

DIGITAL EDITION

FORTINET[®] SECURITY DAY

**Минимизация времени обнаружения и
реагирования на кибератаки**

Кирилл Михайлов, системный инженер

6 апреля 2021 | Киев | Минск



Минимизация издержек



Разведка



Вооружение



Доставка



Эксплуатация



Установка



Получение управления



Выполнение действий



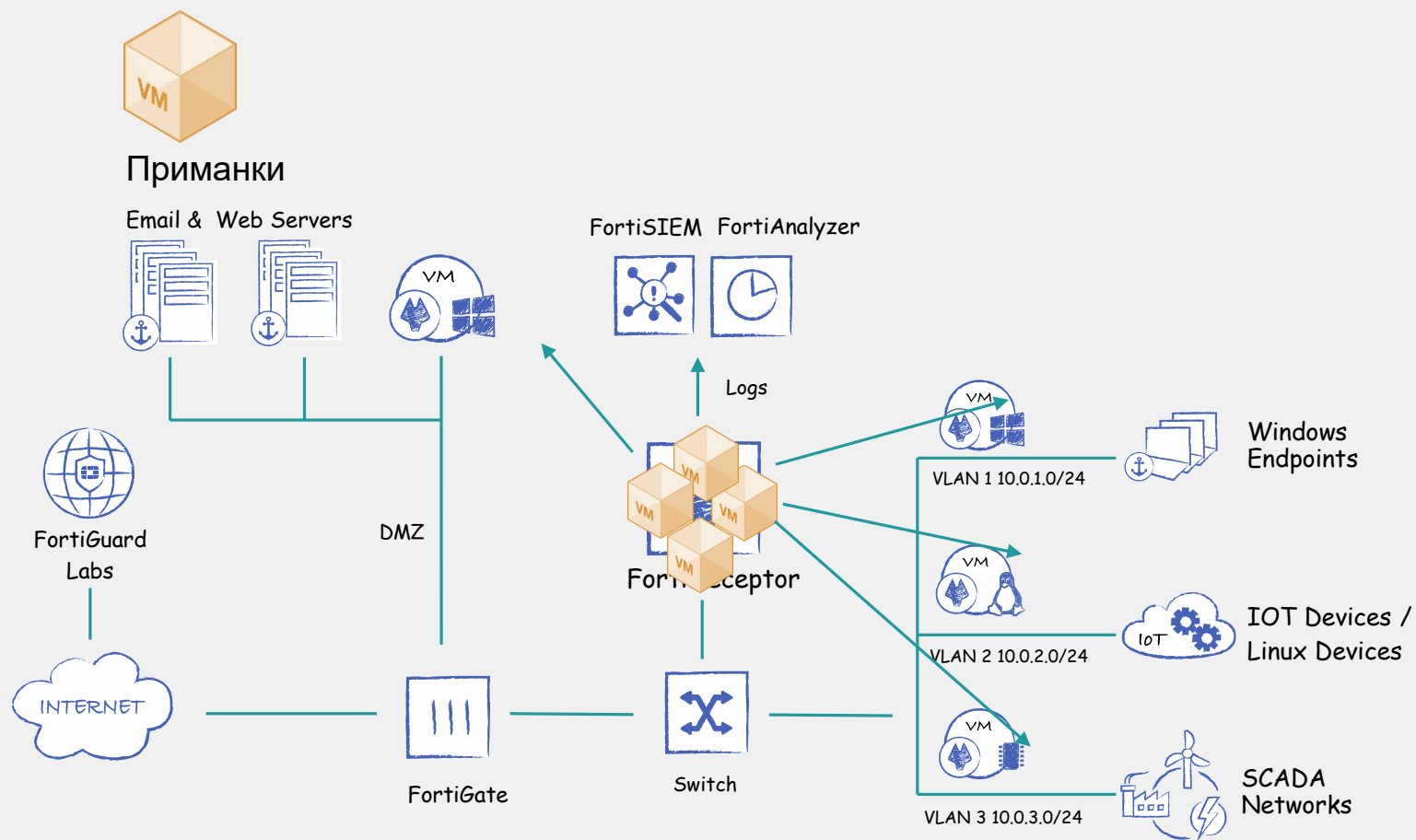


Обнаружение атаки

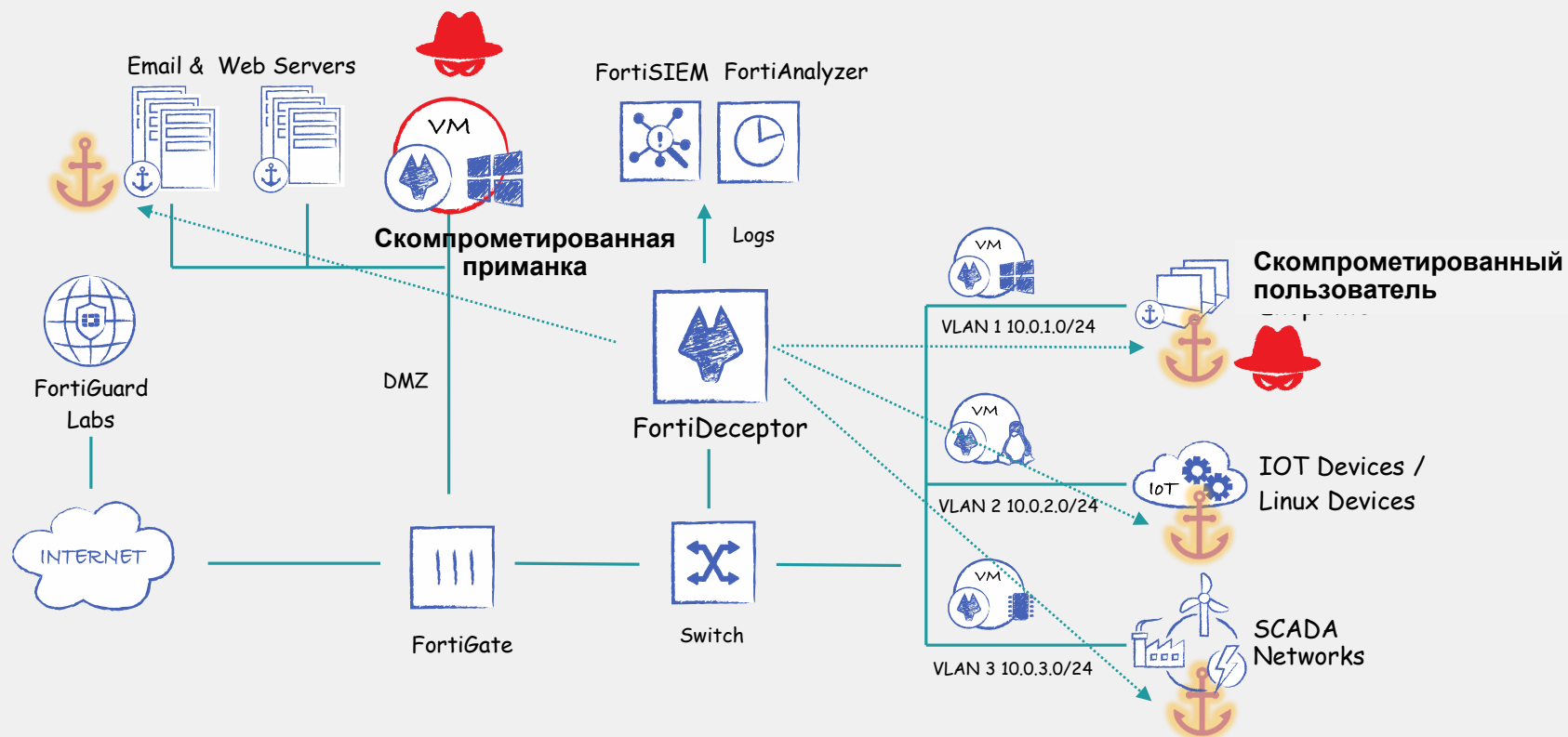
на стадии разведки



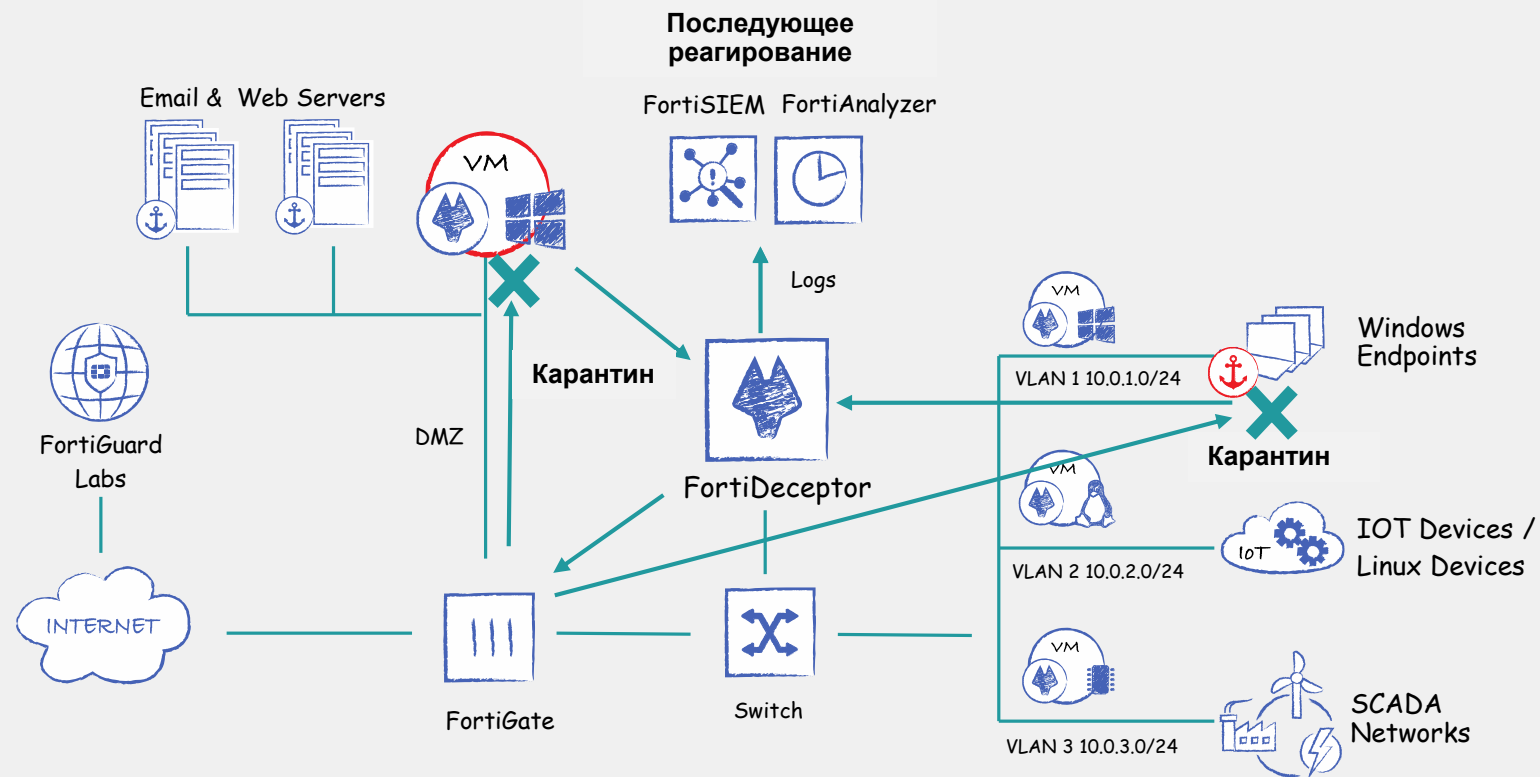
FortiDeceptor: разведка



FortiDeceptor: доставка и эксплуатация



FortiDeceptor: выполнение действий



Видимость и контроль конечных узлов



Fortinet Security Fabric



Рабочие станции / серверы



Видимость и контроль

конечных узлов



Функционал EPP



FortiClient



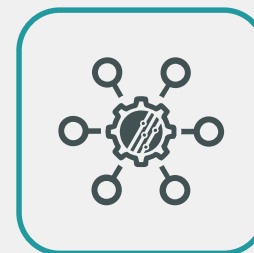
Модуль защиты от
ВПО



Модуль VPN



Модуль Compliance



Модуль интеграции со
сторонними системами

Функционал EDR



FortiEDR



Антивирусный модуль



Модуль анализа
активности

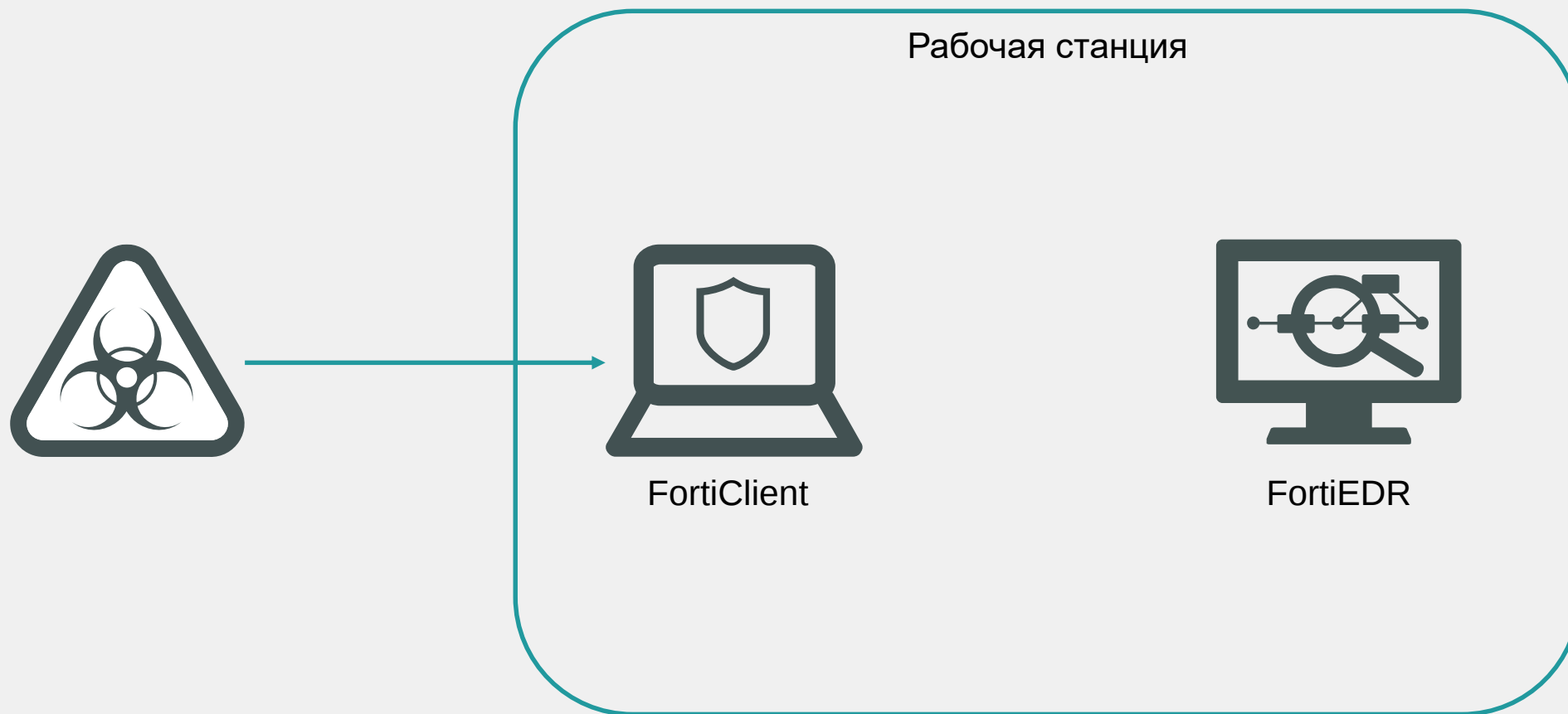


Модуль реагирования и
восстановления
системы

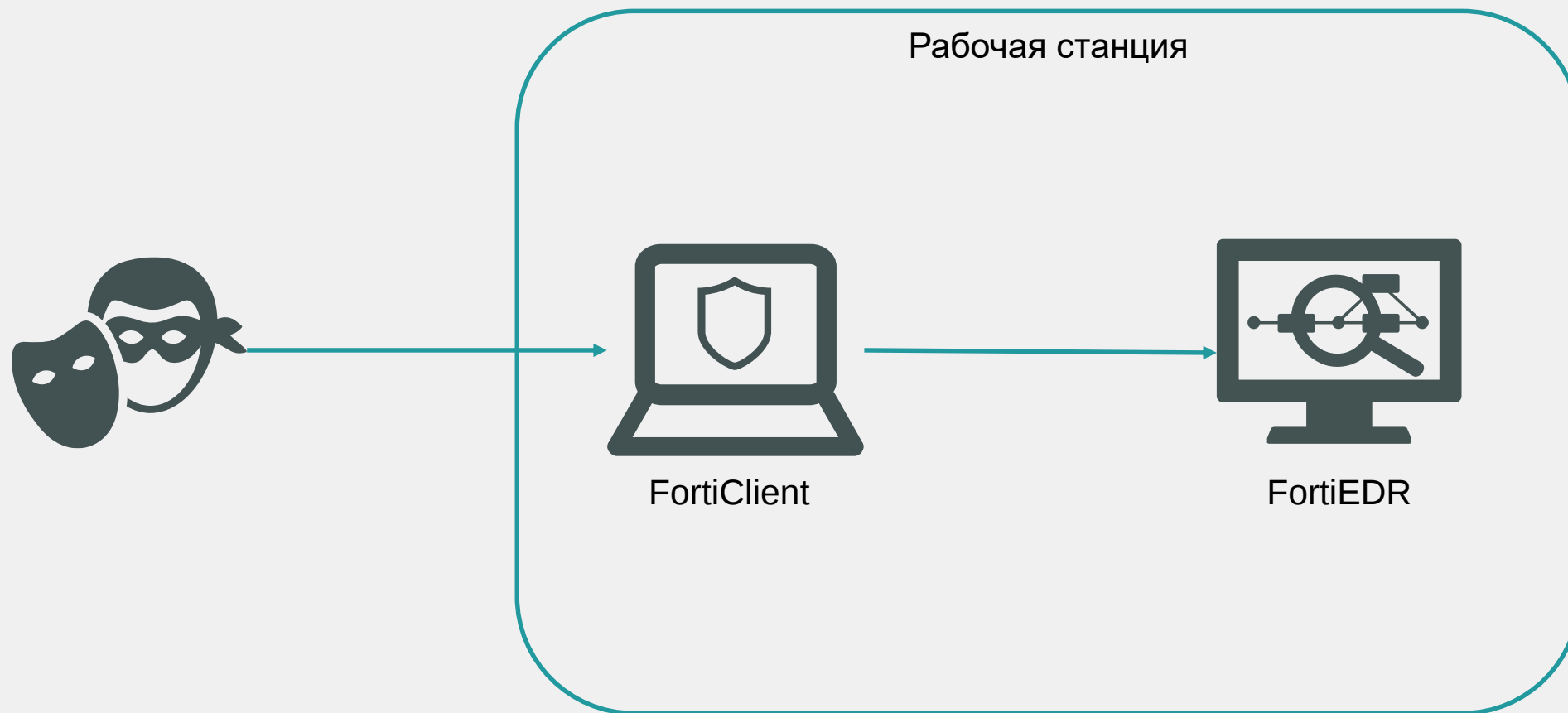


Модуль анализа и
закрытия уязвимостей

ERP: защита от известных угроз



EDR: обнаружение продвинутых атак



FortiEDR: гипотеза

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL

204

SECURITY SETTINGS

INVENTORY

ADMINISTRATION

19

Protection

kmikhaylov

APPLICATIONS

Showing 1-10/284

Search Application

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		Unknown	Critical	09-Feb-2021	20-Feb-2021
☐ 88.0.4324.190		Unknown	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

Облачная, локальная, Гибридная архитектура

Легкий агент

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



FortiEDR: блокировка

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL

204

SECURITY SETTINGS

INVENTORY

ADMINISTRATION

19

Protection

kmikhaylov

SECURITY POLICIES

Clone Policy

Set Mode

Assign Collector Group

Delete

All

	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			

Showing 1-10/19

Search

ASSIGNED COLLECTOR GROUPS

Unassign Group

☐ Kirill (1 collector included)

ADVANCED POLICY & RULE DATA

Copyright © Fortinet Version 5.0.1.200



Облачная, локальная,
Гибридная архитектура



Легкий агент

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



FortiEDR: обнаружение

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL 205

SECURITY SETTINGS

INVENTORY

ADMINISTRATION 26

Simulation

kmikhaylov

EVENTS

Archive

Mark As...

Export

Handle Event

Delete

Forensics

Exception Manager

All

ID

DEVICE

PROCESS

CLASSIFICATION

DESTINATIONS

RECEIVED

LAST UPDATED

mimilove.exe (2 events)

Malicious

07-Dec-2020, 09:34:20

wscript.exe (2 events)

Suspicious

22-Mar-2021, 15:48:03

8238402

win10-vm

vbs.vbs

Suspicious

140.82.121.4

22-Mar-2021, 15:48:03

22-Mar-2021, 15:48:03

8230755

win10-vm

1.vbs

Suspicious

140.82.121.4

22-Mar-2021, 12:04:03

22-Mar-2021, 12:04:03

mimikatz.exe (2 events)

Malicious

16-Mar-2021, 09:32:10

Logged-in User:

Process owner:

Certificate:

Process path:

Raw data items:

INTERNAL\Administrator

INTERNAL\Administrator

Signed

C:\Windows\System32\wscript.exe

1

ADVANCED DATA

Event Graph

Geo Location

Automated Analysis

Inconclusive

Fortinet on 22-Mar-2021 15:48:03

Suspicious

FortiCloudServices on 23-Mar-2021 01:58:39

Fortinet Cloud Services comment

Suspicious execution of .vbs file.

File (1)

Memory (0)

Network & Extended Data (1)

wscript.exe

SHA1

Hash reputation

542c46c652ddefc87414213a8bea0c65dd0377a9

Safe

by FortiLabs, Kaspersky, VirusTotal, FortiGuard, Reversing...

140.82.121.4

IP reputation

Inconclusive

by FortiLabs intelligence services

Copyright © Fortinet Version 5.0.1.200

Облачная, локальная,
Гибридная архитектура

Легкий агент

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

© Fortinet Inc. All Rights Reserved.

15

FortiEDR: реагирование

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL 204

SECURITY SETTINGS

INVENTORY

ADMINISTRATION

Protection

kmikhaylov

THREAT HUNTING

CATEGORYAll Categories

DEVICEAll Devices

Behavior: execution and Type: ("Process Creation") and Target.Process.Name: ("cmd.exe")

TIMELast 7 days

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

CATEGORY	TIME	OS	DEVICE NAME	TYPE	BEHAVIOR	PROCESS AND ATTRIBUTES	TARGET	EVENT ATTRIBUTES
	16-Mar-2021 09:...	win10-vm	win10-vm	Process Cr...	Execution	win10_upd_block.exe	cmd.exe	SOURCE PID 6076
	16-Mar-2021 09:...	win10-vm	win10-vm	Process Cr...	Execution	explorer.exe	cmd.exe	SOURCE PID 1820
	16-Mar-2021 09:...	win10-vm	win10-vm	Process Cr...	Execution	explorer.exe	cmd.exe	SOURCE PID 1820
	15-Mar-2021 18:...	win10-vm	win10-vm	Process Cr...	Execution	vmtoolsd.exe	cmd.exe	SOURCE PID 2832
	15-Mar-2021 17:...	win10-vm	win10-vm	Process Cr...	Execution	win10_upd_block.exe	cmd.exe	SOURCE PID 2528
	15-Mar-2021 17:...	win10-vm	win10-vm	Process Cr...	Execution	win10_upd_block.exe	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...

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

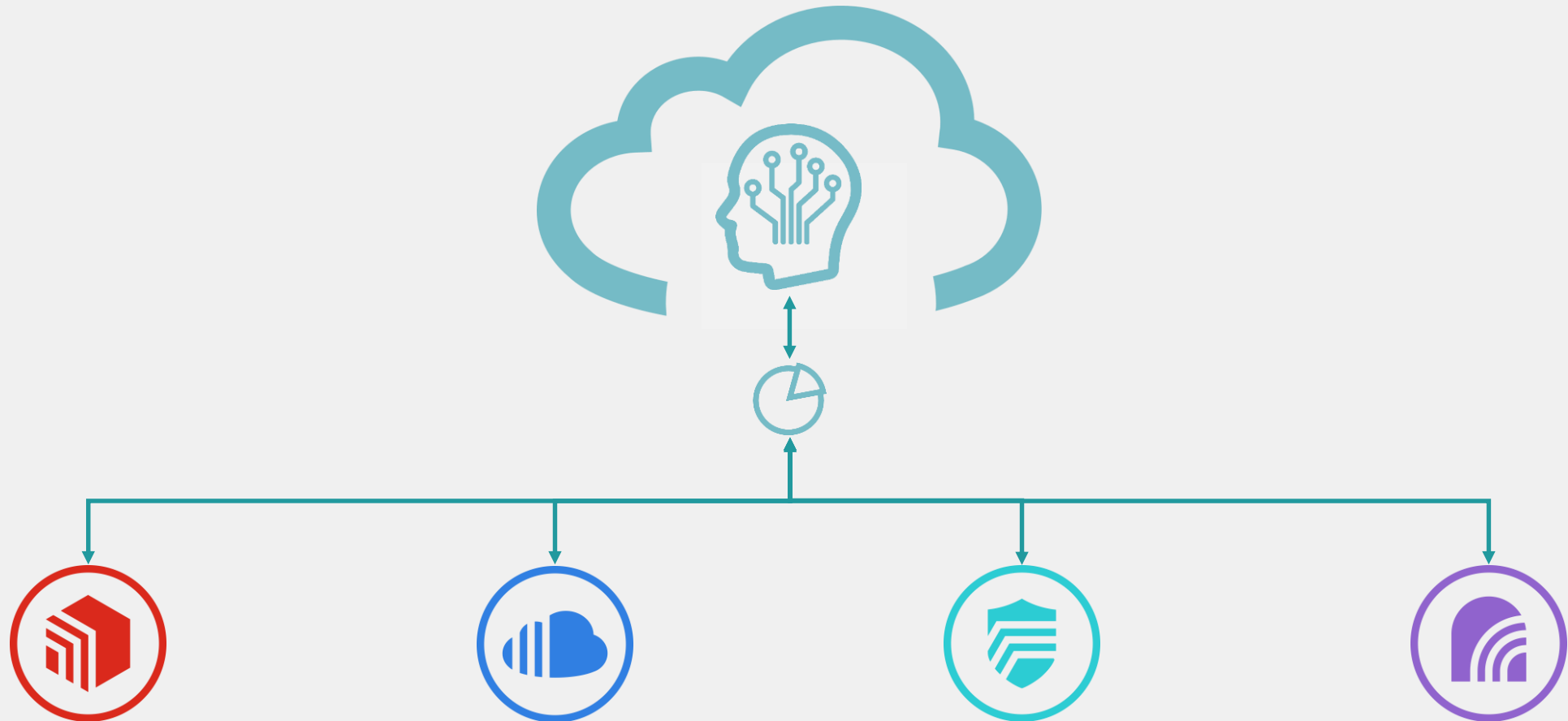


Автоматизация обнаружения

и реагирования на угрозы

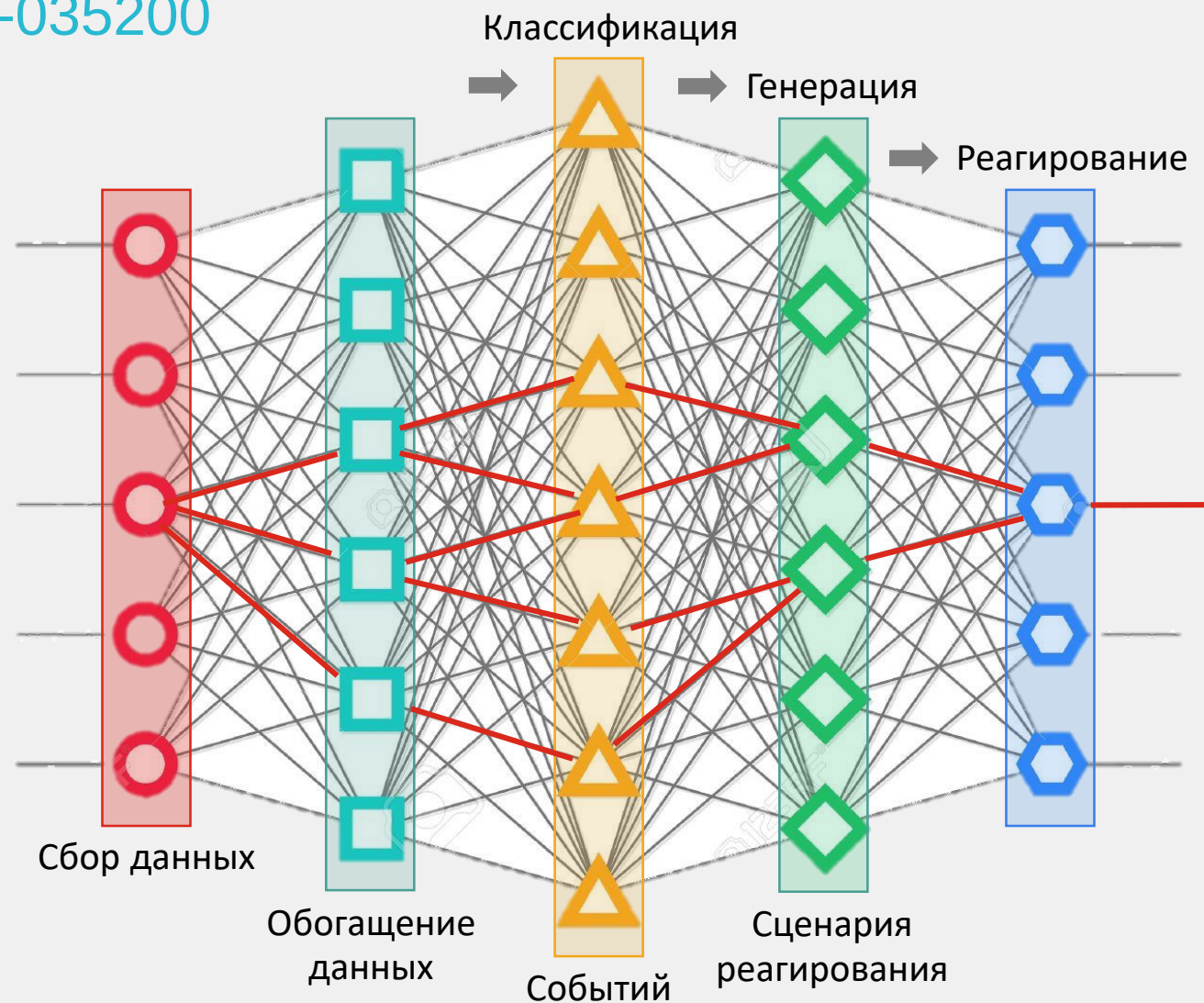


FortiXDR



FortiXDR: ANN

Патент: #FORT-035200



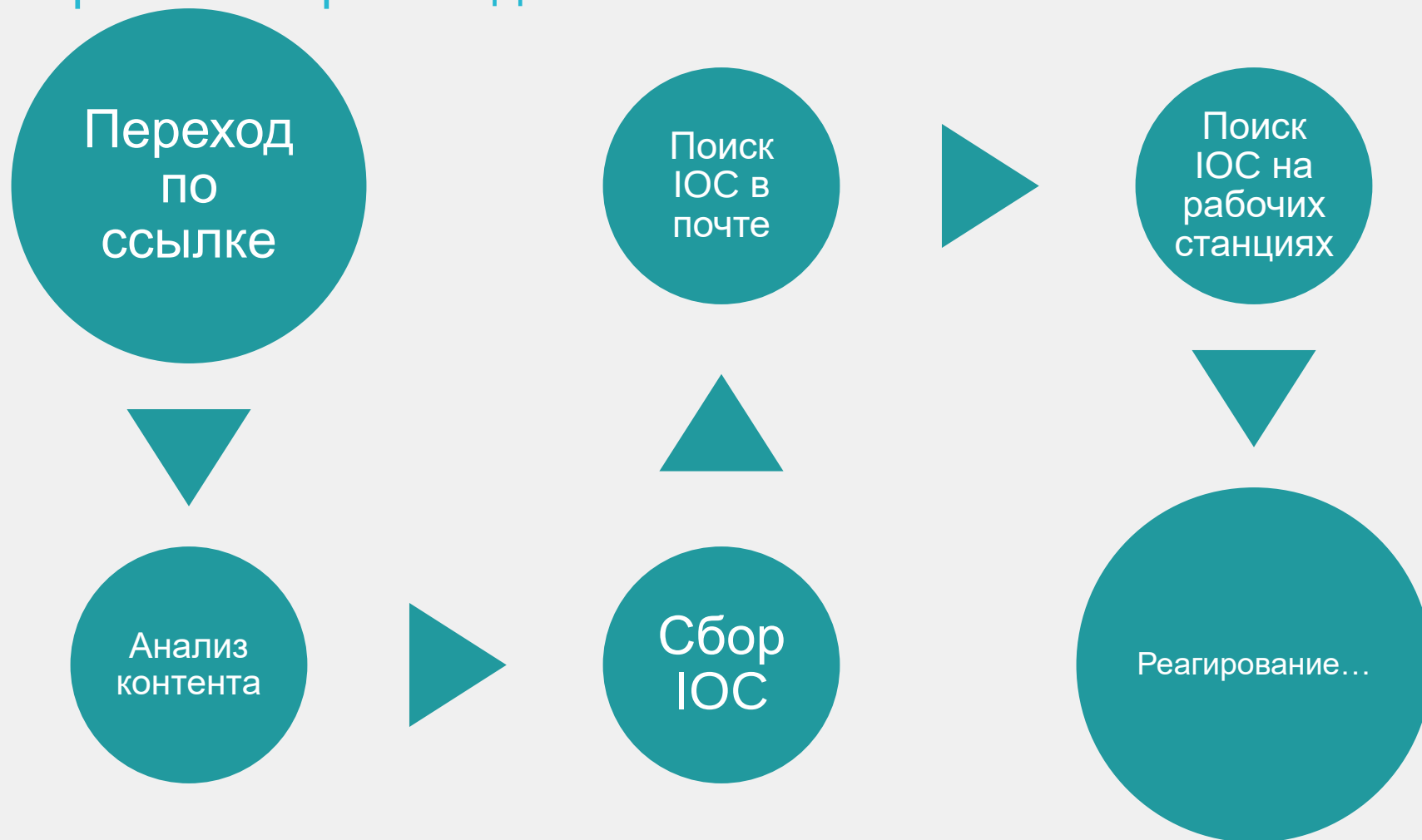
FortiXDR

Пример: целевой фишинг



FortiXDR

Автоматизированное расследование



FortiXDR

Автоматизированное реагирование



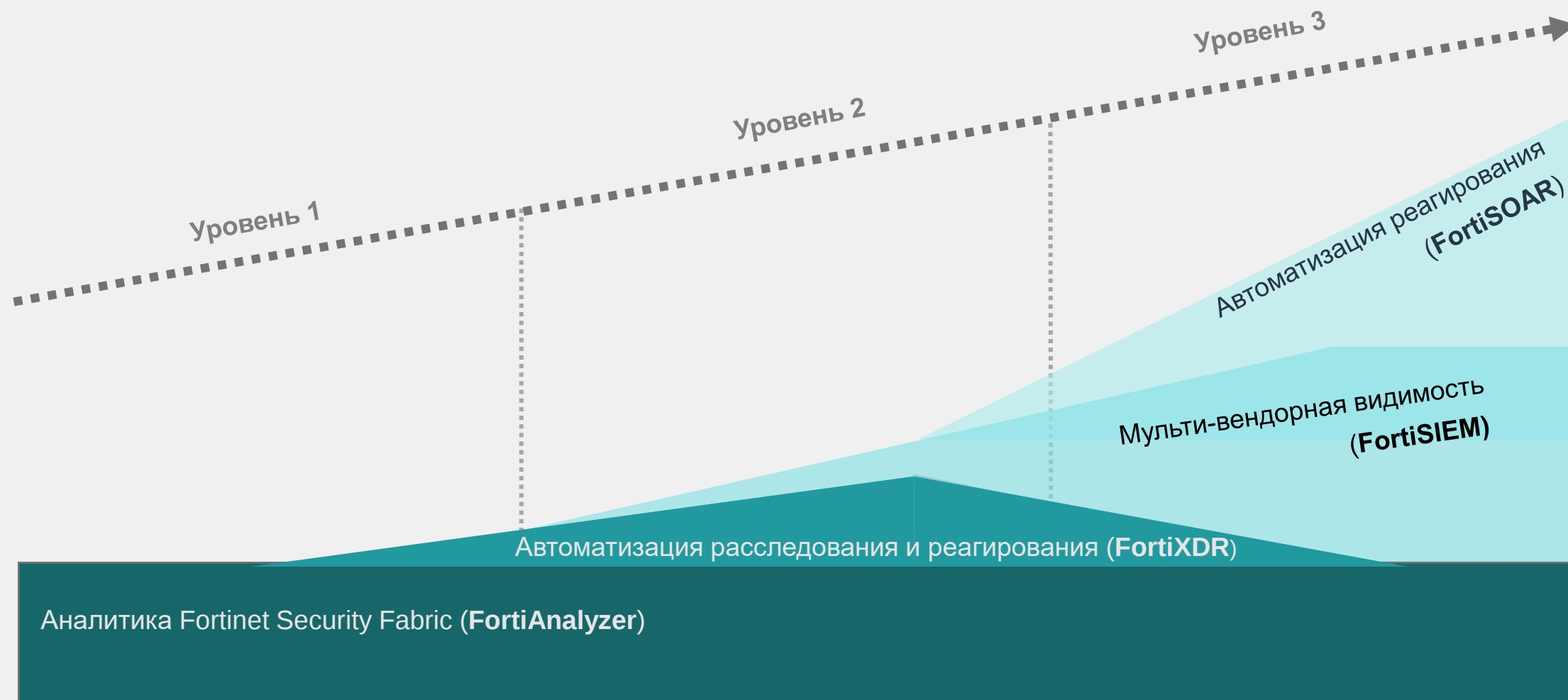


Автоматизация расследования

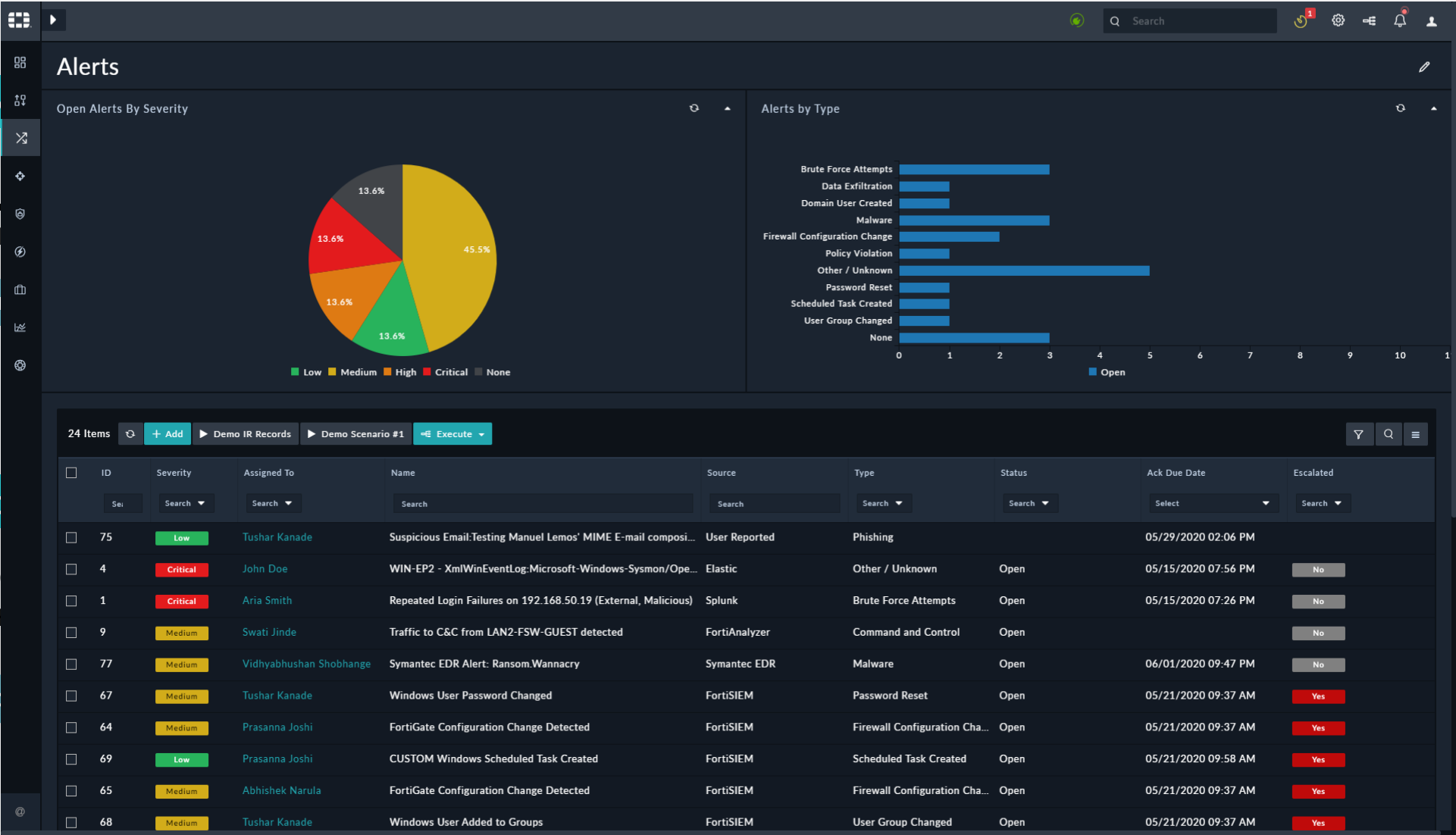
и реагирования на инциденты в мультивендорной среде



Упрощение security operations



FortiSOAR



FortiSOAR

The screenshot displays the FortiSOAR interface with a dark theme. The main window shows an alert titled 'Alert: Windows User Password Changed' with a severity of 'Medium' and ID 'Alert-67'. The alert description states 'User jack, created an account FORTIPOC/Administrator'. The alert is assigned to 'Tushar Kanade' and is currently 'Open'. The state is 'Indicator Extracted'. The type is 'Password Reset' for user 'jack' on computer 'DC1.fortipoc.test' with destination IP '10.0.1.11'. The detection date is '05/21/2020 08:57 AM' and the assigned date is '06/01/2020 01:36 PM'. The escalation status is 'Yes'. The SLA details show an acknowledgment due date of '05/21/2020 09:37 AM' and a response due date of '05/21/2020 09:47 AM', both with a status of 'Met'.

Below the alert details, there is a section for 'Indicators' with 3 items. The table lists indicators for IP Address, User, and Host, all with a reputation of 'No Reputation Available'.

Type	Reputation	Last Seen	First Seen	Value	File	Sources	Status	ID
IP Address	No Reputation Available	05/21/2020 08:58...	05/21/2020 08:57...	10.0.1.11				41
User	No Reputation Available	05/21/2020 08:58...	05/15/2020 08:49...	jack				38
Host	No Reputation Available	05/21/2020 08:58...	05/21/2020 08:57...	DC1.fortipoc.test				40

On the right side, the 'Workspace' panel shows 'Field Suggestions' and 'Similar Records'. The 'Similar Records' section lists several events, including 'Windows User Added to Groups', 'Windows User Created', 'CUSTOM Windows Scheduled Task Created', and 'FortiGate Configuration Change Detected'.



FortiSOAR



FortiSOAR

FortiSOAR™

Dashboard

Queue Management

Incident Response

- Alerts
- Incidents
- Hunts
- MITRE ATT&CK Techniq...
- Tasks
- Emails

Threat Intelligence

- Indicators
- Campaigns

Vulnerability Management

Automation

Resources

Reports

Help

FortiSOAR™ 6.4.0-1555
POWERED BY FORTINET

Incidents

Open Incidents By SeverityUnresolved Incidents By Severity By Type

22 Items

+ Add

Execute

ID	Severity	Name	Source	Type	Phase	Status	Incident Lead	Ack Due Date
22	High	Breach	Multiple Escalated Alerts		Detection	Open	Abhishek Narula	05/29/2020 09:14 PM
12	High	Suspicious eMail - Subj: ...	eMail	Phishing	Containment	In Progress	Abhishek Narula	
13	High	Suspicious eMail - Subj: ...	eMail	Phishing	Containment	In Progress	CS Admin	
10	High	Suspicious eMail - Subj: ...	eMail	Phishing	Containment	In Progress	Swati Jinde	
11	High	Suspicious eMail - Subj: ...	eMail	Phishing	Containment	In Progress	Prasanna Joshi	
9	High	Suspicious eMail - Subj: ...	eMail	Phishing	Aftermath	Resolved	Prasanna Joshi	
8	High	Suspicious eMail - Subj: ...	eMail	Phishing	Aftermath	Resolved	Prasanna Joshi	
6	High	Suspicious eMail - Subj: ...	eMail	Phishing	Aftermath	Resolved	CS Admin	
7	High	Suspicious eMail - Subj: ...	eMail	Phishing	Aftermath	Resolved	Swati Jinde	
4	Low	Password Reset		Policy Violation	Detection	In Progress	Swati Jinde	
5	High	Security Lock Compromi...		Explained Anomaly	Detection	In Progress	Abhishek Narula	
3	Critical	Sensitive Data Breach		Policy Violation	Detection	In Progress	Abhishek Narula	
2	Medium	Root Level Intrusion on ...		Root Access	Detection	Open	CS Admin	05/15/2020 07:57 PM
1	High	Phishing eMail		Phishing	Detection	In Progress	Tushar Kanade	
21	High	Malware reported on m...		Malware Outbreak	Detection	Open		05/15/2020 07:37 PM
20	High	Suspicious eMail - Subj: ...	eMail	Phishing	Containment	Resolved		
17	High	Suspicious eMail - Subj: ...	eMail	Phishing	Containment	Resolved		
18	High	Suspicious eMail - Subj: ...	eMail	Phishing	Containment	Resolved		

Инцидент

Стандартный вид

Увеличить

Оптимизация

Быстрый просмотр

Авто

Бора данных

назначение и событийности

я рисков

ия SOC

ональный SOC с зонами

тирования

FortiSOAR

Incident: IOC - Brute Force

Critical Incident-53 | IOC - Brute Force

Last Modified 05/29/2020 04:15 PM by Playbook

+ Add Tags

Aftermath

Type Details

TypeBrute Force Attempts

Source IP43.225.46.25

Target AssetLinep71

Destination IP192.168.60.172

Graph Elements

Indicators

Assets

Alerts

Vulnerabilities

Incidents

Assigned Date05/29/2020 03:45 PM

Resolved DateSelect Date

Acknowledge SLA

Ack Due Date05/29/2020 03:00 PM

Ack Date05/29/2020 02:58 PM

Ack SLAMet

Response SLA

Response Due D...05/29/2020 03:10 PM

Response Date-NA-

Response SLA--

Phase Times

Identification...05/29/2020 02:52 PM

Confirmation ...05/29/2020 03:59 PM

Containment ...05/29/2020 04:12 PM

Eradication D...05/29/2020 04:14 PM

Recovery Date05/29/2020 04:15 PM

Workspace

CommentsRecommendations

Search..

Filter By Tags ..

Account has been disabled in AD and their manager has been notified.
IP 43.225.46.25 blocked at the firewall.
2 months ago

Jared Betts
ACMECORP\rsavanna was not used to log in to any other hosts on the network and did not create any new accounts to move laterally.
2 months ago

Jared Betts
Looks like we caught it before things got worse.
CRITICAL FINDING: Those hosts should not have been accessible via the public internet, including LinEp71. Sending urgent ticket to Network team to fix the routing issue leaving internal assets exposed
Ticket: INC000314159
2 months ago

Jared Betts
Just got off the phone with Alphonse from the networking team. They have resolved the routing issue that left those hosts exposed.
Testing from my workstation and our cloud assets confirms their resolution.
2 months ago

Playbook
Requested "Incident Summary Report" available for download
[IncidentSummaryReport2020-06-11::22:21:45.pdf](#)
2 months ago

H B I S X Write Preview

Add comment here. Press Shift+Enter for new line.

+ Add Tags

Generate Incident Summary Report

Execute

Actions

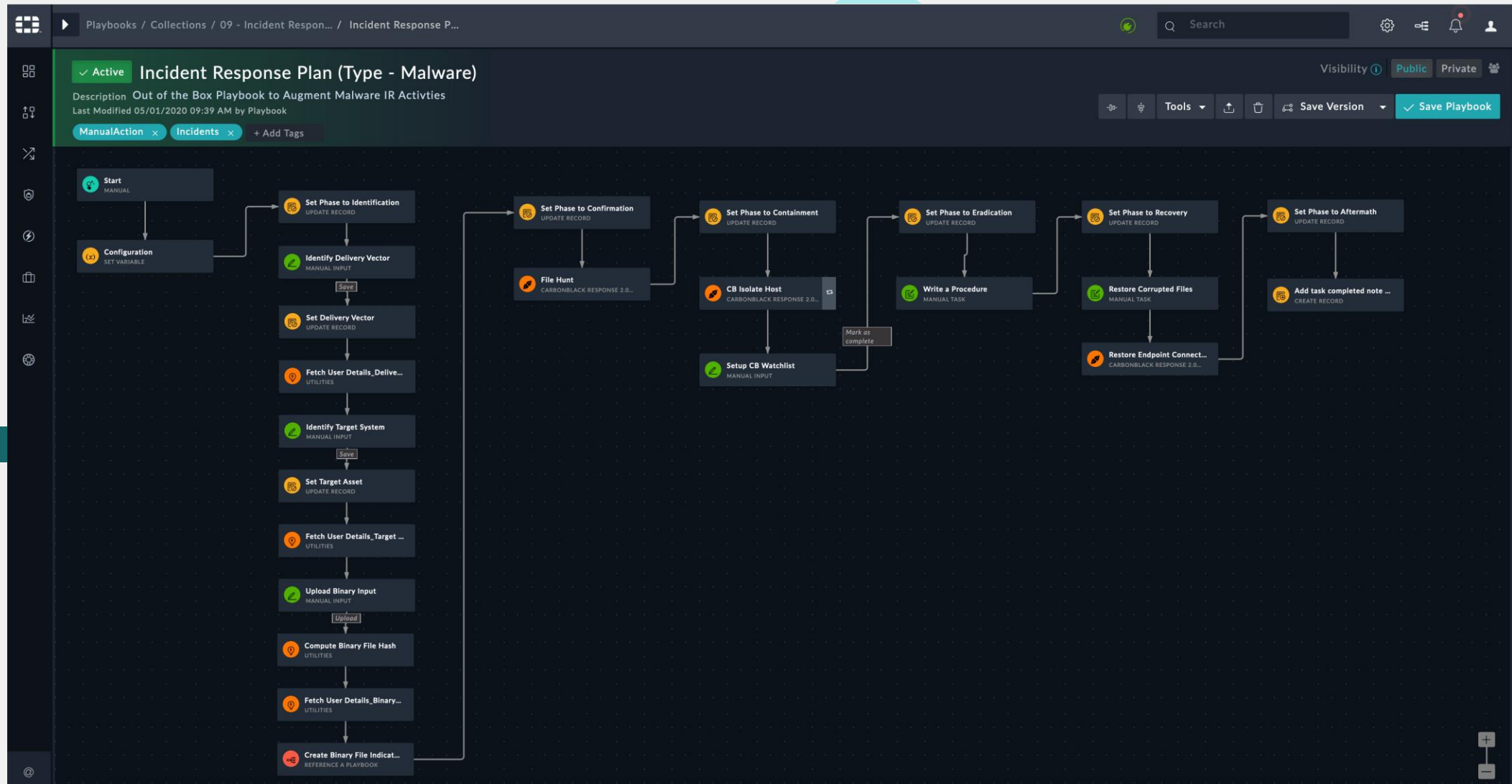
Edit Record

Export Record

Delete Record



FortiSOAR



FortiSOAR

FortiSOAR™

Playbooks / Collections / 09 - Incident Respon... / Incident Response P...

Search

41

Settings

Help

Profile

Dashboard

Queue Management

Incident Response

Vulnerability Management

Automation

Resources

Reports

Help

Connector

Back

Step Name*

+ Add Step Description

Fortinet FortiEDR

Connector Version 1.1.0

Certified: Yes

Publisher: Fortinet

DOCUMENTATION

Configuration*

FortiFabric Connector

Action*

Search Filehash

Searches a file hash among the current events, threat hunting repository, and communicating applications that exist in the Fortinet FortiEDR system.

Inputs

Filehash:*

{{vars.input.records[0].filehash}}

Step Utilities

None added

+ Variables + Loop + Condition + Message + Mock Output + Ignore Error No

Save Cancel

Dynamic Values

Expressions

modules

Incidents

@id

@type

Ack Date

Ack Due Date

Aftermath Date

Assigned Date

Type

Confirmation Date

Containment Date

Containment Time (Minutes)

Created On

Created By

Date of Incident

Delivery Vector

Description

Destination IP

Device UID

Discovered Date

Dwell Time (Minutes)

Eradication Date

File Hash

ID filehash

Identification Date

Impact Assessments

Incident Lead

Phase Infographics

Incident Summary

Metrics

Visibility

Public

Private

Tools

Save Version

Save Playbook

Set Phase to Identification

UPDATE RECORD

Identify Delivery Vector

MANUAL INPUT

Save

Set Delivery Vector

UPDATE RECORD

Fetch User Details_Delive...

UTILITIES

Identify Target System

MANUAL INPUT

Save

Set Target Asset

UPDATE RECORD

Fetch User Details_Target ...

UTILITIES

Upload Binary Input

MANUAL INPUT

Select a Step

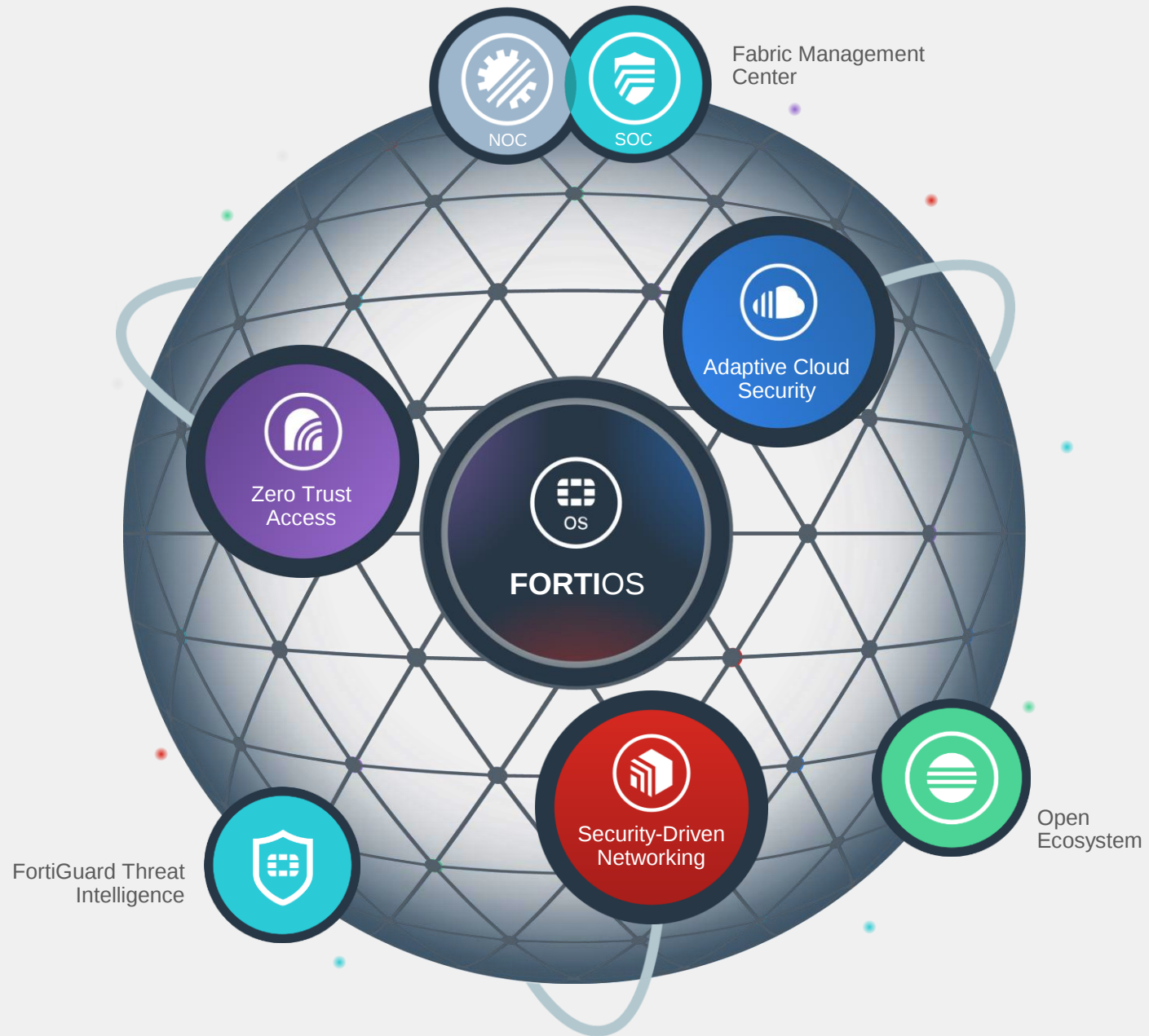
PLACEHOLDER





Заключение







FORTINET®