



FortiEDR/FortiXDR

Кирилл Михайлов, системный инженер

kmikhaylov@fortinet.com

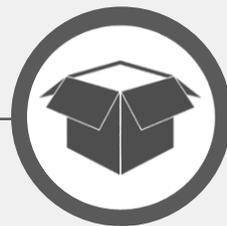
Минимизация издержек



Разведка



Вооружение



Доставка



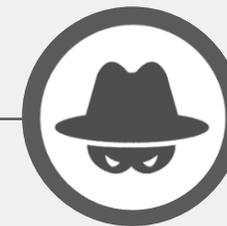
Эксплуатация



Установка



Получение управления



Выполнение действий



Инструменты обнаружения и предотвращения



Fortinet Security Fabric



Рабочие станции / серверы



Видимость и контроль

конечных узлов



Функционал EPP



FortiClient



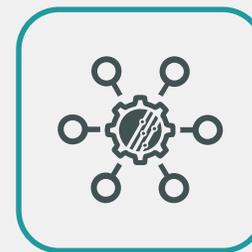
Модуль защиты от
ВПО



Модуль VPN



Модуль Compliance



Модуль интеграции со
сторонними системами

Функционал EDR



FortiEDR



Антивирусный модуль



Модуль анализа активности



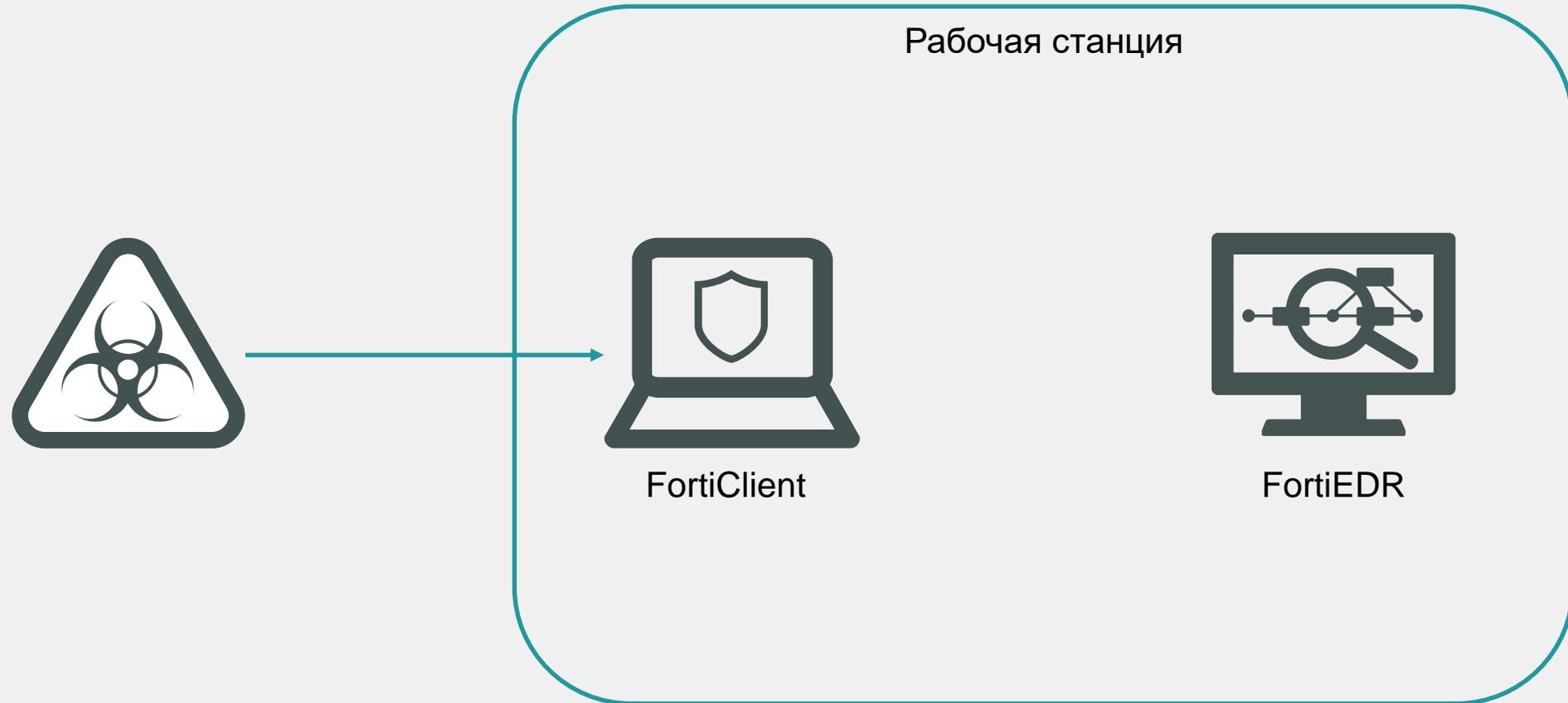
Модуль реагирования и восстановления системы



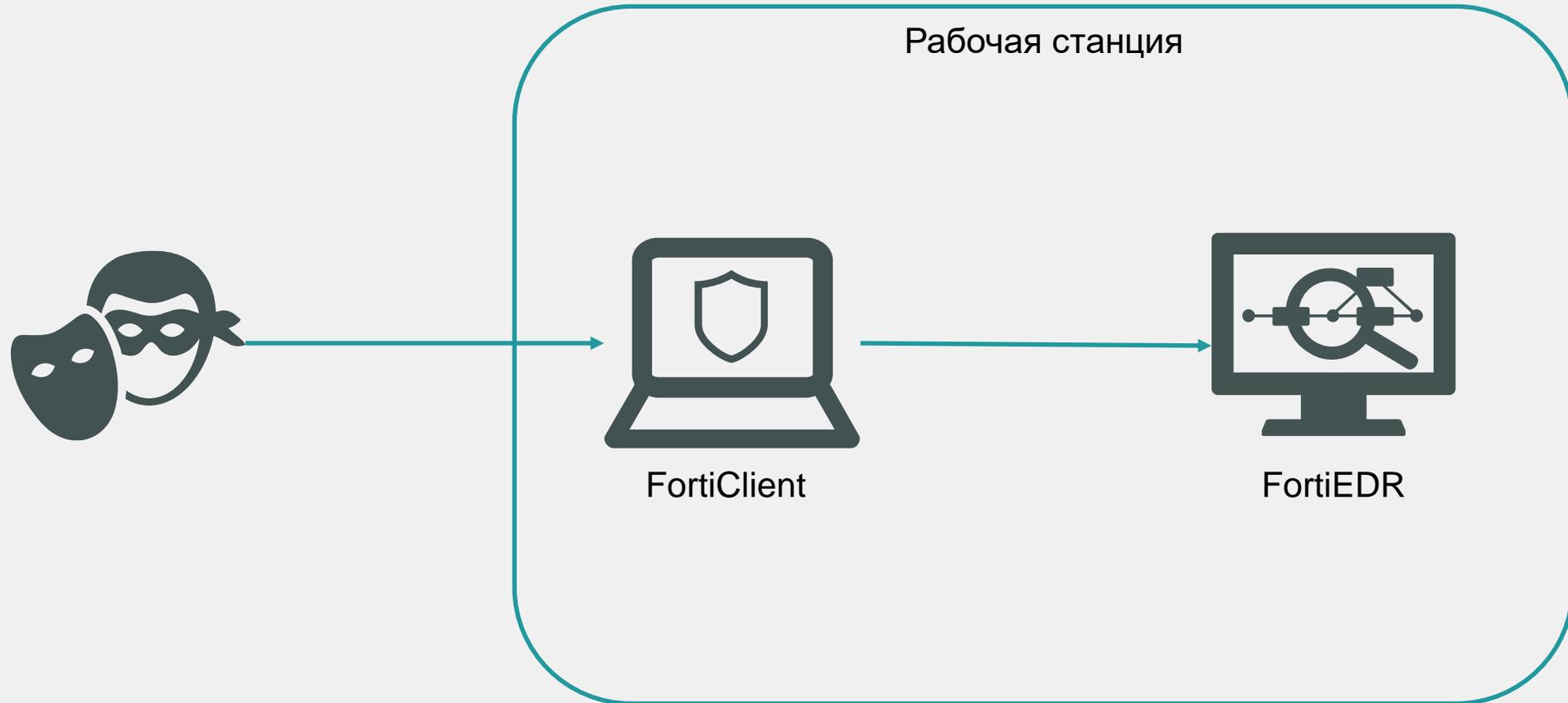
Модуль анализа и закрытия уязвимостей



EDR: защита от известных угроз



EDR: обнаружение продвинутых атак



EDR замена EPP?



FortiClient



FortiEDR

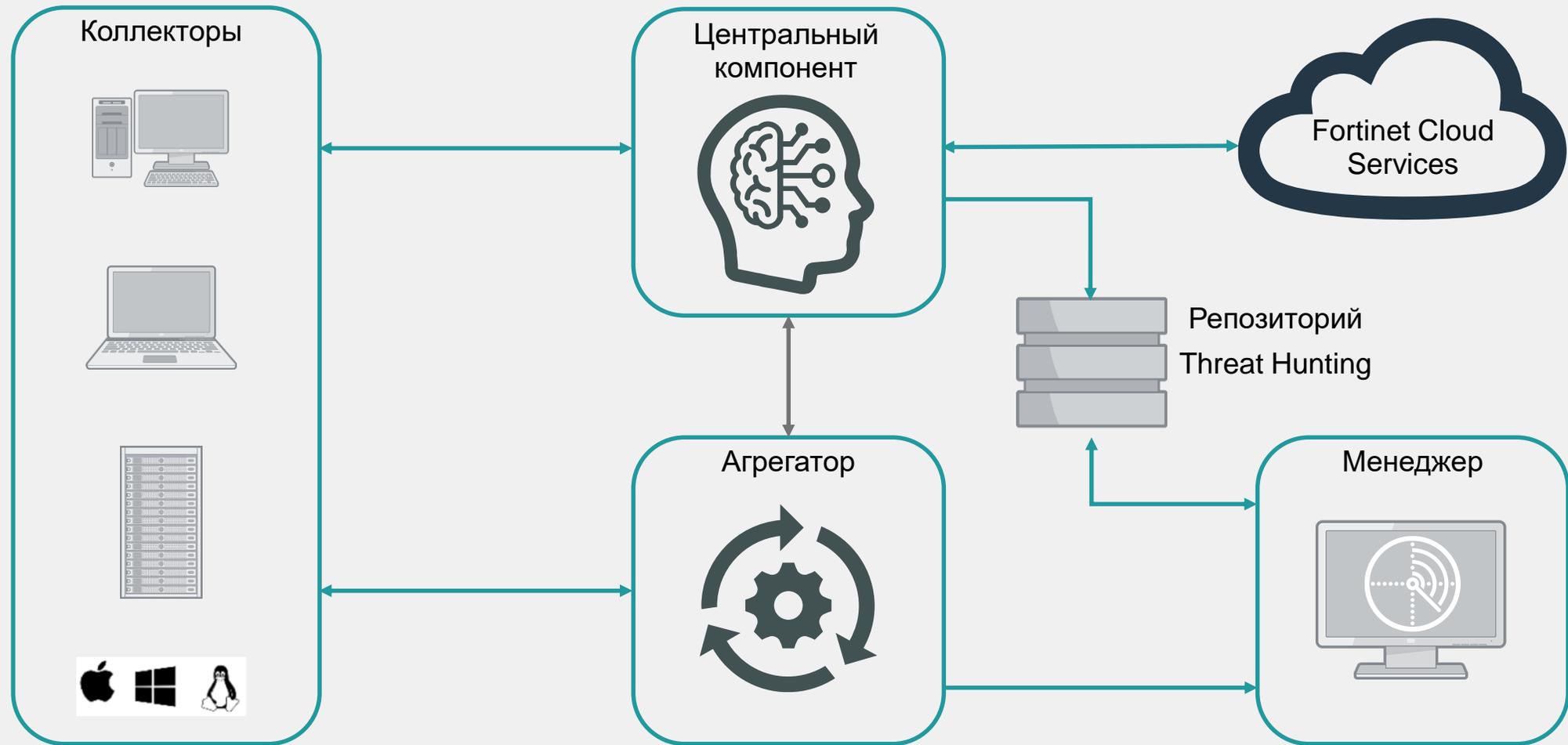


FortiEDR

Компоненты и архитектура



FortiEDR: архитектура



FortiEDR

Технологии обнаружения и реагирования



FortiEDR: блокировка

DASHBOARD
EVENT VIEWER
FORENSICS
COMMUNICATION CONTROL 204
SECURITY SETTINGS
INVENTORY
ADMINISTRATION 19
Protection ●
kmikhaylov

APPLICATIONS

Showing 1-10/284

All |
 Mark As... |
 Delete |
 Modify Action |
 Advanced Filter |
 Export

APPLICATION	VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
GoToMeeting	Signed LogMeIn, Inc	3	Unknown	15-May-2020	28-Jan-2021
FortiClient Sandbox Agent	Signed Fortinet Inc.	5	Unknown	15-May-2020	28-Jan-2021
Spooler SubSystem App	Signed Microsoft Corporation	3	Unknown	15-May-2020	16-Mar-2021
Google Chrome	Signed Google	3	Critical	15-May-2020	28-Feb-2021
88.0.4324.146		3	Critical	08-Feb-2021	28-Feb-2021
88.0.4324.150			Critical	09-Feb-2021	20-Feb-2021
88.0.4324.190			High	28-Feb-2021	28-Feb-2021
Dropbox Update	Signed Dropbox, Inc.	5	Unknown	15-May-2020	28-Jan-2021

VERSION DETAILS

Google Chrome, v. 88.0.4324.146

Policies

Policy	Action
Default Communication Control ...	Deny According to policy
Servers Policy	Deny According to policy
ComControl_K	Deny Manually
ComControl R	Deny According to policy

Vulnerabilities

Total 35 CVEs

- CVE-2021-21155 - Critical (CVSS 3.0: 9.6, CVSS 2.0: 6.8)
- CVE-2021-21154 - Critical (CVSS 3.0: 9.6, CVSS 2.0: 6.8)

ADVANCED DATA

APPLICATION INFO

Application Description: Google Chrome

First Connection Time: 08-Feb-2021, 11:50:43

Last Connection Time: 28-Feb-2021, 19:15:17

Process Names:

- \Device\HarddiskVolume3\Program Files (x86)\Google\Chrome\Application\c...
- \Device\HarddiskVolume2\Program Files (x86)\Google\Chrome\Application\c...

APPLICATION USAGE

Total System: 218.2 connections / day

Almaty: 218.2 connections / day

[More...](#)

DESTINATIONS

IP	CONNECTION TIME	COUNTRY
108.177.14.113	28-Feb-2021, 19:15:17	United States
239.255.255.250	28-Feb-2021, 19:14:55	N/A
64.233.161.100	28-Feb-2021, 19:07:31	United States

[More...](#)

Copyright © Fortinet Version 5.0.1.200

System Time (UTC +01:00) 09:40:35



Облачная, локальная,
Гибридная архитектура



Легкий агент



FortiEDR: блокировка

Fortinet FortiEDR Security Settings interface showing Security Policies and Assigned Collector Groups.

SECURITY POLICIES

Showing 1-10/19

POLICY NAME	RULE NAME	ACTION	STATE
Device Control			
eXtended Detection			
DevC_Kirill			
ExecP_Kirill			
	Malicious File Detected	Block	Enabled
	Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Block	Enabled
	Sandbox Analysis - File was sent to the sandbox for analysis	Log	Enabled
	Stack Pivot - Stack Pointer is Out of Bounds	Block	Enabled
	Suspicious Driver Load - Attempt to load a suspicious driver	Block	Enabled
	Suspicious File Detected	Block	Enabled
	Suspicious Script Execution - A script was executed in a suspicious context	Block	Enabled
	Unconfirmed File Detected	Block	Enabled
ExecP_Renat			
Execution Prevention_OT			
ExfilP_Renat			

ASSIGNED COLLECTOR GROUPS

- Unassign Group
- Kirill (1 collector included)

ADVANCED POLICY & RULE DATA

Copyright © Fortinet Version 5.0.1.200

System Time (UTC +01:00) 09:46:01



Облачная, локальная,
Гибридная архитектура



Легкий агент



FortiEDR: обнаружение

The screenshot displays the FortiEDR interface with the following components:

- Navigation Bar:** DASHBOARD, EVENT VIEWER (active), FORENSICS, COMMUNICATION CONTROL (205), SECURITY SETTINGS, INVENTORY, ADMINISTRATION (26), Simulation (toggle), kmikhaylov (user).
- EVENTS Section:**
 - Tools: Archive, Mark As..., Export, Handle Event, Delete, Forensics, Exception Manager.
 - Search: Showing 1-17/172, Search Event.
 - Table:
- CLASSIFICATION DETAILS Section:**
 - History:
 - Suspicious, by FortinetCloudServices, on 23-Mar-2021, 01:58:51
 - Simulation Device win10-vm was isolated once
 - Inconclusive, by Fortinet, on 23-Mar-2021, 01:58:38

- ADVANCED DATA Section:**
- Event Graph, Geo Location, Automated Analysis (active).
- Timeline: Inconclusive (Fortinet on 22-Mar-2021 15:48:03) → Suspicious (FortiCloudServices on 23-Mar-2021 01:58:39). Comment: Suspicious execution of .vbs file.
- File (1): wscript.exe
 - SHA1: 542c46c652ddefc87414213a8bea0c65dd0377a9
 - Hash reputation: Safe by FortiLabs, Kaspersky, VirusTotal, FortiGuard, Reversing...
- Memory (0)
- Network & Extended Data (1): 140.82.121.4
 - IP reputation: Inconclusive by FortiLabs intelligence services

Copyright © Fortinet Version 5.0.1.200

System Time (UTC +01:00) 14:11:54



Облачная, локальная,
Гибридная архитектура



Легкий агент



FortiEDR: реагирование

DASHBOARD EVENT VIEWER **FORENSICS** COMMUNICATION CONTROL 204 SECURITY SETTINGS INVENTORY ADMINISTRATION ! Protection ! kmikhaylov

THREAT HUNTING

CATEGORY: All Categories | DEVICE: All Devices | Behavior: execution and Type: ("Process Creation") and Target.Process.Name: ("cmd.exe")

TIME: Last 7 days

All Activity (20) | Process (20) | File (0) | Network (0) | Registry (0) | Event Log (0)

CATEGORY	OS	DEVICE NAME	TYPE	BEHAVIOR	PROCESS AND ATTRIBUTES	TARGET	EVENT ATTRIBUTES
Process Creation	win10-vm	win10-vm	Process Cr...	Execution	win10_upd_block.exe 64 bit	cmd.exe	SOURCE PID 6076
Process Creation	win10-vm	win10-vm	Process Cr...	Execution	explorer.exe 64 bit	cmd.exe	SOURCE PID 1820
Process Creation	win10-vm	win10-vm	Process Cr...	Execution	explorer.exe 64 bit	cmd.exe	SOURCE PID 1820
Process Creation	win10-vm	win10-vm	Process Cr...	Execution	vmtoolsd.exe 64 bit	cmd.exe	SOURCE PID 2832
Process Creation	win10-vm	win10-vm	Process Cr...	Execution	win10_upd_block.exe 64 bit	cmd.exe	SOURCE PID 2528
Process Creation	win10-vm	win10-vm	Process Cr...	Execution	win10_upd_block.exe 64 bit	cmd.exe	SOURCE PID 3728

Choose Columns | Process Creation | Execution

Mitre Techniques

- Technique: Command and Scripting Interpreter: Windows Command Shell, T1059.003
- Tactic: Execution, TA0002

cmd.exe | PID-4908

Path: C:\Windows\System32\cmd.exe

Executing user: INTERNAL\Administrator

Parent: \Device\HarddiskVolume3\Users\Administrator\Downloads\win10... ID - 6...

Product: Microsoft® Windows® Operating System, v10.0.18362.1316

SHA1: 3D7A84C1E63362D1213CCF9F25A869FE936C8156

Command line: /c "win10_upd_block.bat"

Copyright © Fortinet Version 5.0.1.200

System Time (UTC +01:00) 08:18:28



Облачная, локальная,
Гибридная архитектура



Легкий агент



Расширенные обнаружение и реагирование



FortiEDR



Fortinet Security Fabric

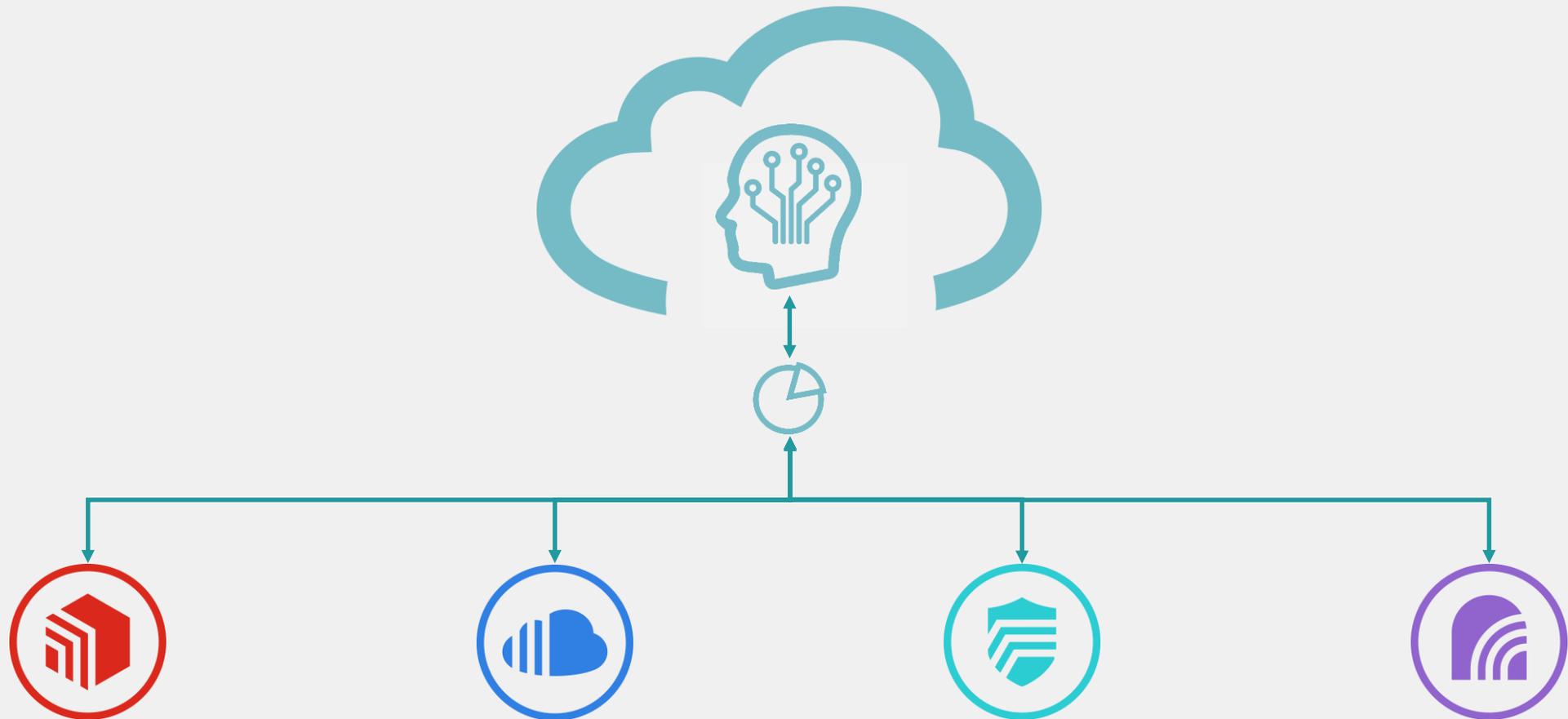


Расширение автоматизации

Обнаружения и реагирования на угрозы

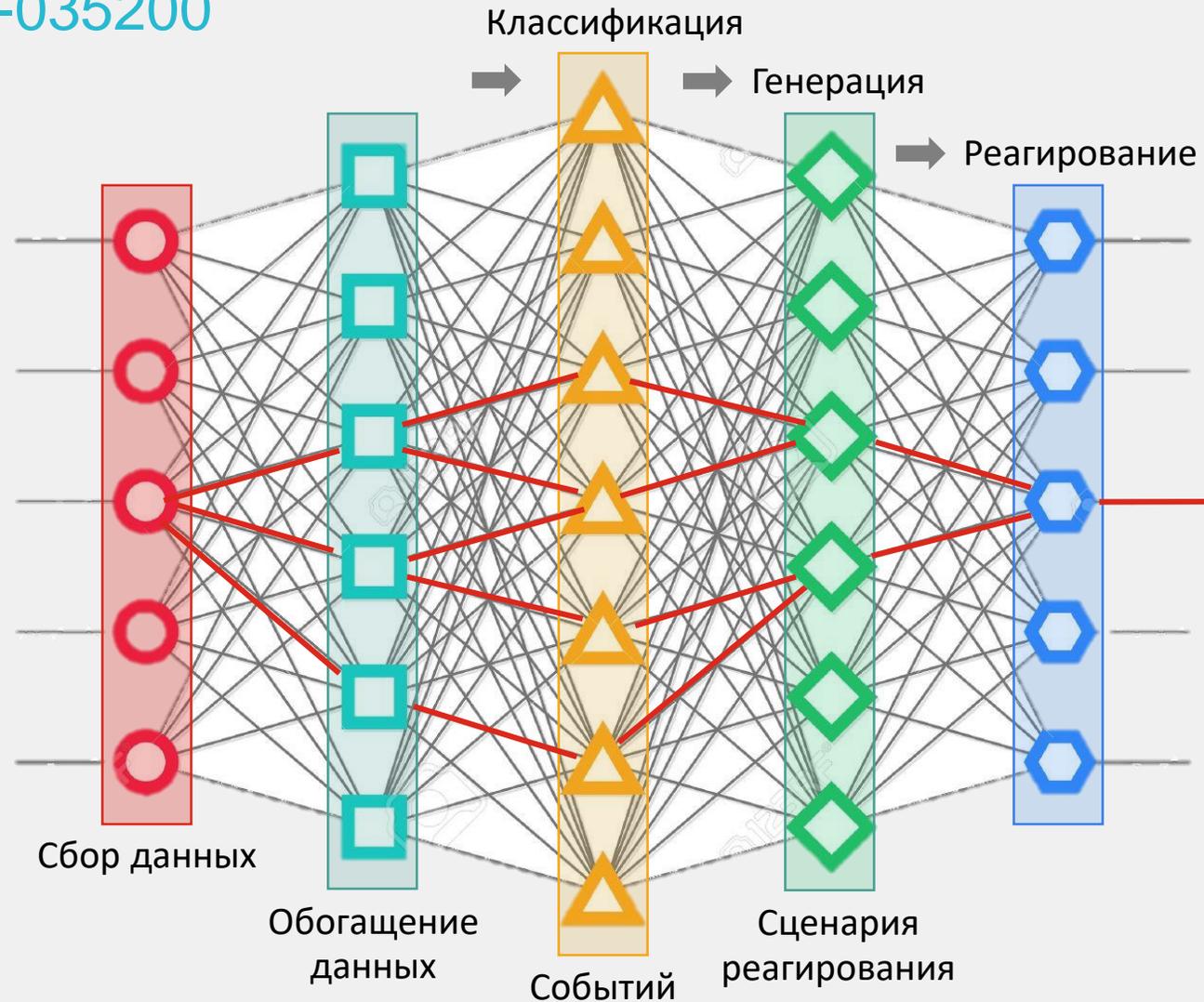


FortiXDR



FortiXDR: ANN

Патент: #FORT-035200



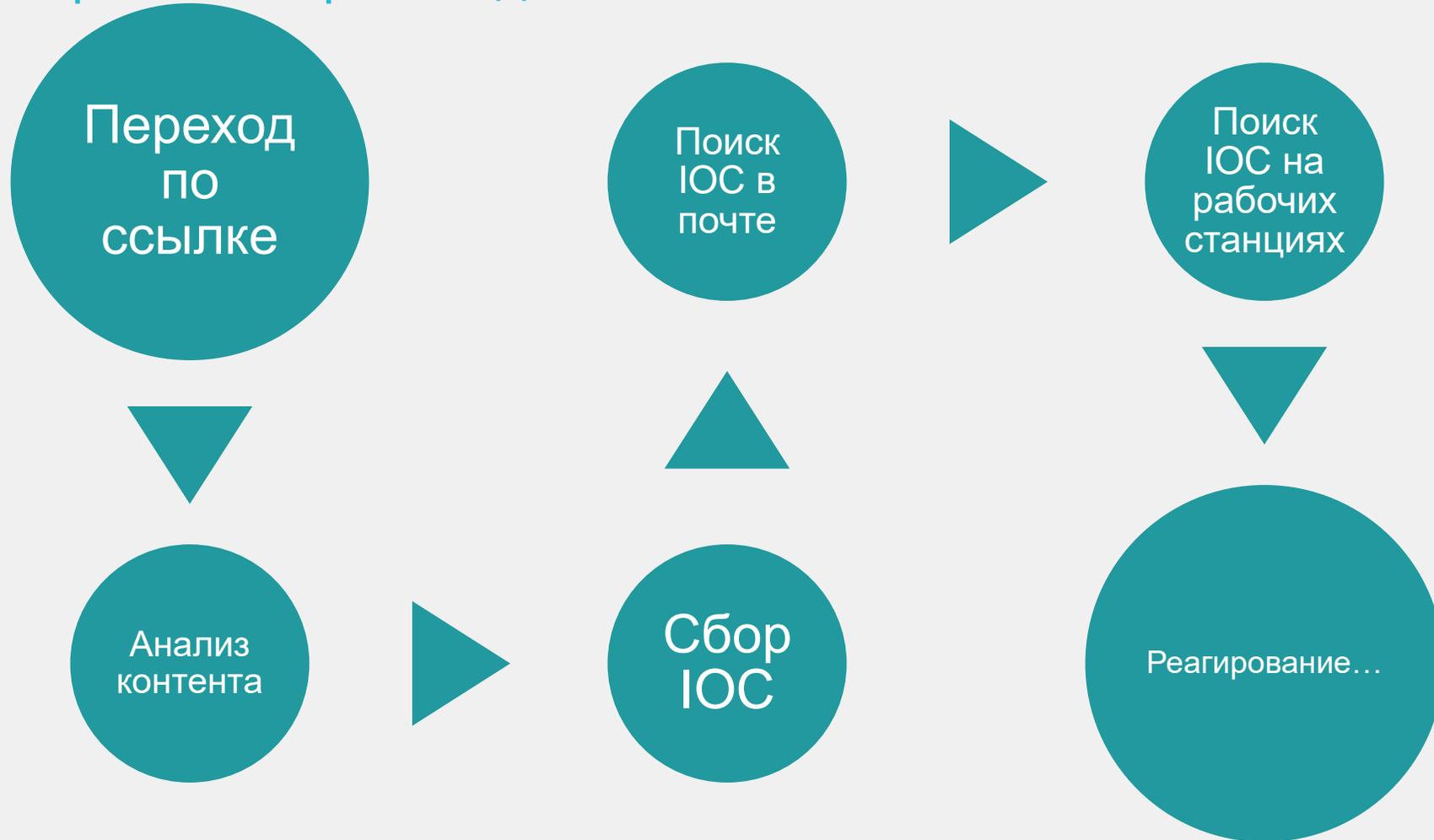
FortiXDR

Пример: целевой фишинг



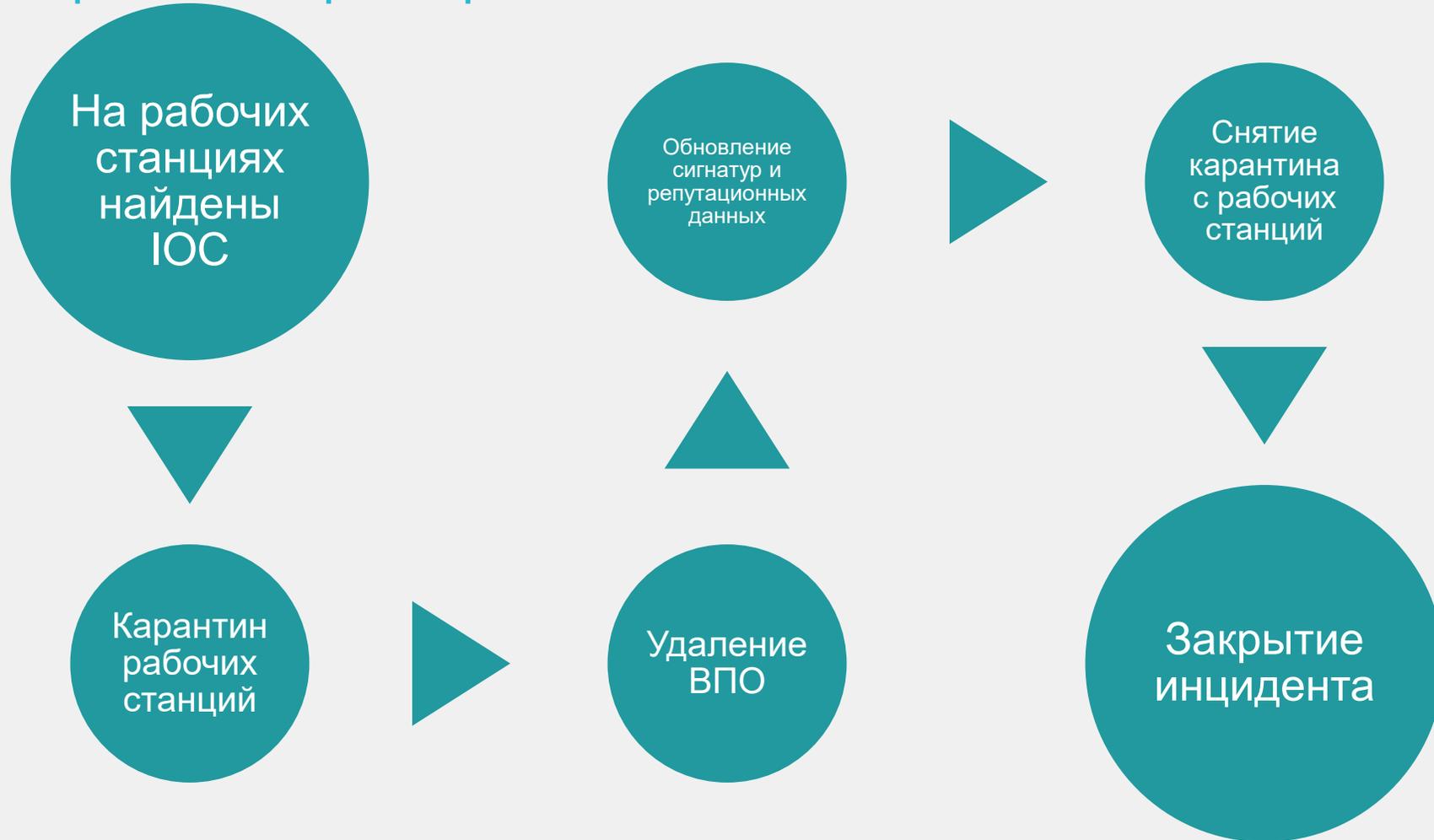
FortiXDR

Автоматизированное расследование



FortiXDR

Автоматизированное реагирование



Заключение



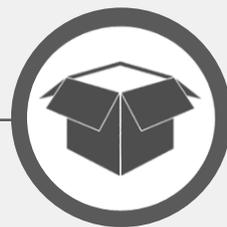
Минимизация издержек



Разведка



Вооружение



Доставка



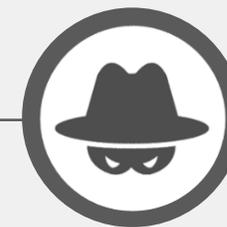
Эксплуатация



Установка



Получение управления



Выполнение действий



FortiEDR: MITRE

“The results showed that FortiEDR has:

- The ability to block 100% of the Protection tests, used by Carabank, FIN 7 and other similar campaigns; past, present and future.
- Precise tracing and assessment of granular system activity, for comprehensive detection of the techniques and tactics in the scope of evaluation as well as confident blocking at the optimal time of the campaign.
- A clear picture of conscious design principles, especially the balance between effectiveness and accuracy, valuable vs. overwhelming information.” *

* <https://www.fortinet.com/blog/business-and-technology/interpreting-mitre-evaluations-to-better-understand-endpoint-security-solutions>



FORTINET®