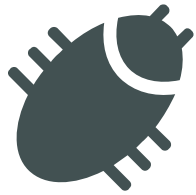
Размытие границ сети



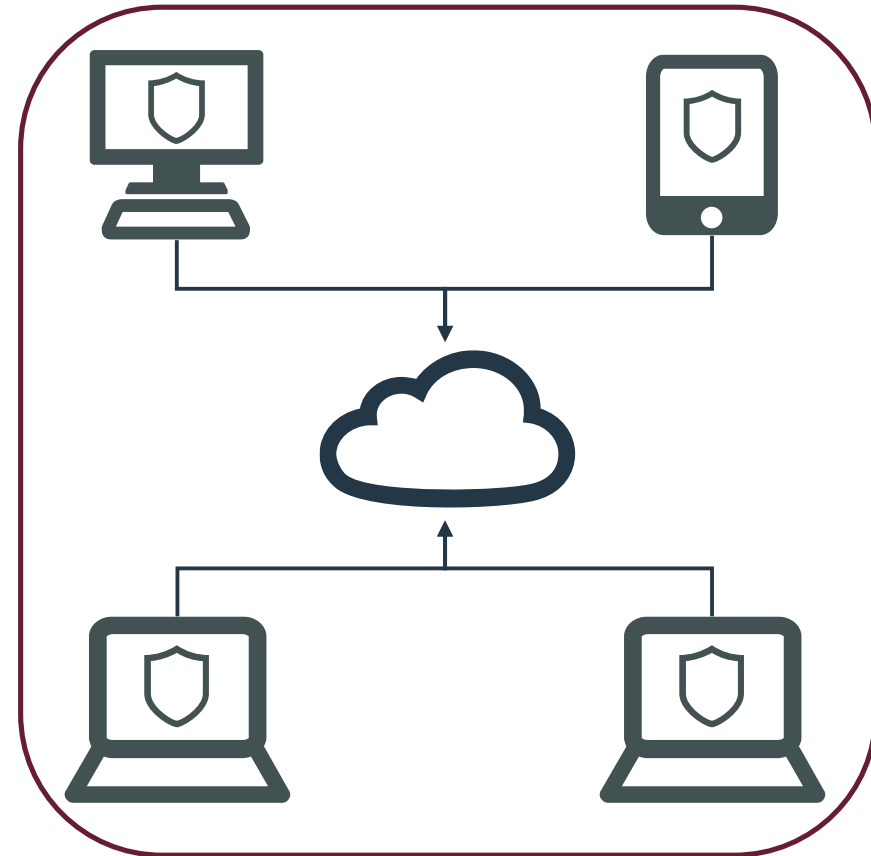
Размытие границ сети



Управление уязвимостями



Управление уязвимостями



Антивирусное ПО необходимо



Антивирусное ПО необходимо, но не достаточно



FortiClient как EDR?

| Функционал | FortiClient | FortiEDR |
|-----------------------------|-------------|----------|
| Защитные механизмы | + | + |
| Безопасный удаленный доступ | + | - |
| Проведение расследований | - | + |
| Проактивный поиск угроз | - | + |
| Реагирование на инциденты | - | + |

Автоматизация EDR

FortiEDR vs. неавтоматизированный EDR



Схема работы FortiEDR

Защита: pre-infection

Защита: post-infection

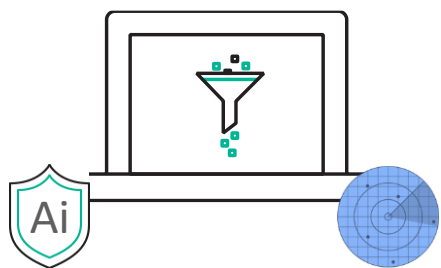
Реагирование

Префилтрация

Запись

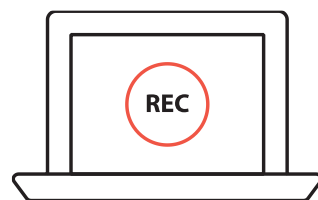
Сбор данных

Центральный компонент

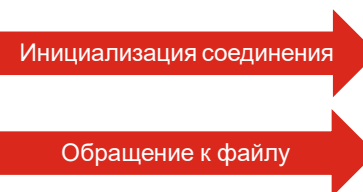


Шаг 1:
Коллектор блокирует известные угрозы

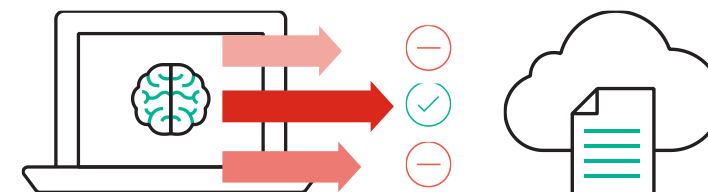
Шаг 2:
Коллектор реагирует на угрозы в соответствии с заранее заданными политиками



Шаг 3:
Коллектор собирает метаданные ОС



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



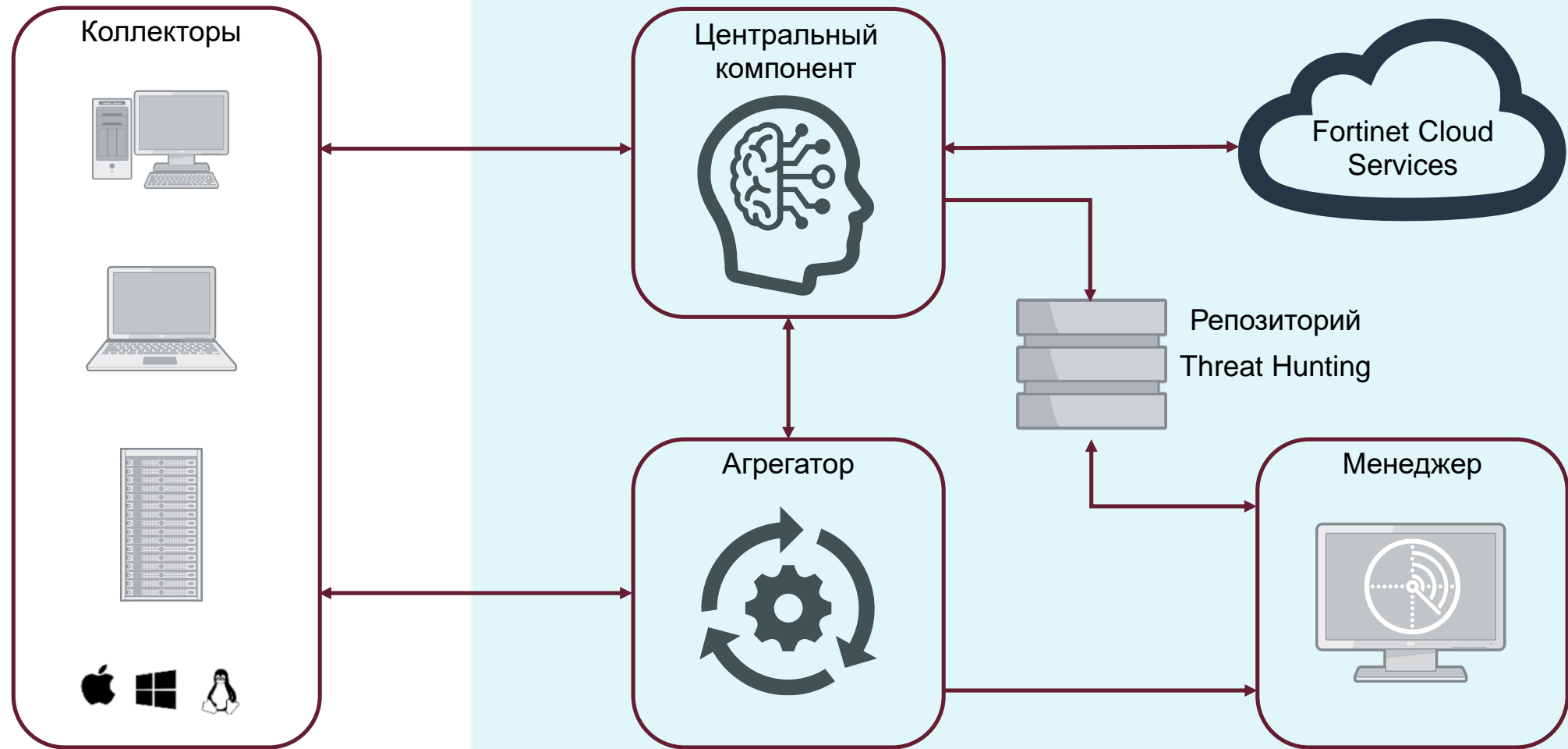
Шаг 5:
Центральный компонент анализирует данные, полученные от коллектора

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

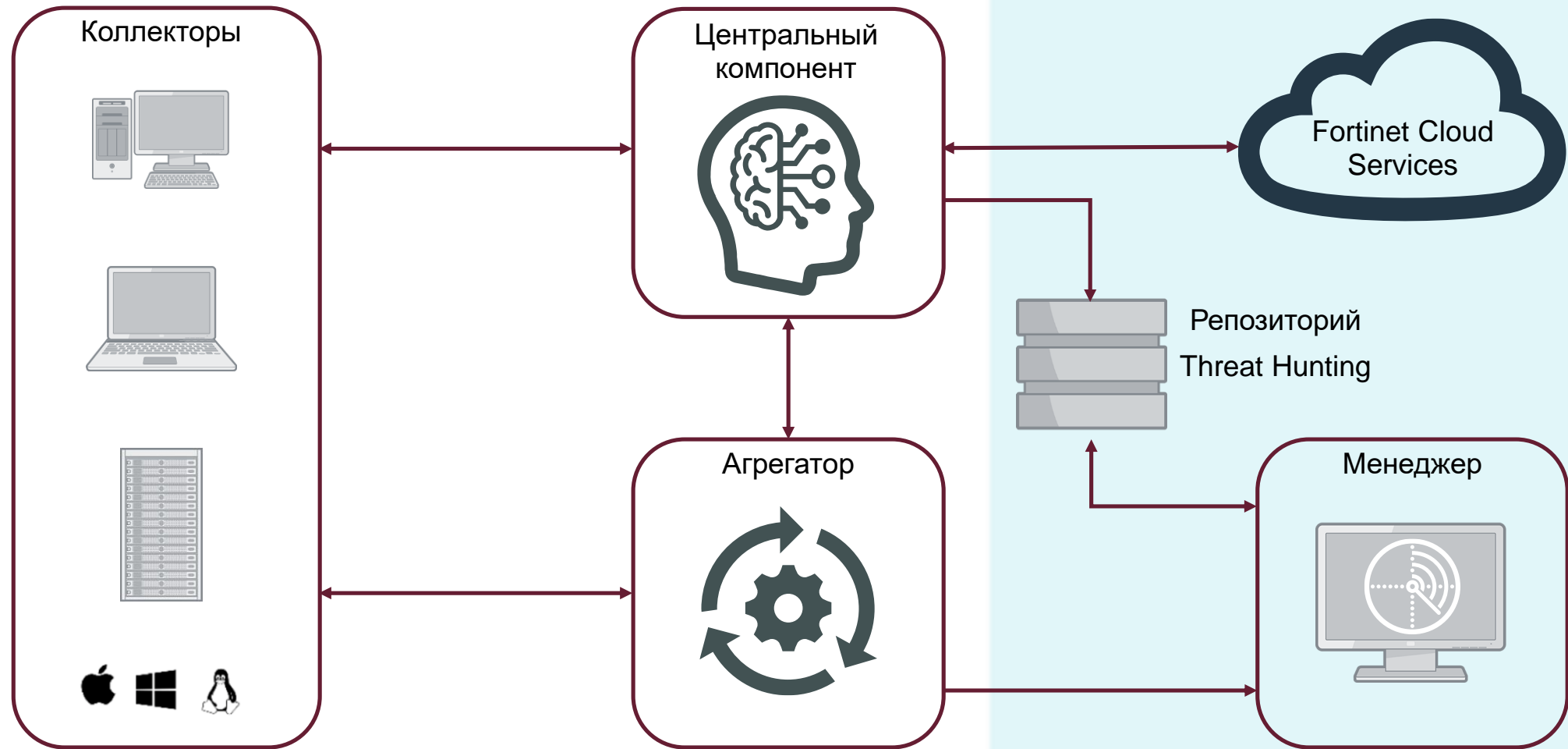
FortiEDR

Архитектура

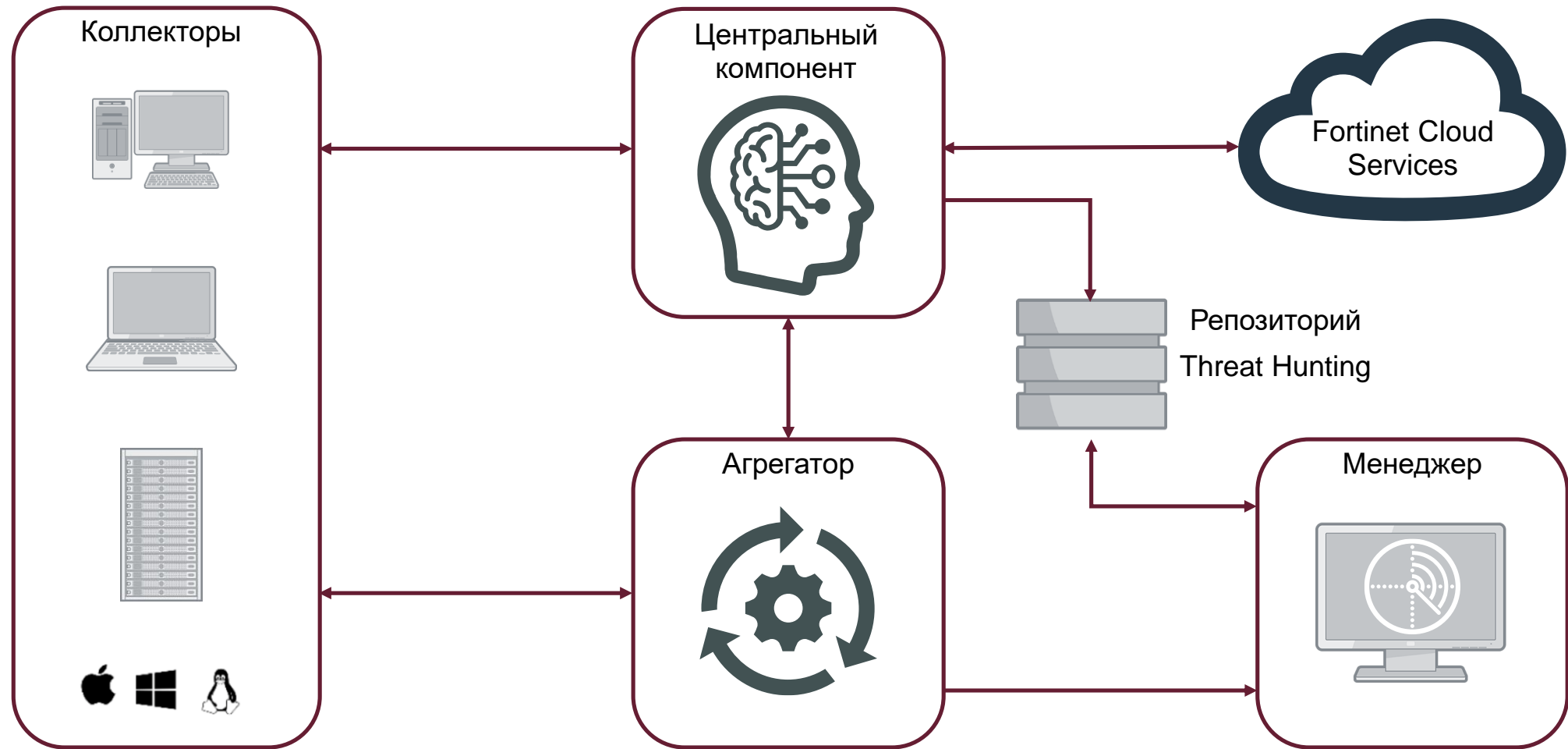
FortiEDR: варианты развертывания: облако



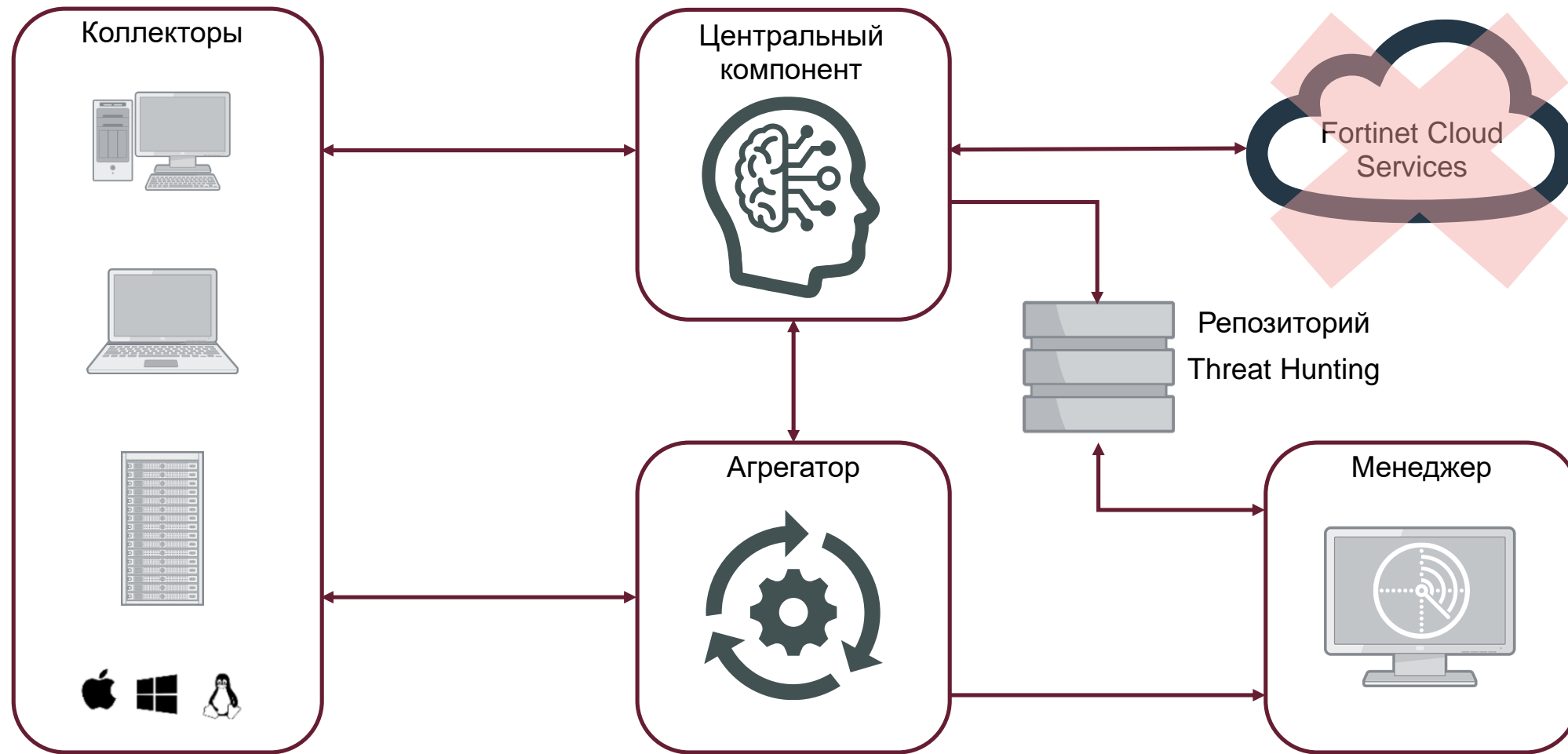
FortiEDR: варианты развертывания: гибрид



FortiEDR: варианты развертывания: локальный



FortiEDR: варианты развертывания: offline



FortiEDR

Интерфейс

FortiEDR: главный экран

SECURITY EVENTS

Unhandled Devices

1 Malicious

1 Devices protected by Fortinet

COMMUNICATION CONTROL

Unresolved Communicating Applications

There are no unhandled applications in the system

COLLECTORS

View by operating system

- Running
- Degraded
- Disconnected
- Pending reboot
- Disabled

Windows

MOST TARGETED

Devices (#)

- Malicious
- Suspicious
- PUP
- Inconclusive
- Likely Safe

1 Malicious 1 Suspicious 1 PUP 1 Inconclusive

EXTERNAL DESTINATIONS

Applications

Day

SYSTEM COMPONENTS

- Running
- Degraded
- Disconnected

FortiEDR: политики безопасности

SECURITY POLICIES

Clone Policy Set Mode Assign Collector Group Exception Manager Delete

All

| POLICY NAME | RULE NAME | ACTION | STATE |
|-------------------------------|--|--------|--------------------------|
| IRansomware Prevention | | | <input type="checkbox"/> |
| | 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.

FortiEDR: автоматизация

AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

Clone Playbook Set Mode Assign Collector Group Delete

| NAME | | MALICIOUS | SUSPICIOUS | PUP | INCONCLUSIVE | LIKELY SAFE |
|---|---|--|--------------------------|--------------------------|--------------------------|--------------------------|
| Default Playbook | <input type="checkbox"/> <input type="checkbox"/> | | | | | |
| my_playbook | <input type="checkbox"/> <input type="checkbox"/> | | | | | |
| 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.

FortiEDR: события

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

| <input type="checkbox"/> | 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 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

| 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

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

▶ **ADVANCED DATA**

FortiEDR: события

EVENTS

Archive Mark As

Unhandled ID

- report.pdf.exe (10 events)
- cscript.exe (3 events)
- User: DESKTOP-CLLEKQ2
- dkINTpuA.dll (1 event)
- rundll32.exe (3 events)

Suspicious Application - Connection Attempt from a Suspicious...

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 Corresponding File

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 Suspicious...
 - Unmapped Executable - Executable File Without a Corresponding File

FortiEDR: события

EVENTS

Archive
Mark As..
Export
Handle Event
Delete
Forensics
Exception Manager

| <input type="checkbox"/> | Unhandled | ID | DEVICE | PROCESS | CLASSIFICATION | DESTINATIONS | RECEIVED | LAST UPDATED |
|-------------------------------------|-----------|----------------------------------|-----------------|-----------------------|--|---------------------|-----------------------|-----------------------|
| <input type="checkbox"/> | | 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 |
| <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

Malicious **FORTINET**
 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

- IExfiltration Prevention
 - Invalid Checksum - Connection Attempt from Application with I...
 - Unconfirmed Executable - Executable File Failed Verification T...
 - Unmapped Executable - Executable File Without a Correspon...

ADVANCED DATA

FortiEDR: события

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 | |

```

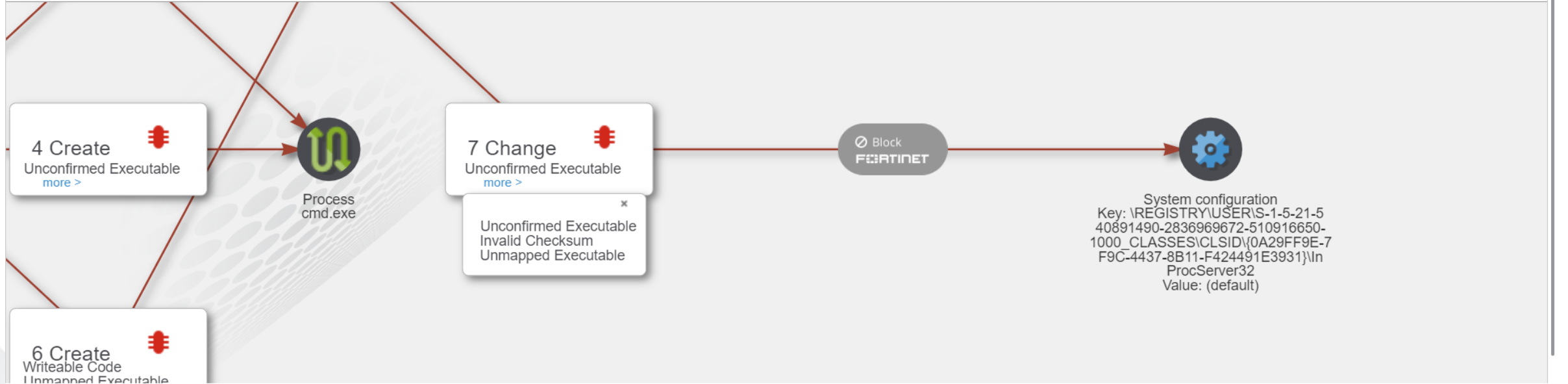
graph LR
    A[Process winlogon.exe] --> B[1 Create]
    B --> C[Process userinit.exe]
    C --> D[2 Create]
    D --> E[Process explorer.exe]
    E --> F[3 Create]
    F --> G[Process report.pdf.exe]
    G --> H[4 Create Unconfirmed Executable]
    G --> I[5 Open Unconfirmed Executable]
    G --> J[6 Create Writable Code Unmapped Executable]
    H --> K[Process cmd.exe]
    I --> L[Thread]
    J --> L
    L --> M[7 Change Unconfirmed Executable]
    M --> N[System configuration]
            
```

FortiEDR: события

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 | | |



FortiEDR: события

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 |
| <div style="display: flex; justify-content: space-between; font-size: small;"> 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> | | | | | | |
| <div style="display: flex; justify-content: space-around; align-items: center;"> PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION CREATE PROCESS OPEN PROCESS THREAD CREATION SYSTEM CONFIGURATION </div> | | | | | | |

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 -\Device\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... |

FortiEDR: события

Navigation: 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

| 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 PROCESS CREATION

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 -\Device\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... |

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: to address:

Retrieve the entire process memory

Estimated **Memory** Retrieval file size: **5.2 MB**

Retrieve
Cancel

Raw Data Items: All Selected 1/1

| LAST SEEN | | |
|----------------------------------|-----------------------|----------|
| 13:05:33 | 01-Apr-2020, 13:05:33 | 🚫 |
| User: DESKTOP-CLLEKQ2\kmikhaylov | | Count: 1 |

PARENT PROCESS CREATION

SYSTEM CONFIGURATION

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

FortiEDR: события

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

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

PARENT PROCESS CREATION
PARENT PROCESS CREATION
PARENT PROCESS CREATION

SYSTEM CONFIGURATION

Process ID: 4348 Company:

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

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

| EXECUTABLE FILE NAME | WRIT |
|---|------|
| Main -\Device\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
 Handle persistent data (registry)

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 Type

Remediate
Cancel

Raw Data Items: All Selected 1/1

| VED | LAST SEEN |
|----------------------------------|-----------------------|
| -2020, 13:05:33 | 01-Apr-2020, 13:05:33 |
| User: DESKTOP-CLLEKQ2\kmikhaylov | Count: 1 |

THREAD CREATION
SYSTEM CONFIGURATION

Process Hash (SHA-1): 208982E88ABA811BD5AA307A664ED55473B4D2BE

Process Owner: DESKTOP-CLLEKQ2\kmikhaylov

| ADDRESS | END ADDRESS | HASH |
|-----------|----------------|----------------------------|
| 92c270000 | 0x7ff92c458000 | 208982E88ABA811BD5AA30... |
| 0000 | 0x57d000 | 3A0D965CED62D33A830A41... |
| | 0x4fa000 | B64978FE52B04A841A7ADD... |
| | 0x4c0000 | 27F027309612871D237AE17... |
| | 0x7ff92cc80000 | AD3E678DB0413EEDD9AAF... |

Copyright © Fortinet Version 4.1.0.78 System Time (UTC +02:00) 15:29:21

FortiEDR: события

Remediate



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

| COLLECTOR NAME | PATH | FILE NAME | CREATION TIME | MODIFICATION TIME | OS |
|-----------------|--|----------------|--------------------|--------------------|-----------------------|
| DESKTOP-CLLEKQ2 | \device\harddiskvolume3\users\kmikhaylov\downloads | report.pdf.exe | 01-Apr-2020, 13:01 | 01-Apr-2020, 13:01 | Windows 10 Enterprise |
| DESKTOP-CLLEKQ2 | \device\harddiskvolume3\users\kmikhaylov\downloads | report.pdf.exe | 30-Mar-2020, 17:39 | 30-Mar-2020, 17:39 | Windows 10 Enterprise |
| DESKTOP-CLLEKQ2 | \device\harddiskvolume3\users\kmikhaylov\downloads | report.pdf.exe | 30-Mar-2020, 15:35 | 30-Mar-2020, 15:35 | Windows 10 Enterprise |
| DESKTOP-CLLEKQ2 | \device\harddiskvolume3\users\kmikhaylov\downloads | report.pdf.exe | 25-Mar-2020, 15:56 | 25-Mar-2020, 15:56 | Windows 10 Enterprise |
| DESKTOP-CLLEKQ2 | \device\harddiskvolume3\users\victim\downloads | report.pdf.exe | 25-Mar-2020, 15:42 | 25-Mar-2020, 15:42 | Windows 10 Enterprise |
| DESKTOP-CLLEKQ2 | ...in\1-5-21-251774275-78421870-3683231849-1111 | \$ri7973z.exe | 25-Mar-2020, 15:10 | 25-Mar-2020, 15:31 | Windows 10 Enterprise |
| DESKTOP-CLLEKQ2 | ...in\1-5-21-251774275-78421870-3683231849-1111 | \$r7jymp.exe | 25-Mar-2020, 15:30 | 25-Mar-2020, 15:30 | Windows 10 Enterprise |
| DESKTOP-CLLEKQ2 | ...in\1-5-21-251774275-78421870-3683231849-1111 | \$rae3z2r.exe | 25-Mar-2020, 15:29 | 25-Mar-2020, 15:29 | Windows 10 Enterprise |
| DESKTOP-CLLEKQ2 | ...in\1-5-21-251774275-78421870-3683231849-1111 | \$rc0l286.exe | 25-Mar-2020, 15:10 | 25-Mar-2020, 15:10 | Windows 10 Enterprise |
| DESKTOP-CLLEKQ2 | \device\harddiskvolume3\users\victim\downloads | report.pdf.exe | 25-Mar-2020, 14:49 | 25-Mar-2020, 14:49 | Windows 10 Enterprise |

FortiEDR: контроль сетевых соединений

The screenshot displays the FortiEDR interface with the 'COMMUNICATION CONTROL' section active. A 'MODIFY ACTION' dialog is open for the application 'Host Process for Windows Services'. The dialog shows a list of policies with their respective actions:

| Policy | Action |
|-----------------------------------|--------|
| Default Communication Control ... | Allow |
| Servers Policy | Allow |
| my_policy | Allow |
| Isolation Policy | Allow |

The 'my_policy' dropdown menu is expanded, showing the following options:

- Allow
- According to policy (Allow)
- According to policy (Allow)
- Deny

The 'According to policy (Allow)' option is currently selected. Below the dropdown is a 'Type comment' text area and a checkbox labeled 'Will be applied to all current and future versions of the selected applications' with an 'Exclude All Current Versions' sub-option. At the bottom of the dialog are 'Save and Unresolve', 'Save', and 'Cancel' buttons.

APPLICATIONS

| APPLICATION | VENDOR |
|-----------------------------------|--------------------------------|
| Host Process for Windows Ser... | Signed Microsoft Corporation |
| 10.0.10586.0 (th2_release... | |
| Windows Explorer | Signed Microsoft Corporation |
| Host Process for Windows Tasks | Signed Microsoft Corporation |
| Photos | Unsigned Microsoft Corporation |
| Windows Problem Reporting | Signed Microsoft Corporation |
| Background Task Host | Signed Microsoft Corporation |
| Microsoft Compatibility Teleme... | Signed Microsoft Corporation |
| Search and Cortana application | Signed Microsoft Corporation |

ADVANCED DATA

APPLICATION INFO

Application Description: Host Process for Windows Services
First Connection Time: 24-Mar-2020, 12:24:06
Last Connection Time: 01-Apr-2020, 16:01:12
Process Names: \\Device\HarddiskVolume3\Windows\System32\svchost.exe (800...

APPLICATION DETAILS

Host Process for Windows Services

Policies

| Policy | Action |
|-----------------------------------|--------|
| Default Communication Control ... | Allow |
| Servers Policy | Allow |
| my_policy | Allow |
| Isolation Policy | Allow |

DESTINATIONS

| IP | CONNECTION TIME | COUNTRY |
|-----------------|-----------------------|---------------|
| 8.8.8.8 | 01-Apr-2020, 16:01:12 | United States |
| 67.26.5.254 | 01-Apr-2020, 16:01:12 | United States |
| #02:0:0:0:0:1:3 | 01-Apr-2020, 16:01:05 | N/A |



Вопросы?

Кирилл Михайлов, kmikhaylov@fortinet.com