Кибербезопасность критически важных систем

Александр Чупрынин, системный инженер

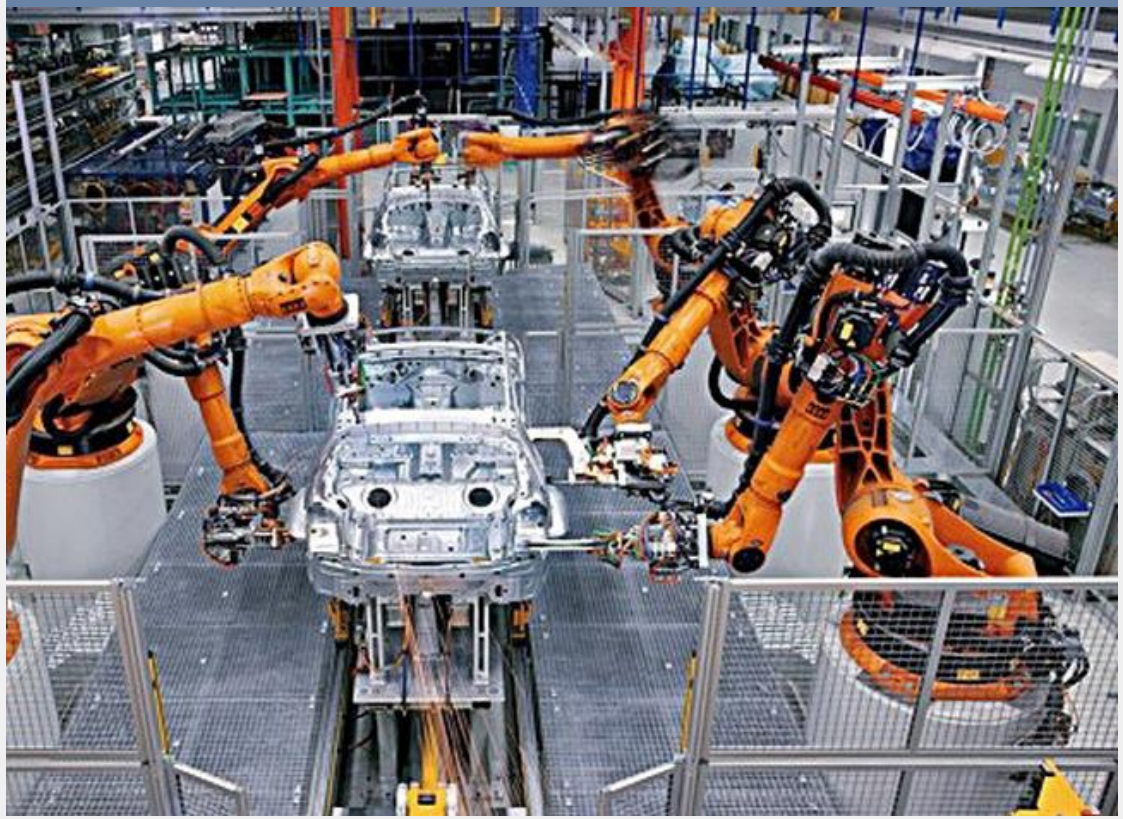
25.11.2021

Операционные технологии (OT)

Используется для…

Мониторинг, управление, работа

Индустриальная автоматизация



Операционные технологии (OT)

Применяются в …




Разнообразные отрасли
Часто «критические» инфраструктуры



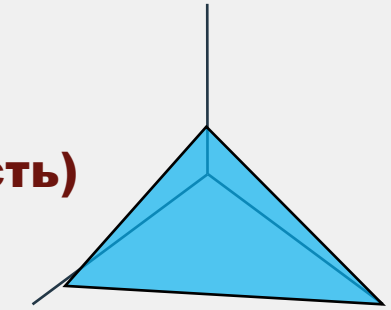

В сложных условиях эксплуатации (тепло, влажность, вибрация)

Чем отличаются IT от OT ?

IT

Конфиденциальность

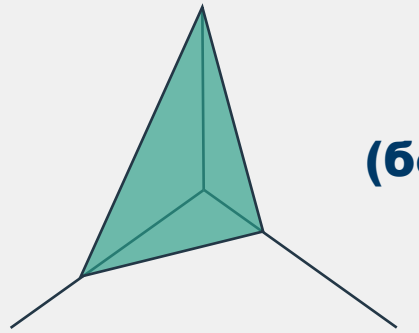
SECURITY (защищенность)



Целостность Доступность

OT

Конфиденциальность



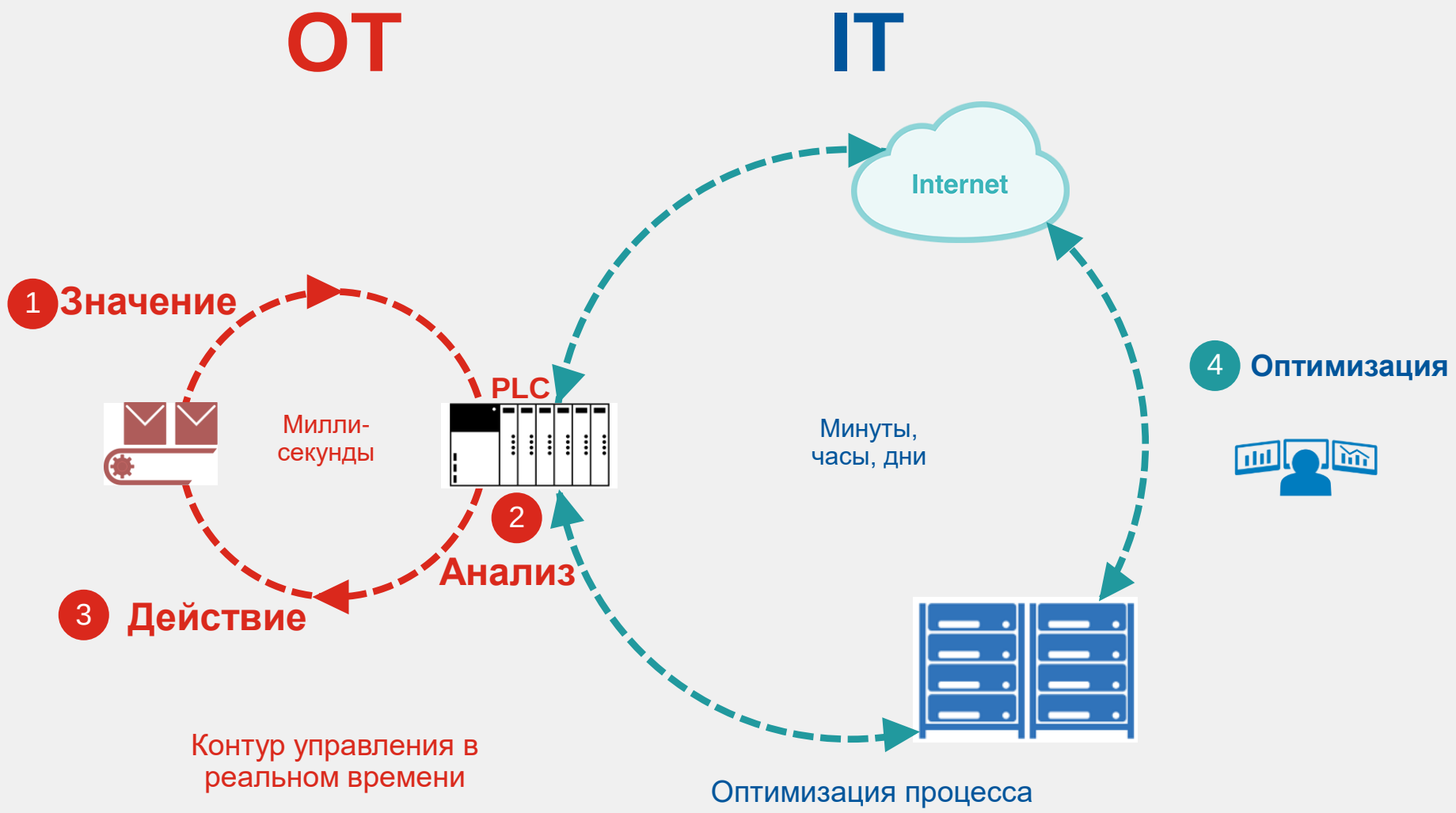
SAFETY (безопасность)

Целостность Доступность

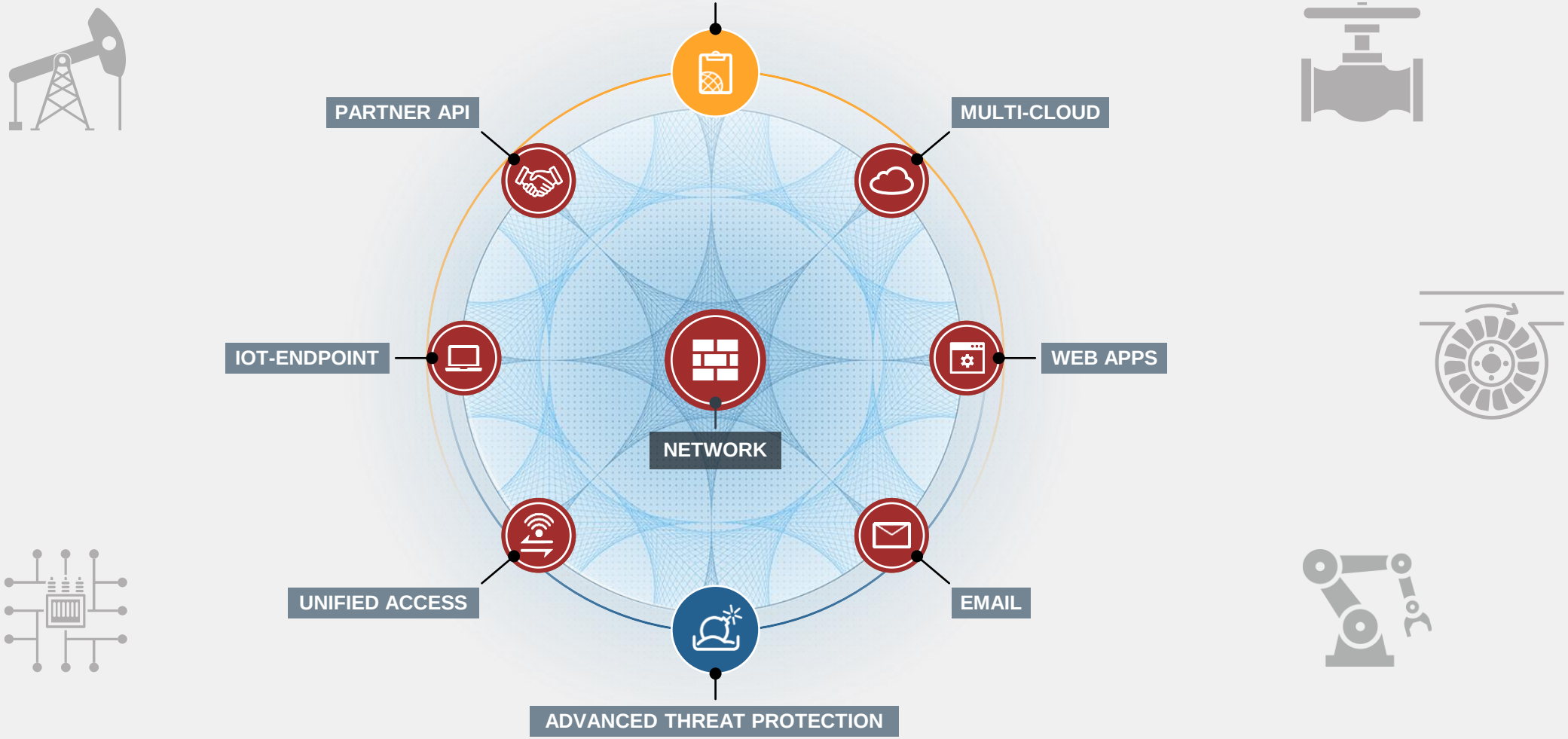
Характеристики

Приоритеты		
Средне	Конфиденциальность	Очень высокая
Допустимы задержки	Работа в реальном времени	Минимальные задержки
3-5 лет	Срок службы	до и более 20 лет
Регулярно / планово	Патчи / исправления	Осторожно / редко
Запланировано / предписано	Проверка безопасности / аудит	При случае / изредка
Высокая / зрелая	Осведомленность	Растущая

Оптимизация бизнес-процессов, способствующая конвергенции ИТ / ОТ



Fortinet Security Fabric для защиты ICS/SCADA



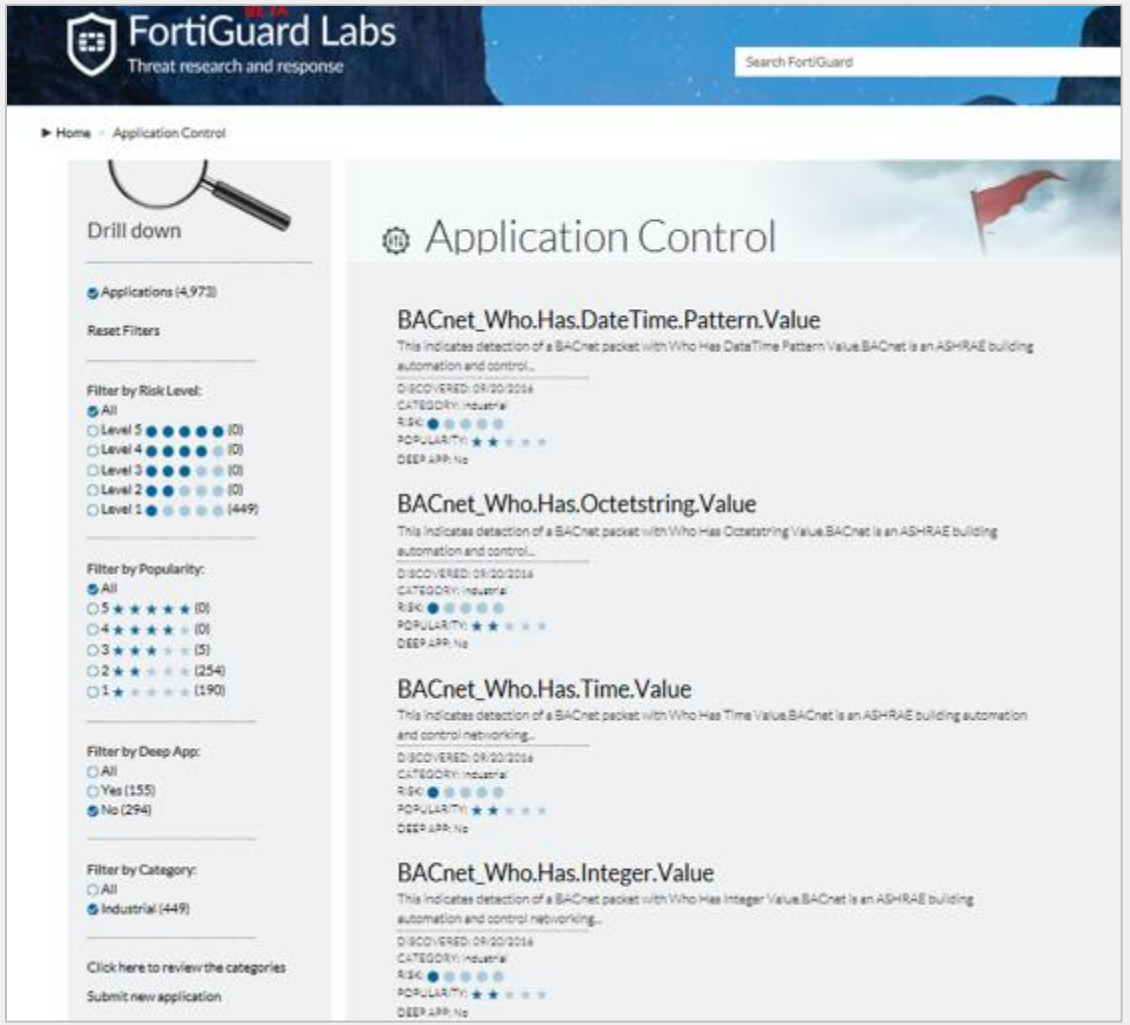
FortiGuard для OT

Специализация на OT

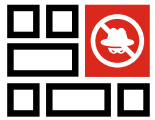
- Industrial Control Systems (ICS)
- Защита промышленных приложений
- Более 1,800 сигнатур пром. Приложений
- Поддержка игроков рынка

Control Vendors

Schneider Electric · GE · ABB · YOKOGAWA · SIEMENS · HIRSCHMANN A BELDEN BRAND · EMERSON · Rockwell Automation · Honeywell · SEL SCHWEITZER ENGINEERING LABORATORIES



Охват сервисов промышленной безопасности



Поддерживаемые протоколы ICS / OT - контроль приложений и сигнатуры IPS

• ADDP	• EtherCAT Automation Protocol (EAP)	• IEC 62056 (DLMS/COSEM)	• OPC UA
• BACnet	• Ethernet Global Data (EGD)	• IEEE 1278.2 Distributed Interactive Simulation	• OpenADR
• CC-Link	• EtherNet/IP	• IEEE C37.118 Synchrophasor	• PROFINET
• CIP	• FL-net	• KNXnet/IP (EIBnet/IP)	• RTPS
• CN/IP (EIA/CEA-852)	• HART-IP	• LonTalk/EIA-709.1	• SafetyNet p
• CoAP	• HL7	• Modbus TCP	• Siemens S7, S7Plus, LOGO
• DICOM	• IEC 60870-5-104	• MOXA	• STANAG 4406
• DNP3	• IEC 60870-6 (TASE.2/ICCP)	• MQTT	• STANAG 5066
• ECHONET Lite	• IEC 61850 MMS	• MTConnect	• TriStation
• ELCOM 90	• IEC 61850 R-GOOSE	• Niagara Fox	• Vedeer-Root
• Ether-S-Bus	• IEC 61850 R-SV	• OPC Classic (DA, HDA, AE)	

Возможности :

- Идентификация протоколов ICS / OT.
- Идентификация функций (команд) протоколов
- Глубокая проверка пакетов (DPI) - идентификация параметров в командах, чтобы обеспечить детальный контроль над полезной нагрузкой протокола ICS.

IPS/ Application Control для индустриальных систем

Гранулярный контроль протоколов и приложений (DNP3 пример)

- DNP3
- DNP3_Assign.Class
- DNP3_Cold.Restart
- DNP3_Confirm
- DNP3_Delay.Measurement
- DNP3_Direct.Operate
- DNP3_Direct.Operate.Without.Ack
- DNP3_Disable.Spontaneous.Messages
- DNP3_Enable.Spontaneous.Messages
- DNP3_Freeze.And.Clear
- DNP3_Freeze.And.Clear.Without.Ack
- DNP3_Freeze.With.Time
- DNP3_Freeze.With.Time.Without.Ack
- DNP3_Immediate.Freeze
- DNP3_Immediate.Freeze.Without.Ack
- DNP3_Initialize.Application
- DNP3_Initialize.Data
- DNP3_Operate
- DNP3_Read
- DNP3_Response
- DNP3_Save.Configuration
- DNP3_Select
- DNP3_Start.Application
- DNP3_Stop.Application
- DNP3_Unsolicited.Message
- DNP3_Warm.Restart
- DNP3_Write

IPS/ Application Control для индустриальных систем

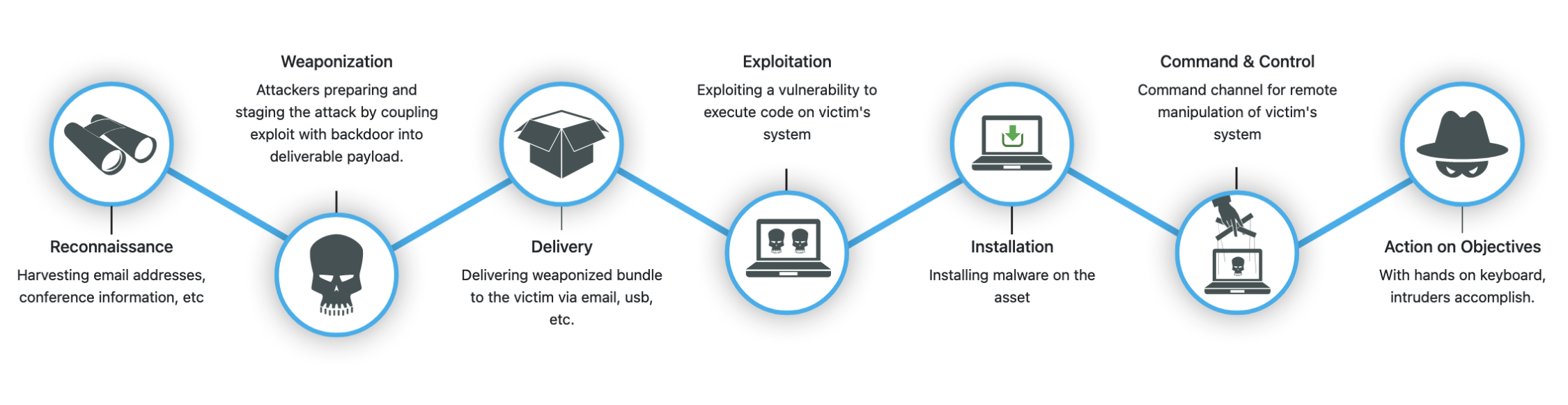
Уязвимости (Schneider Electric пример)

- Schneider.ClearSCADA.OPF.File.Parsing.Out.of.Bounds.Array.Index (CVE-2014-0779)
- Schneider.ClearSCADA.Remote.Authentication.Bypass
- Schneider.Electric.Accutech.Manager.SQL.Injection
- Schneider.Electric.DTM.development.kit.Buffer.Overflow (CVE-2014-9200)
- Schneider.Electric.GP-Pro.EX.ParseAPI.Heap.Buffer.Overflow
- Schneider.Electric.InduSoftWebStudioAgent.Remote.Code.Execution (CVE-2015- 7374)
- Schneider.Electric.Interactive.Graphical.SCADA.Buffer.Overflow (CVE-2013-0657)
- Schneider.Electric.OSF.Configuration.File.Buffer.Overflow (CVE-2014-0774)
- Schneider.Electric.Pelco.DSNVs.Rvctl.RVControl.Buffer.Overflow (CVE-2015-0982)
- Schneider.Electric.ProClima.Atx45.ocx.ActiveX.Access (CVE-2014-8511, CVE-2014-8512)
- Schneider.Electric.ProClima.MDraw30.ocx.ActiveX.Access (CVE-2014-8513, CVE-2014-9188)
- Schneider.Electric.ProClima.MetaDraw.Buffer.Overflow (CVE-2014-8514)
- Schneider.Electric.SCADA.Expert.ClearSCADA.XSS (CVE-2014-5411)
- Schneider.Electric.VAMPSET.CFG.File.Handling.Buffer.Overflow (CVE-2014-8390)
- Schneider.Modicon.M340.Password.Buffer.Overflow (CVE-2015-7937)
- Schneider.Quantum.Module.Backdoor.Access (CVE-2011-4859)
- Schneider.SCADA.Expert.ClearSCADA.Authentication.Bypass (CVE-2014-5412)
- SchneiderElectric.ProClima.F1BookView.Memory.Corruption (CVE-2015-7918,
  CVE-2015-8561)
- SearchBlox.File.Exfiltration (CVE-2015-7919)
- Sielco.Sistemi.Winlog.File.Access.Directory.Traversal (CVE-2012-4356)
- Siemens.0day.40142
- Siemens.ALM.almaxcx.dll.ActiveX.Arbitrary.File.Overwrite (CVE-2011-4532)
- Siemens.Automation.License.Manager.DoS (CVE-2011-4529, CVE-2011-4531)
- Siemens.S7300.Hardcoded.Credentials.Security.Bypass
- Siemens.Simatic.WinCC.Default.Password (CVE-2010-2772)
- Siemens.SIMATIC.WinCC.Flexible.HmiLoad.Multiple.Vulnerabilities (CVE-2011-4877)
- Siemens.SIMATIC.WinCC.Flexible.miniweb.DoS (CVE-2011-4879)
- Siemens.Tecnomatix.FactoryLink.Multiple.Vulnerabilities

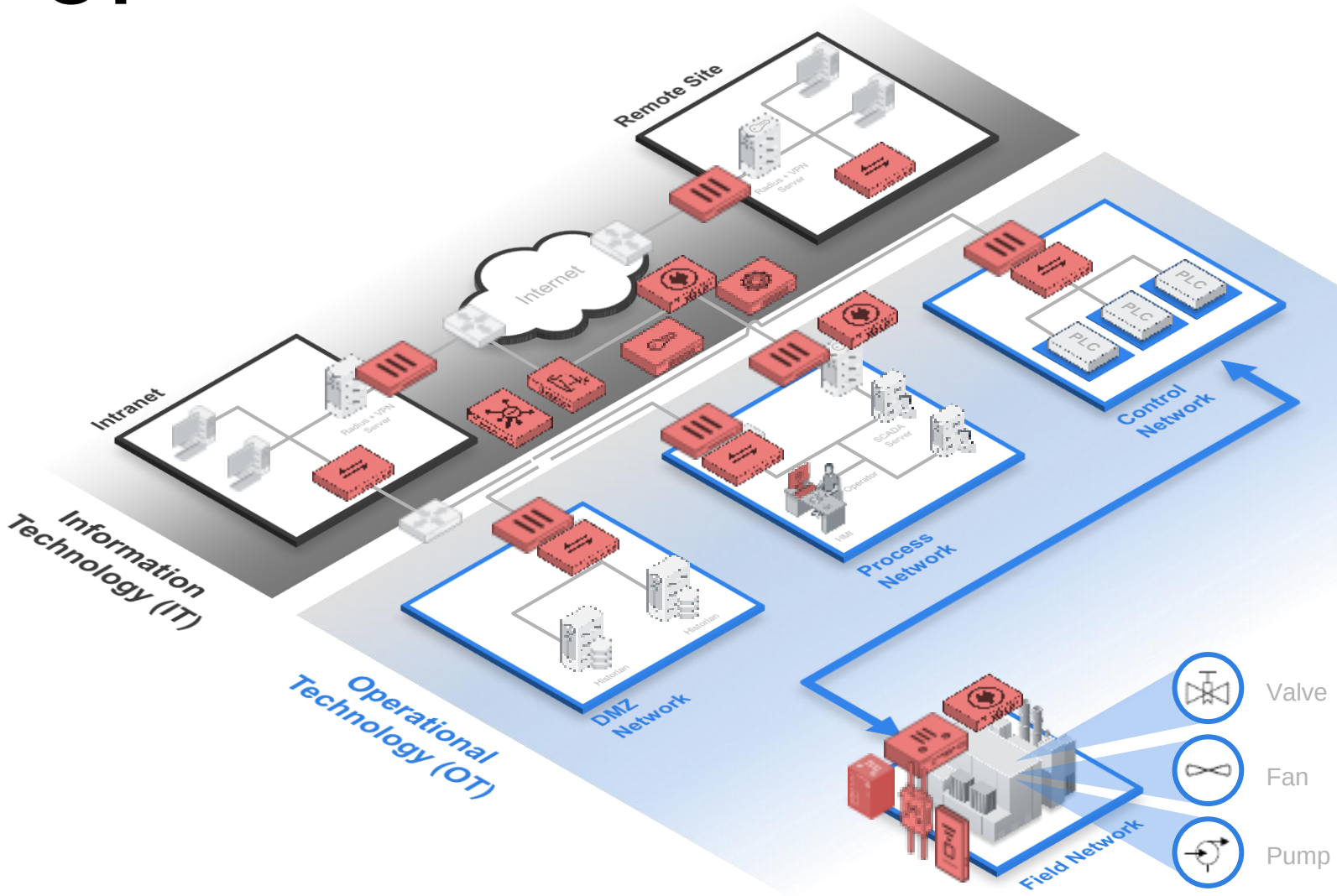
Какие решения Fortinet использовать для защиты ОТ ?

Кто атакует?

Cyber Kill Chain (APT) – дорожная карта злоумышленника



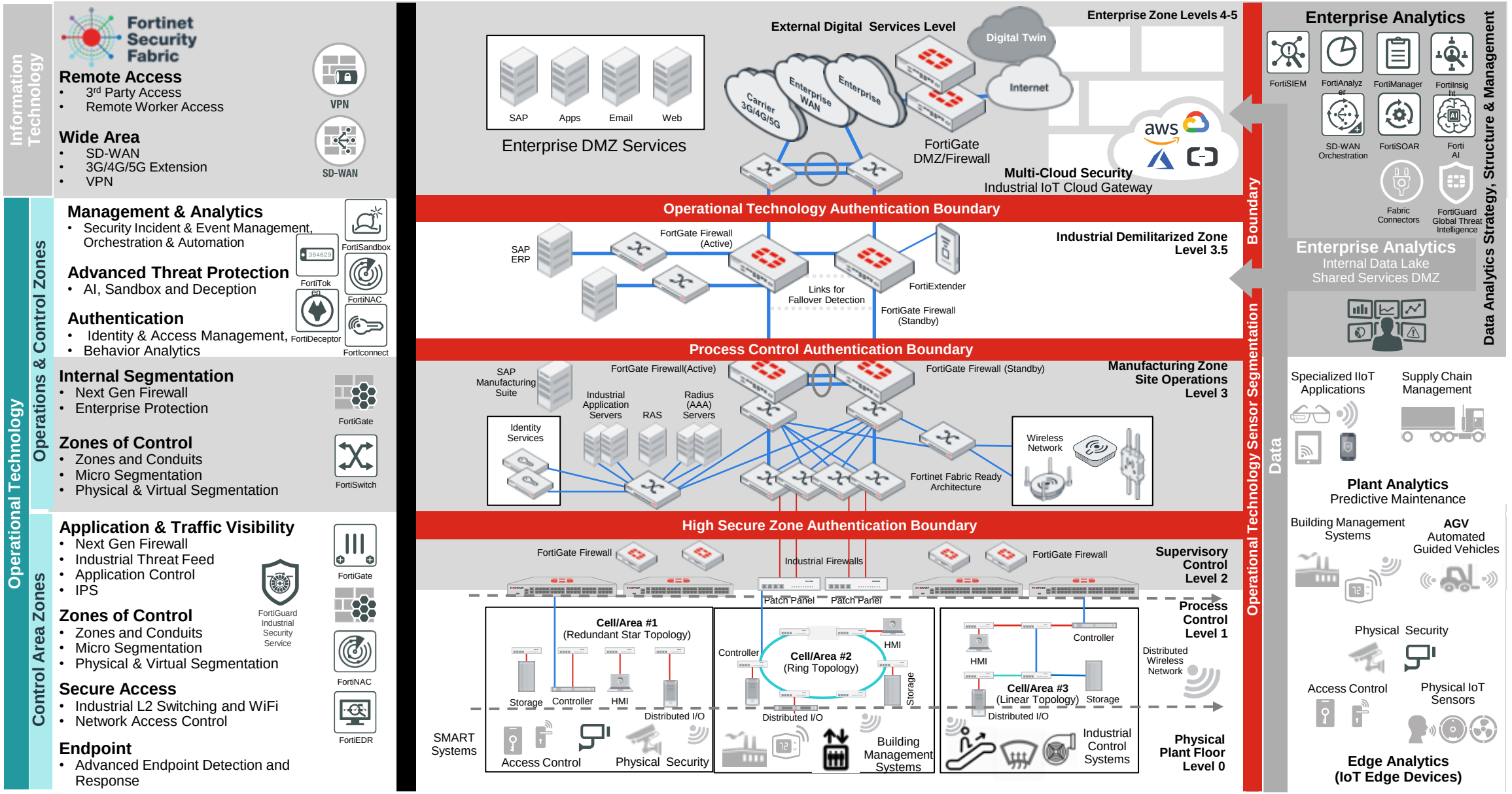
Примеры применений решений Fortinet для защиты ОТ



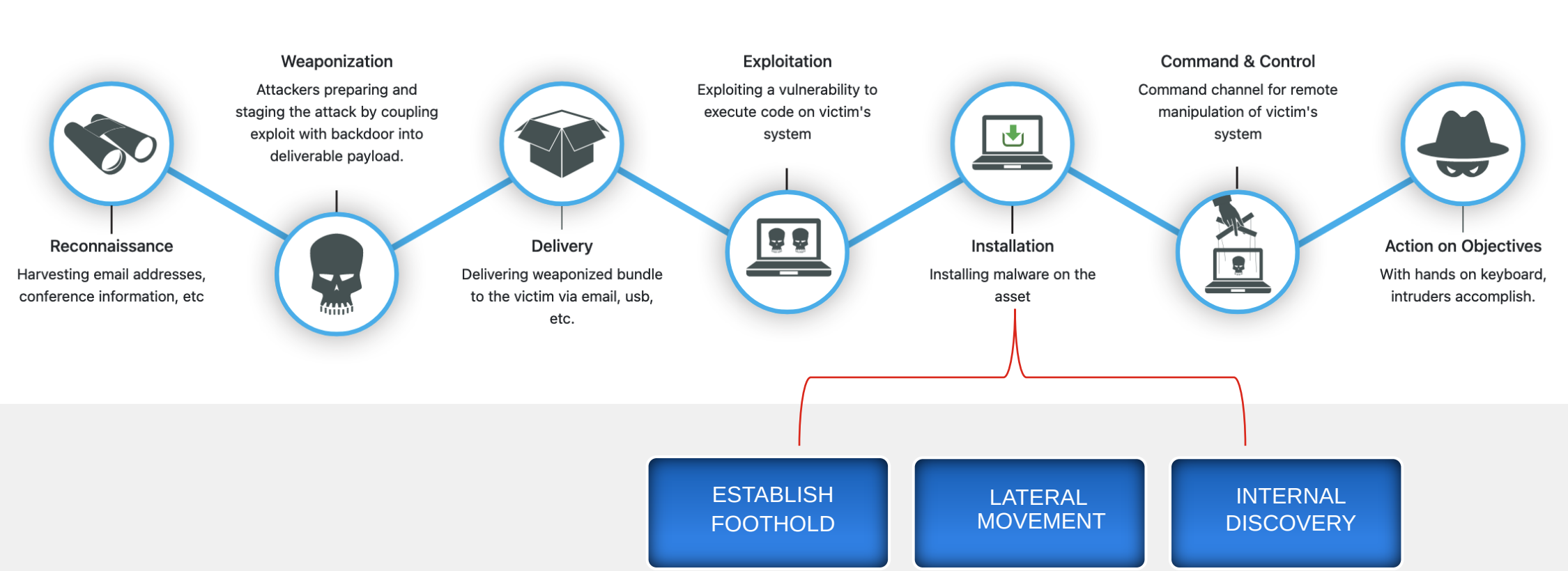
- Сегментация / Шифрованные соединения / IDS/IPS (FortiGate)
- Контроль доступа – Пользователи, Устройства, Приложения и протоколы (FortiGate, FortiAuthenticator, FortiNAC)
- Безопасный доступ в сеть (FortiSwitch/FortiAP/FortiExtender)
- Управление уязвимостями и патч-менеджмент (FortiWeb/FortiClient/FortiEDR/FortiGate)
- Защита от 0-Day атак с помощью FortiSandbox, FortiAI
- Сбор логов, корреляция и аудит и автоматическое реагирование (FortiAnalyzer, FortiSIEM/FortiSOAR)
- Автоматизация выявления нарушителя и реагирование (FortiDeceptor)

Расширенная архитектура Purdue INDUSTRIAL

На основе стандартного подхода и решения Fortinet Security Fabric



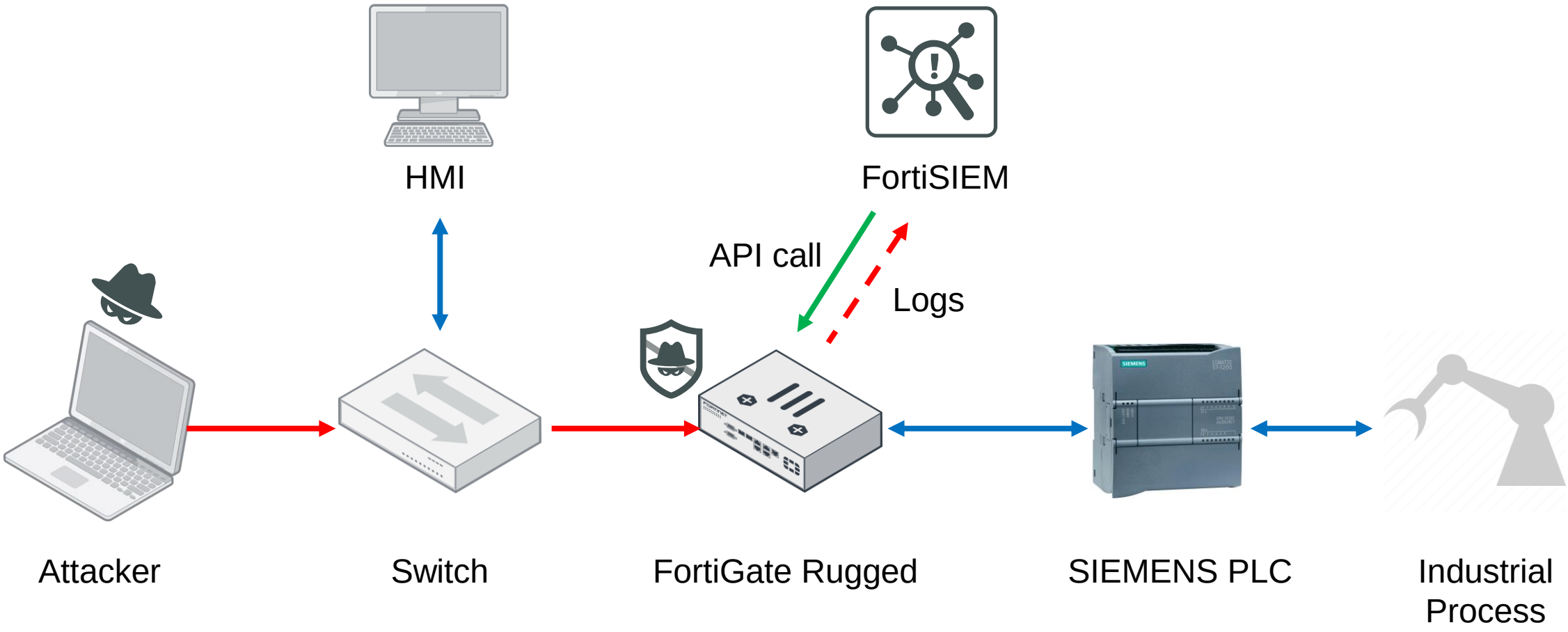
Cyber Kill Chain (APT)



FortiSIEM

Мониторинг, обнаружение и разрушение атаки

Пример OT сети



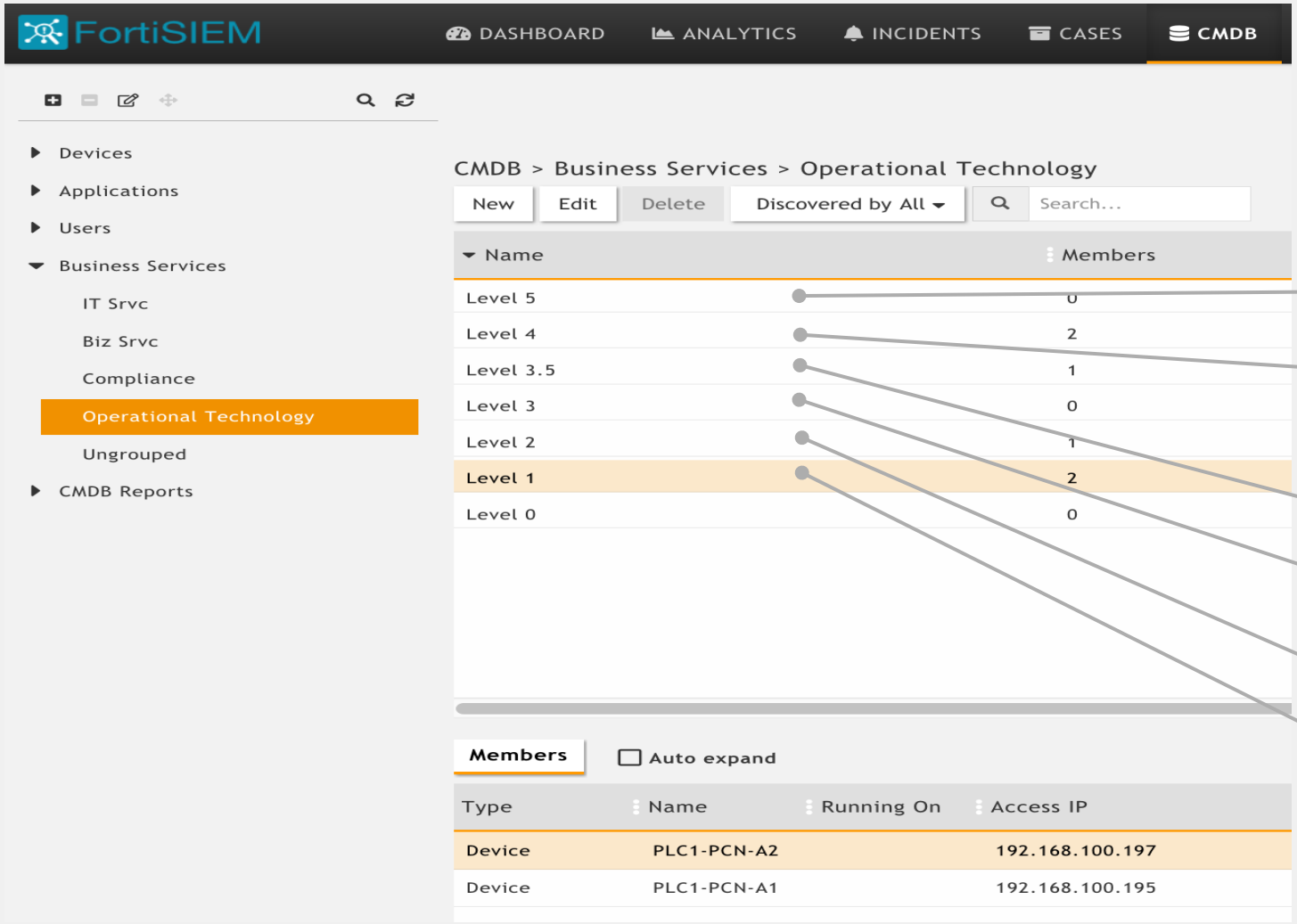
Модель Пердью

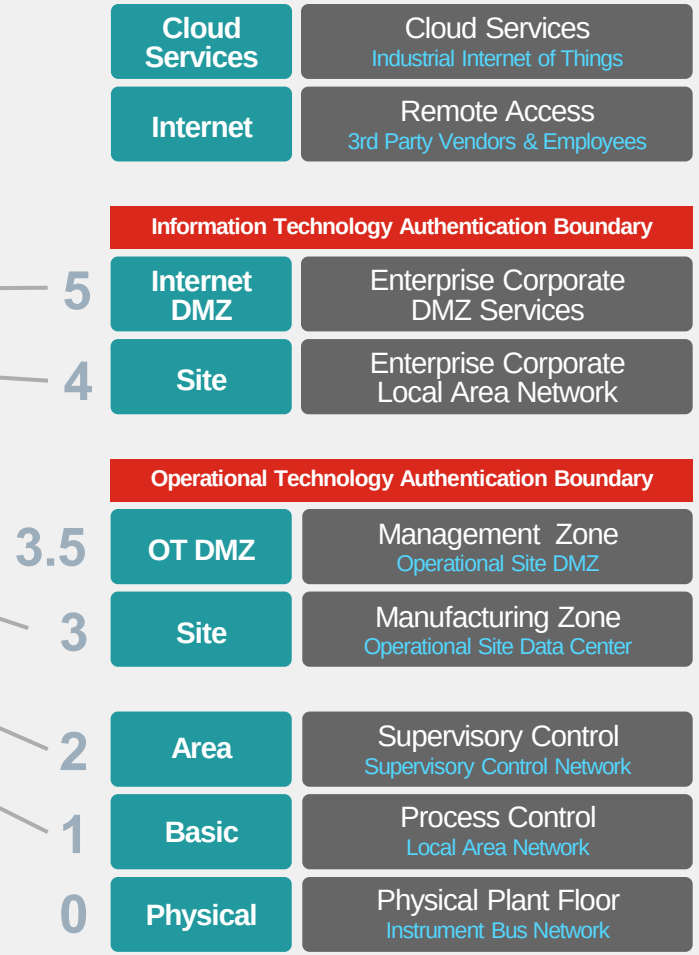
Digital Assets

Enforcement Boundaries

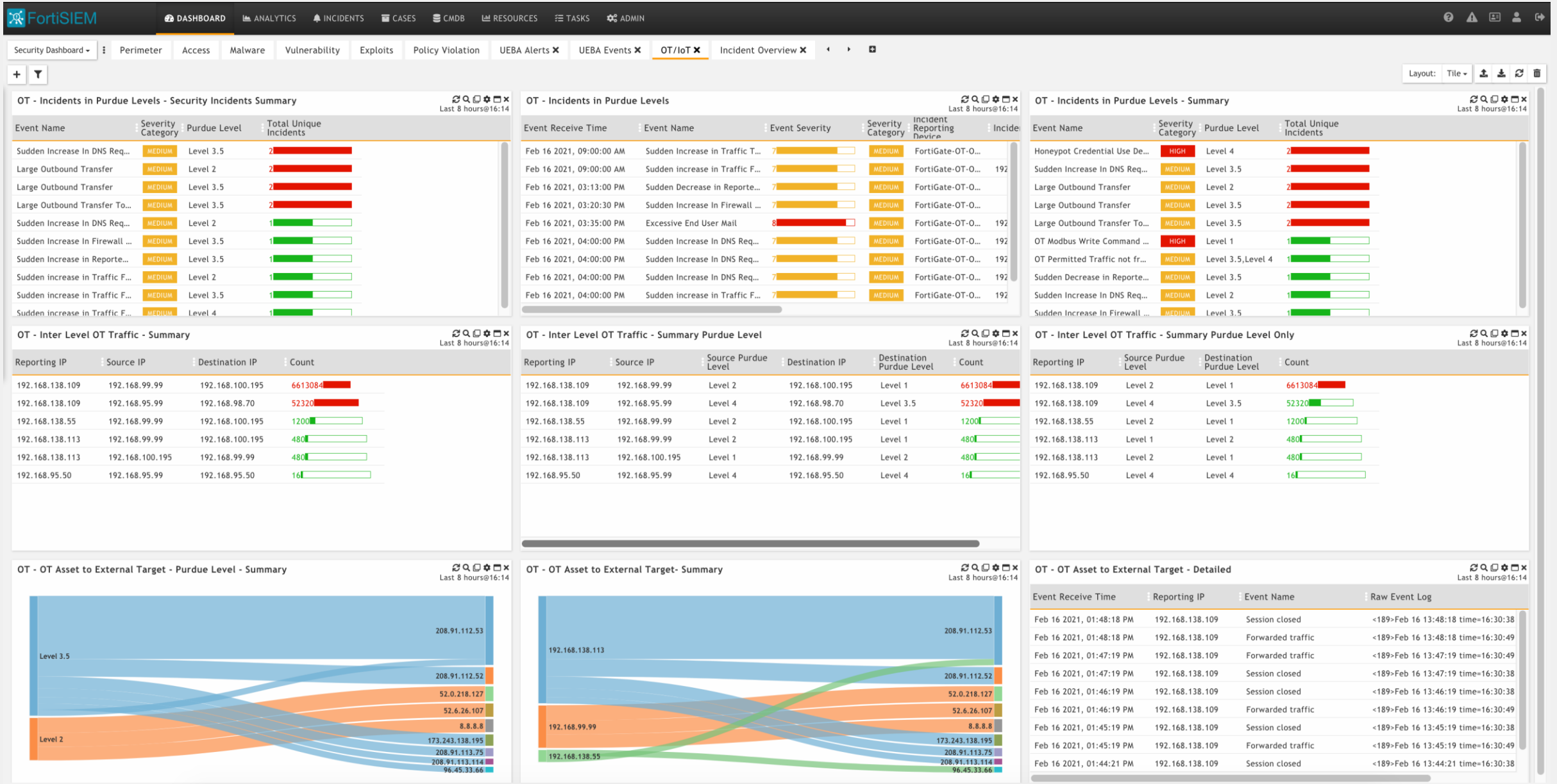
Моделируйте Вашу инфраструктуру

Маппинг устройств к уровню Пердью

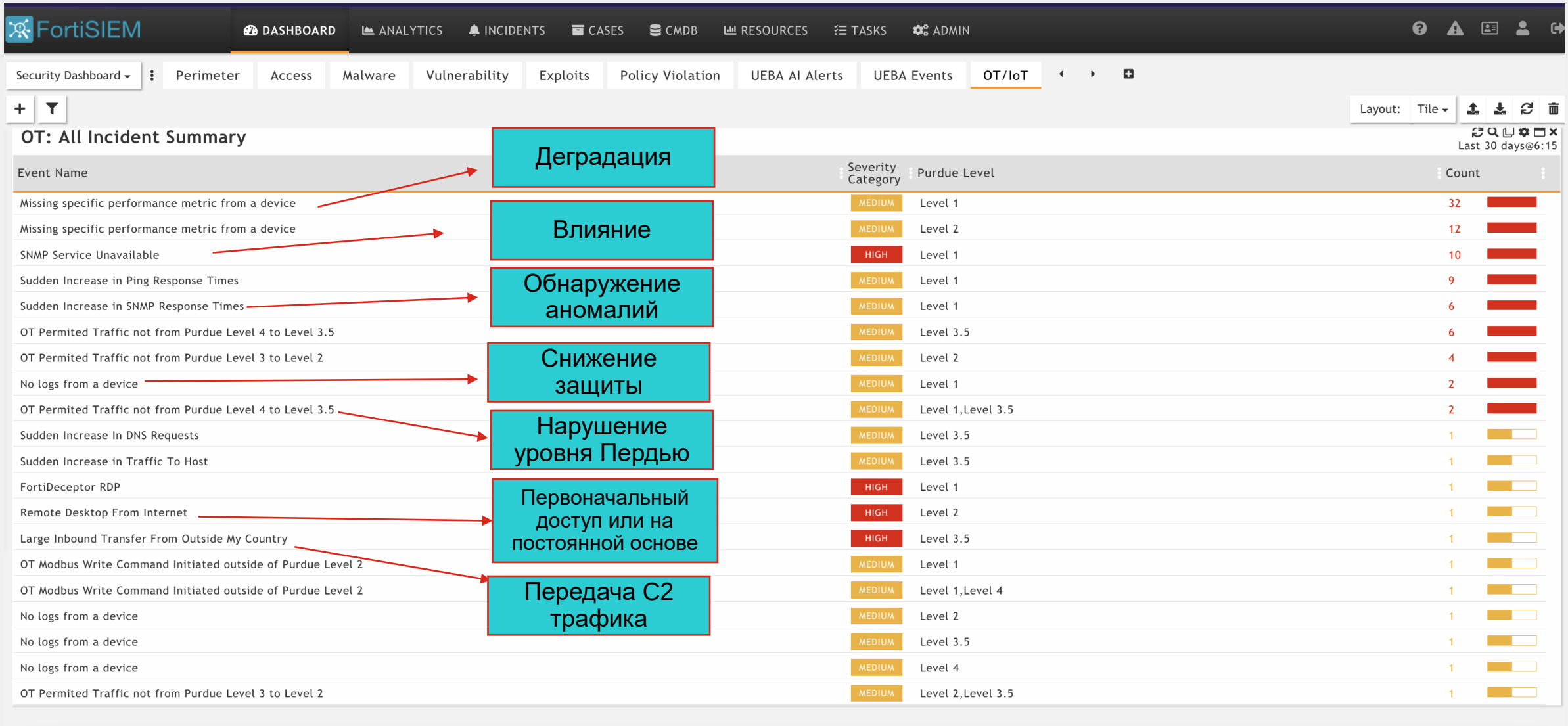




Панель управления

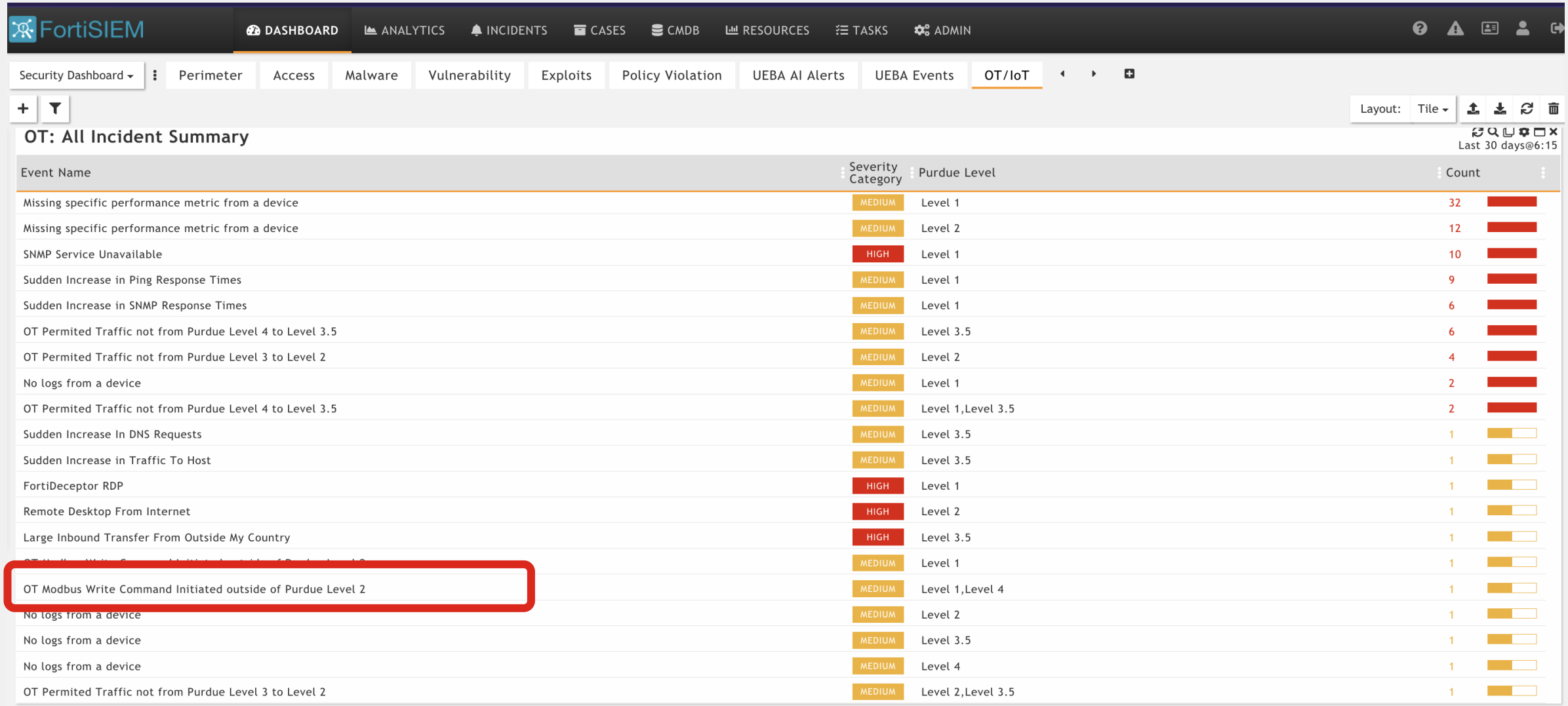


Инциденты



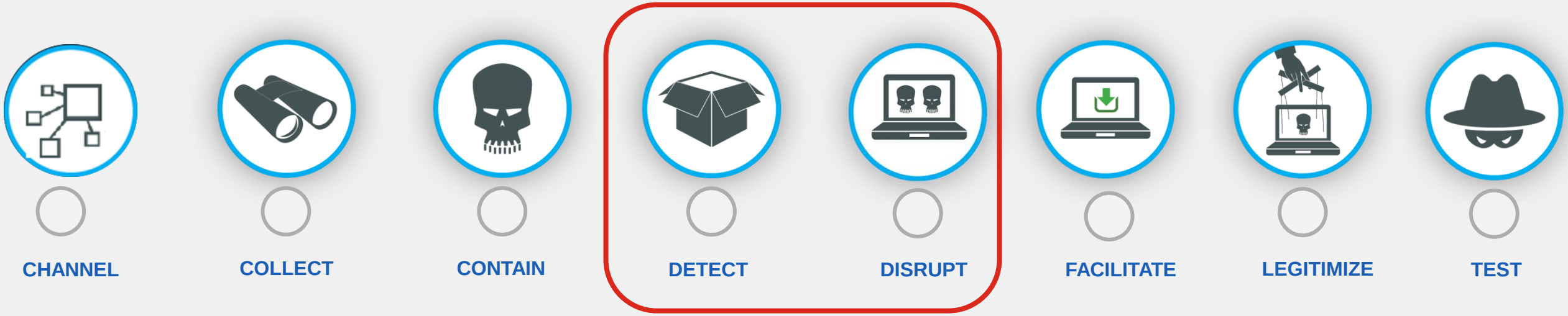
Event Name	Severity Category	Purdue Level	Count
Missing specific performance metric from a device	MEDIUM	Level 1	32
Missing specific performance metric from a device	MEDIUM	Level 2	12
SNMP Service Unavailable	HIGH	Level 1	10
Sudden Increase in Ping Response Times	MEDIUM	Level 1	9
Sudden Increase in SNMP Response Times	MEDIUM	Level 1	6
OT Permited Traffic not from Purdue Level 4 to Level 3.5	MEDIUM	Level 3.5	6
OT Permited Traffic not from Purdue Level 3 to Level 2	MEDIUM	Level 2	4
No logs from a device	MEDIUM	Level 1	2
OT Permited Traffic not from Purdue Level 4 to Level 3.5	MEDIUM	Level 1,Level 3.5	2
Sudden Increase In DNS Requests	MEDIUM	Level 3.5	1
Sudden Increase in Traffic To Host	MEDIUM	Level 3.5	1
FortiDeceptor RDP	HIGH	Level 1	1
Remote Desktop From Internet	HIGH	Level 2	1
Large Inbound Transfer From Outside My Country	HIGH	Level 3.5	1
OT Modbus Write Command Initiated outside of Purdue Level 2	MEDIUM	Level 1	1
OT Modbus Write Command Initiated outside of Purdue Level 2	MEDIUM	Level 1,Level 4	1
No logs from a device	MEDIUM	Level 2	1
No logs from a device	MEDIUM	Level 3.5	1
No logs from a device	MEDIUM	Level 4	1
OT Permited Traffic not from Purdue Level 3 to Level 2	MEDIUM	Level 2,Level 3.5	1

Финальные стадии



Event Name	Severity Category	Purdue Level	Count
Missing specific performance metric from a device	MEDIUM	Level 1	32
Missing specific performance metric from a device	MEDIUM	Level 2	12
SNMP Service Unavailable	HIGH	Level 1	10
Sudden Increase in Ping Response Times	MEDIUM	Level 1	9
Sudden Increase in SNMP Response Times	MEDIUM	Level 1	6
OT Permited Traffic not from Purdue Level 4 to Level 3.5	MEDIUM	Level 3.5	6
OT Permited Traffic not from Purdue Level 3 to Level 2	MEDIUM	Level 2	4
No logs from a device	MEDIUM	Level 1	2
OT Permited Traffic not from Purdue Level 4 to Level 3.5	MEDIUM	Level 1,Level 3.5	2
Sudden Increase In DNS Requests	MEDIUM	Level 3.5	1
Sudden Increase in Traffic To Host	MEDIUM	Level 3.5	1
FortiDeceptor RDP	HIGH	Level 1	1
Remote Desktop From Internet	HIGH	Level 2	1
Large Inbound Transfer From Outside My Country	HIGH	Level 3.5	1
[illegible]	MEDIUM	Level 1	1
OT Modbus Write Command Initiated outside of Purdue Level 2	MEDIUM	Level 1,Level 4	1
No logs from a device	MEDIUM	Level 2	1
No logs from a device	MEDIUM	Level 3.5	1
No logs from a device	MEDIUM	Level 4	1
OT Permited Traffic not from Purdue Level 3 to Level 2	MEDIUM	Level 2,Level 3.5	1

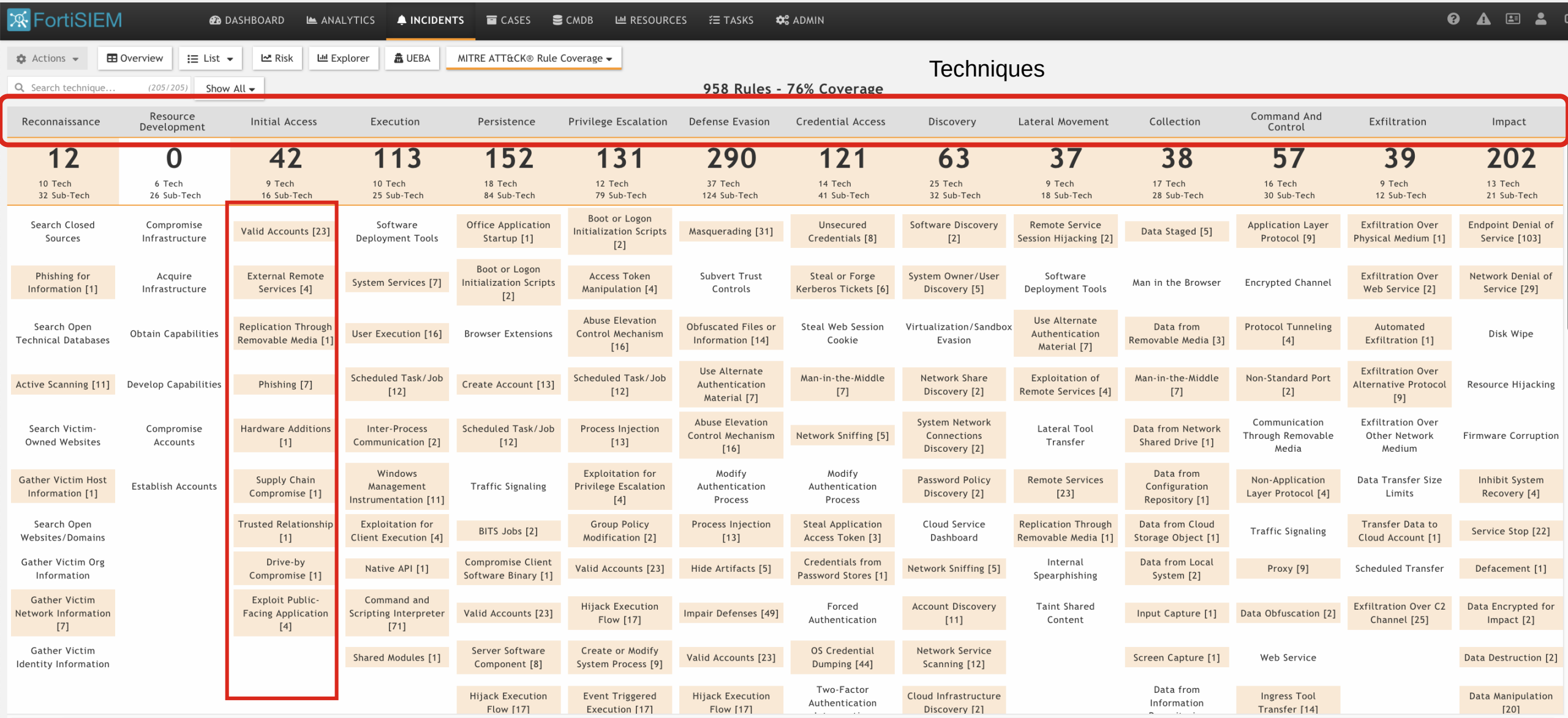
MITRE Shield (Active Defense)



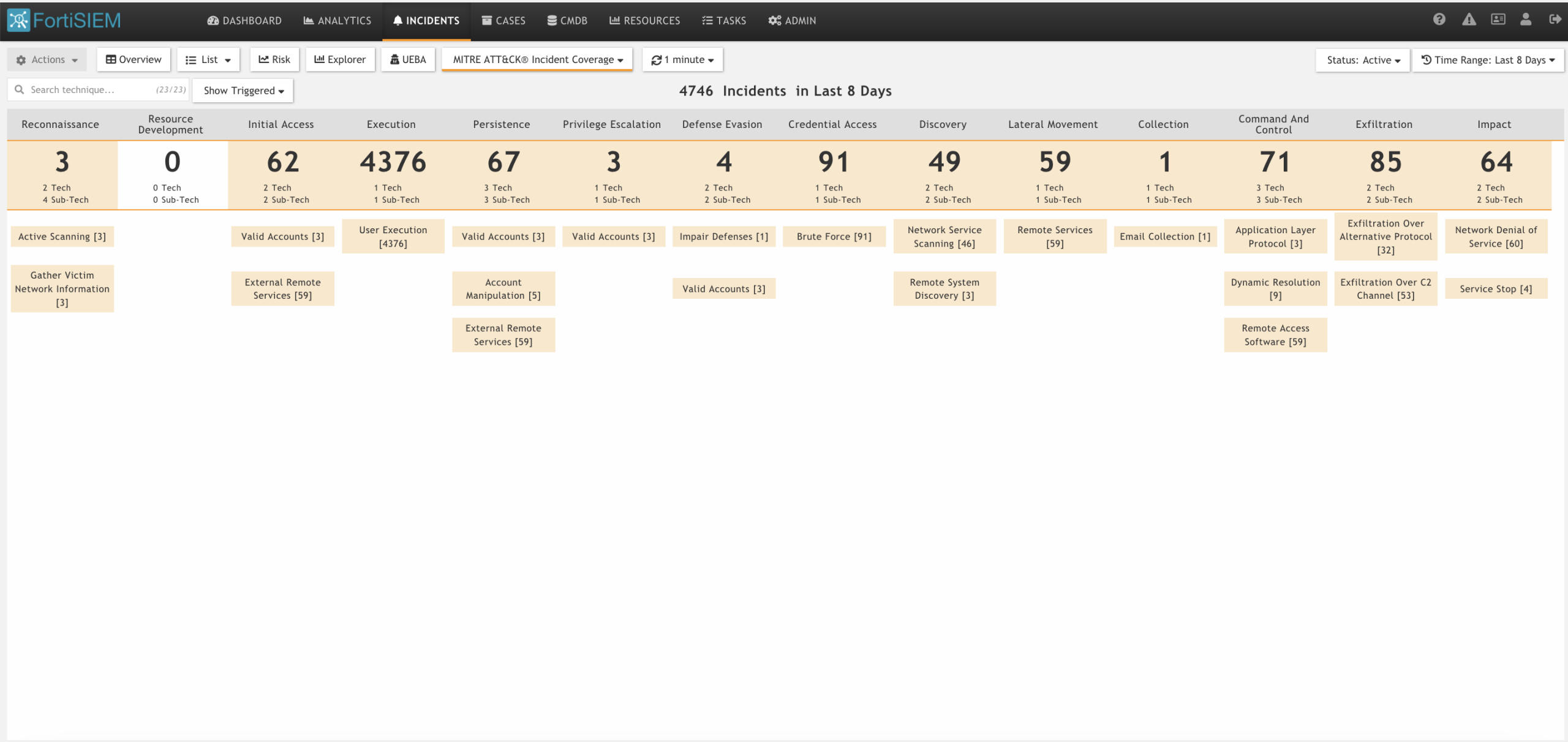
Обнаружение
Установление или поддержание осведомленности о том, что делает противник.

Разрушение
Помешать противнику выполнить часть или всю свою миссию.

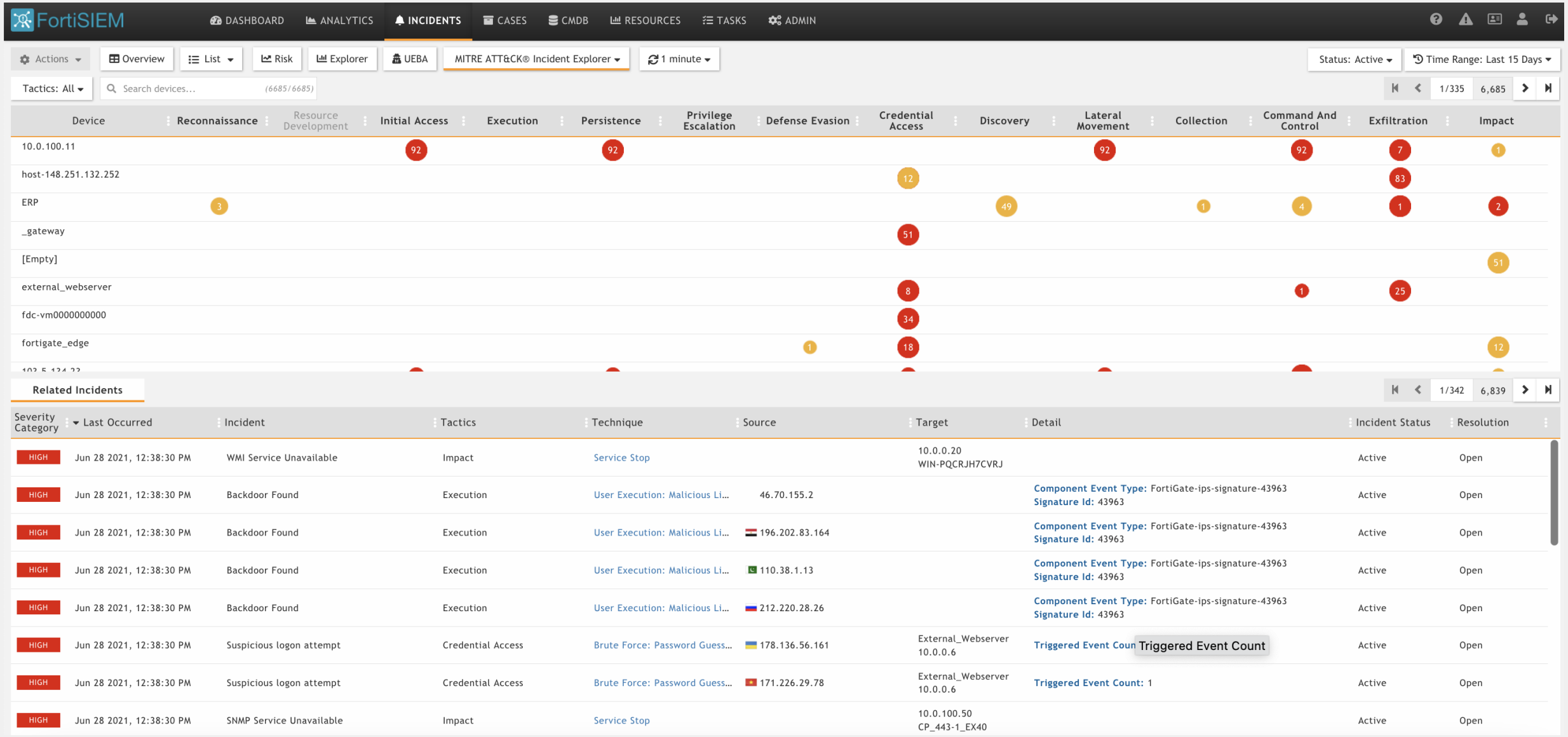
Покрытие правил MITRE ATT&CK



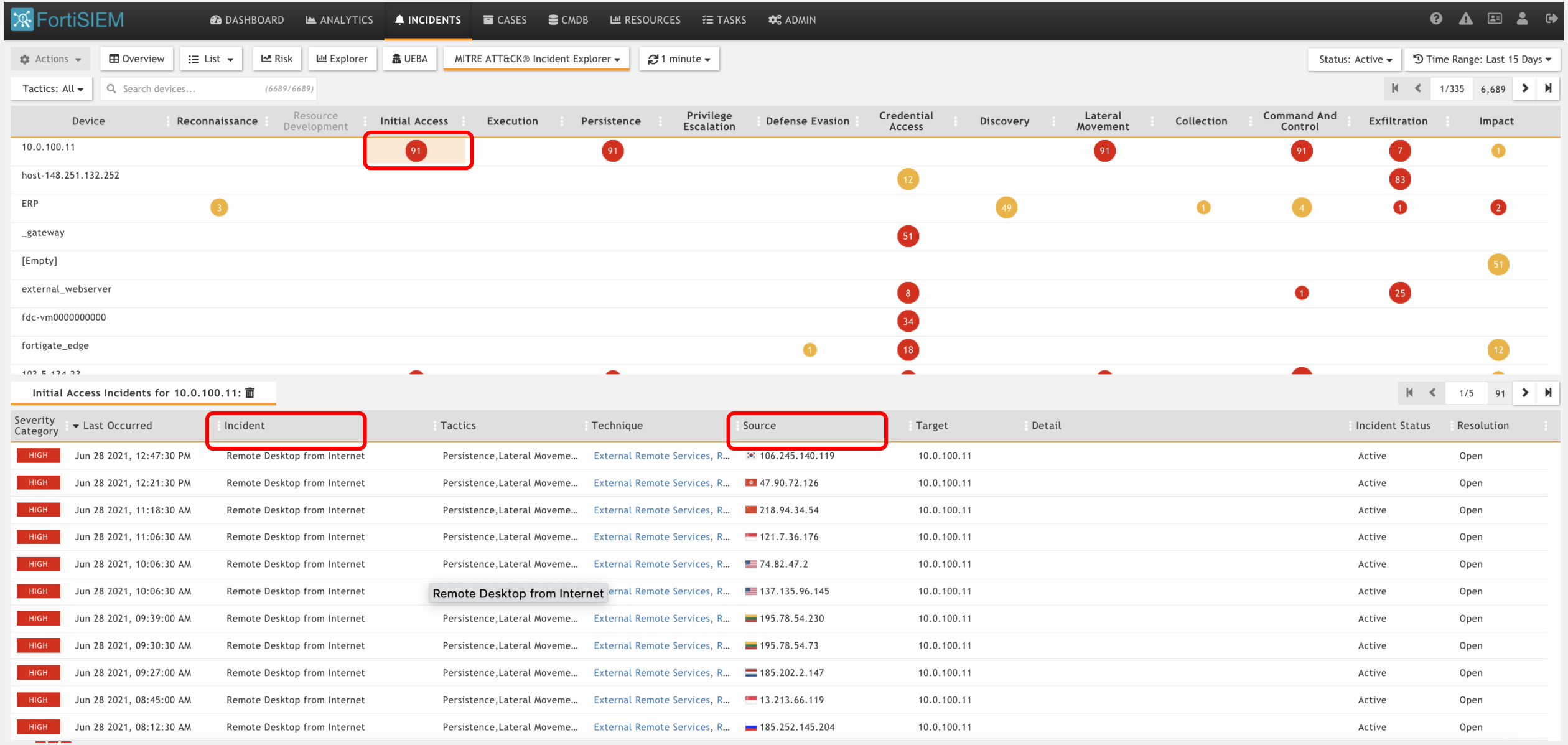
Сработавшие правила(покрытие инцидентов)



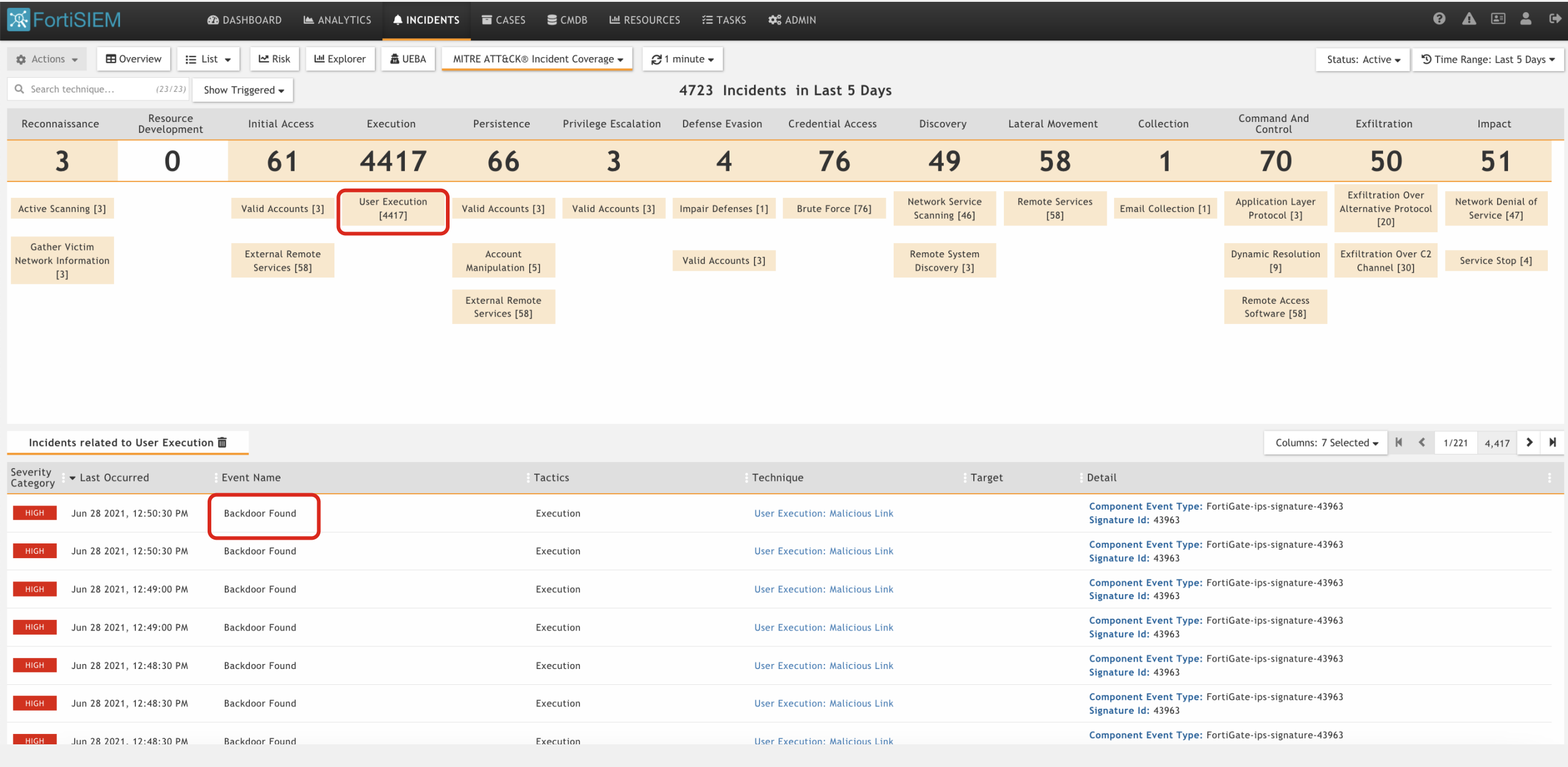
Исследование инцидента



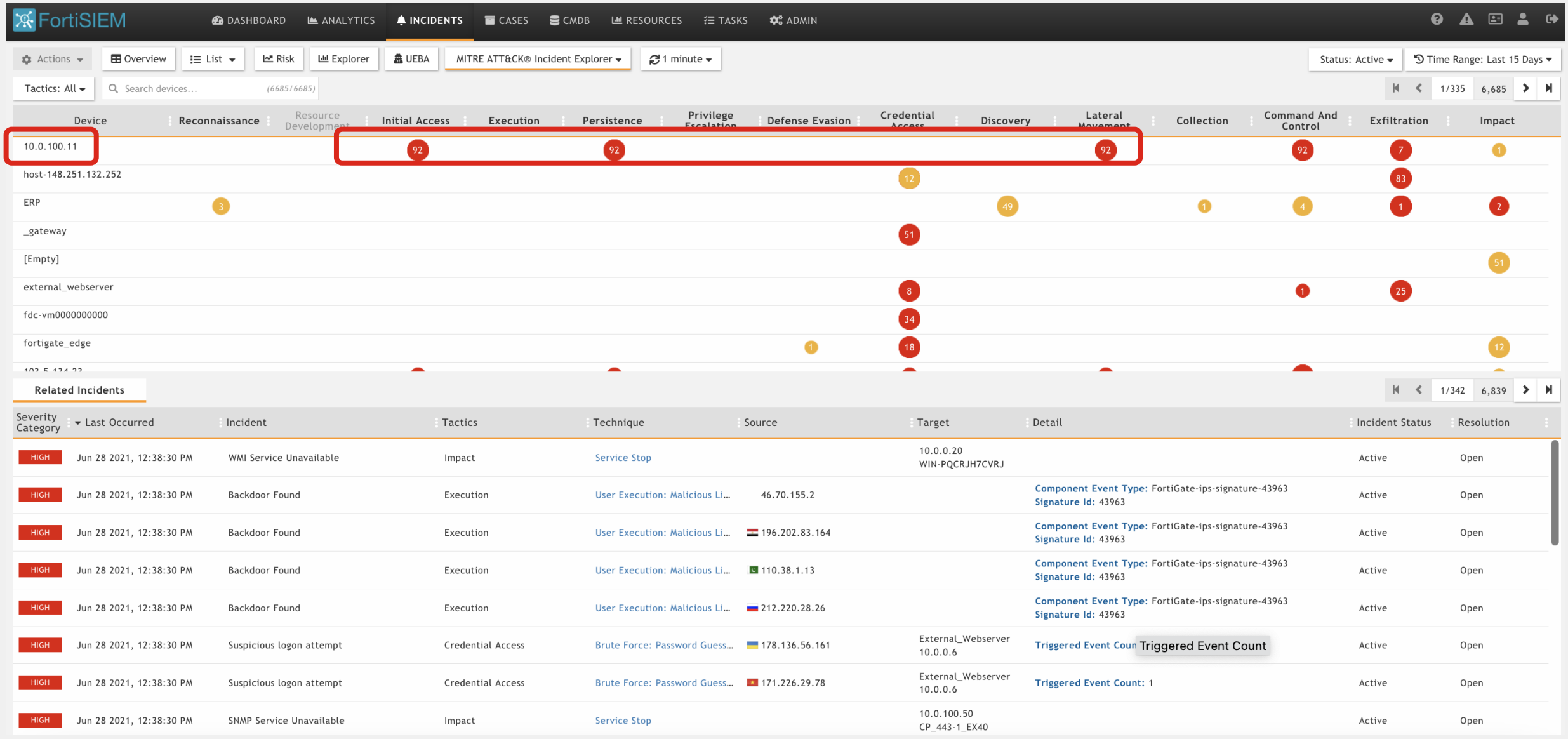
Первоначальный доступ



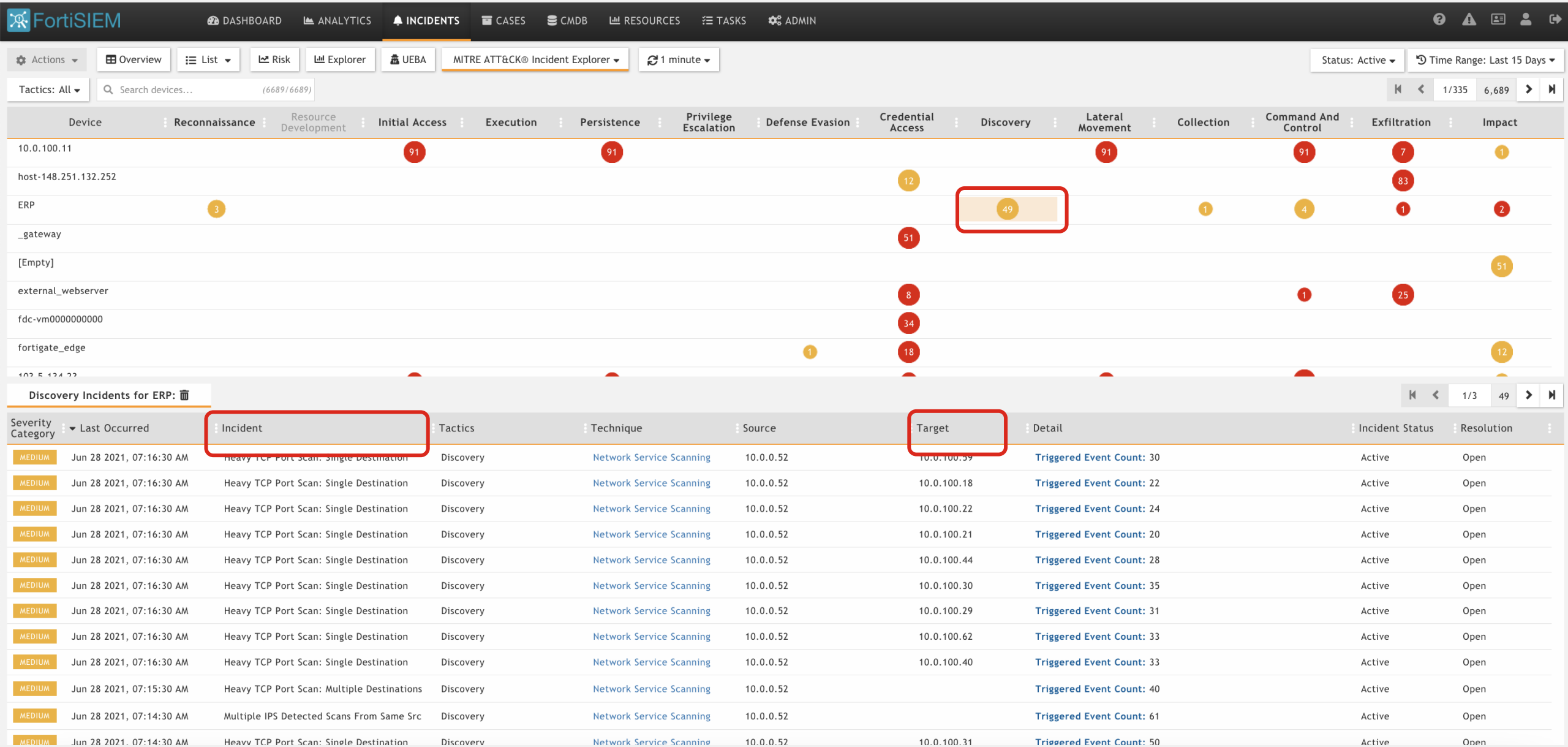
Исполнение


FortiSIEM
DASHBOARD
ANALYTICS
INCIDENTS
CASES
CMDB
RESOURCES
TASKS
ADMIN
Actions
Overview
List
Risk
Explorer
UEBA
MITRE ATT&CK® Incident Coverage
1 minute
Status: Active
Time Range: Last 5 Days
Search technique... (23/23)
Show Triggered
4723 Incidents in Last 5 Days
Reconnaissance 3
Resource Development 0
Initial Access 61
Execution 4417
Persistence 66
Privilege Escalation 3
Defense Evasion 4
Credential Access 76
Discovery 49
Lateral Movement 58
Collection 1
Command And Control 70
Exfiltration 50
Impact 51
Active Scanning [3]
Gather Victim Network Information [3]
Valid Accounts [3]
External Remote Services [58]
User Execution [4417]
Valid Accounts [3]
Account Manipulation [5]
External Remote Services [58]
Valid Accounts [3]
Impair Defenses [1]
Valid Accounts [3]
Brute Force [76]
Network Service Scanning [46]
Remote System Discovery [3]
Remote Services [58]
Email Collection [1]
Application Layer Protocol [3]
Dynamic Resolution [9]
Remote Access Software [58]
Exfiltration Over Alternative Protocol [20]
Exfiltration Over C2 Channel [30]
Network Denial of Service [47]
Service Stop [4]
Incidents related to User Execution
Columns: 7 Selected
1/221
4,417
Severity Category
Last Occurred
Event Name
Tactics
Technique
Target
Detail
HIGH Jun 28 2021, 12:50:30 PM Backdoor Found Execution User Execution: Malicious Link Component Event Type: FortiGate-ips-signature-43963 Signature Id: 43963
HIGH Jun 28 2021, 12:50:30 PM Backdoor Found Execution User Execution: Malicious Link Component Event Type: FortiGate-ips-signature-43963 Signature Id: 43963
HIGH Jun 28 2021, 12:49:00 PM Backdoor Found Execution User Execution: Malicious Link Component Event Type: FortiGate-ips-signature-43963 Signature Id: 43963
HIGH Jun 28 2021, 12:49:00 PM Backdoor Found Execution User Execution: Malicious Link Component Event Type: FortiGate-ips-signature-43963 Signature Id: 43963
HIGH Jun 28 2021, 12:48:30 PM Backdoor Found Execution User Execution: Malicious Link Component Event Type: FortiGate-ips-signature-43963 Signature Id: 43963
HIGH Jun 28 2021, 12:48:30 PM Backdoor Found Execution User Execution: Malicious Link Component Event Type: FortiGate-ips-signature-43963 Signature Id: 43963
HIGH Jun 28 2021, 12:48:30 PM Backdoor Found Execution User Execution: Malicious Link Component Event Type: FortiGate-ips-signature-43963

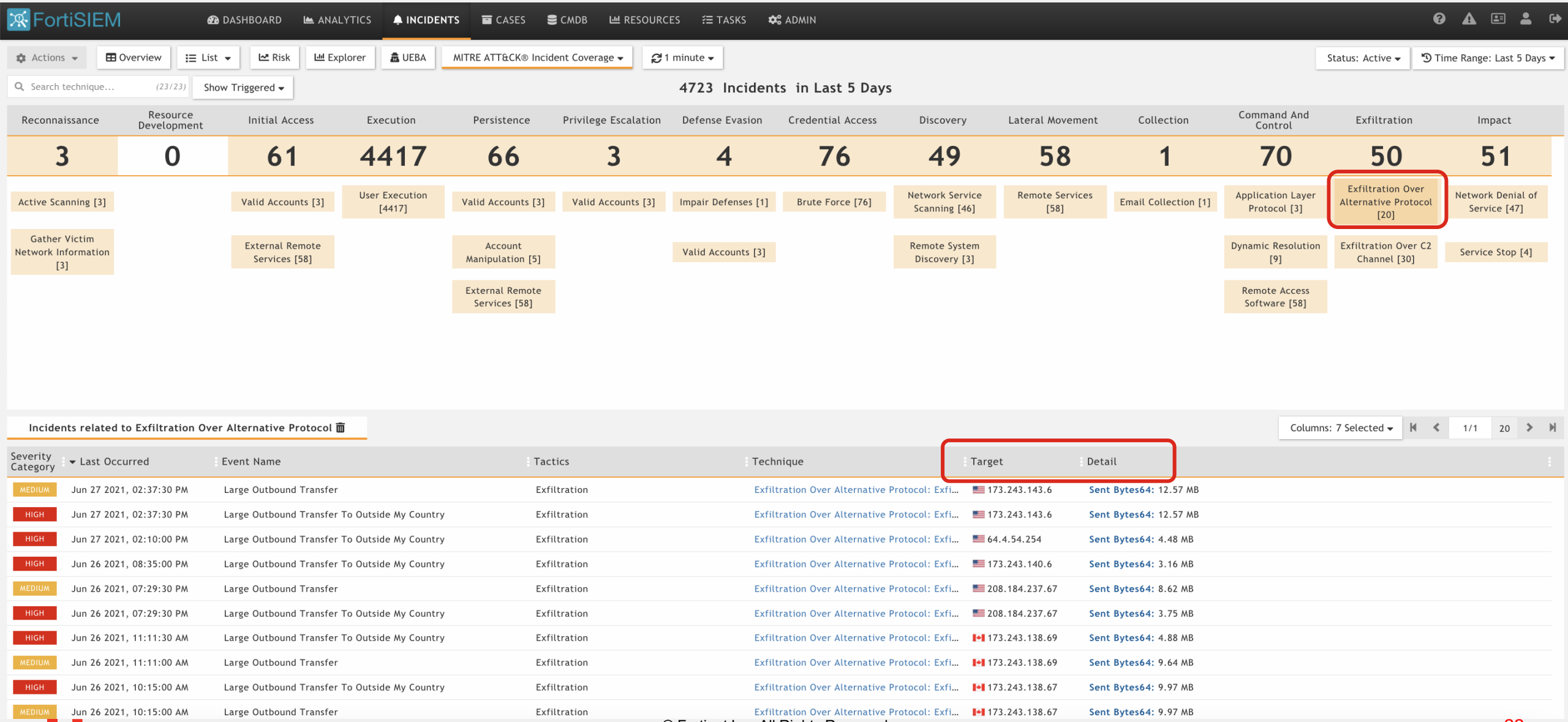
Закрепление



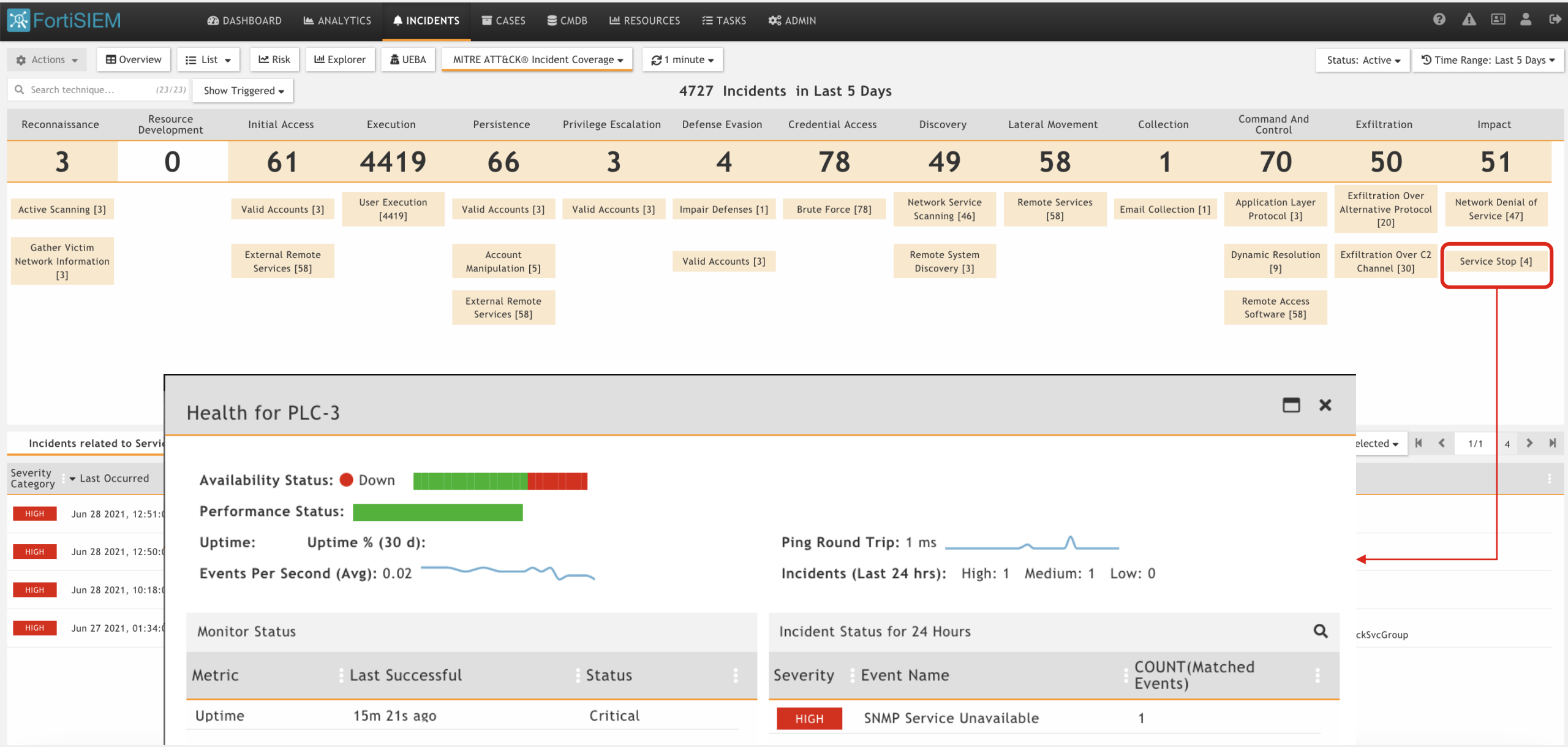
Внутренняя разведка



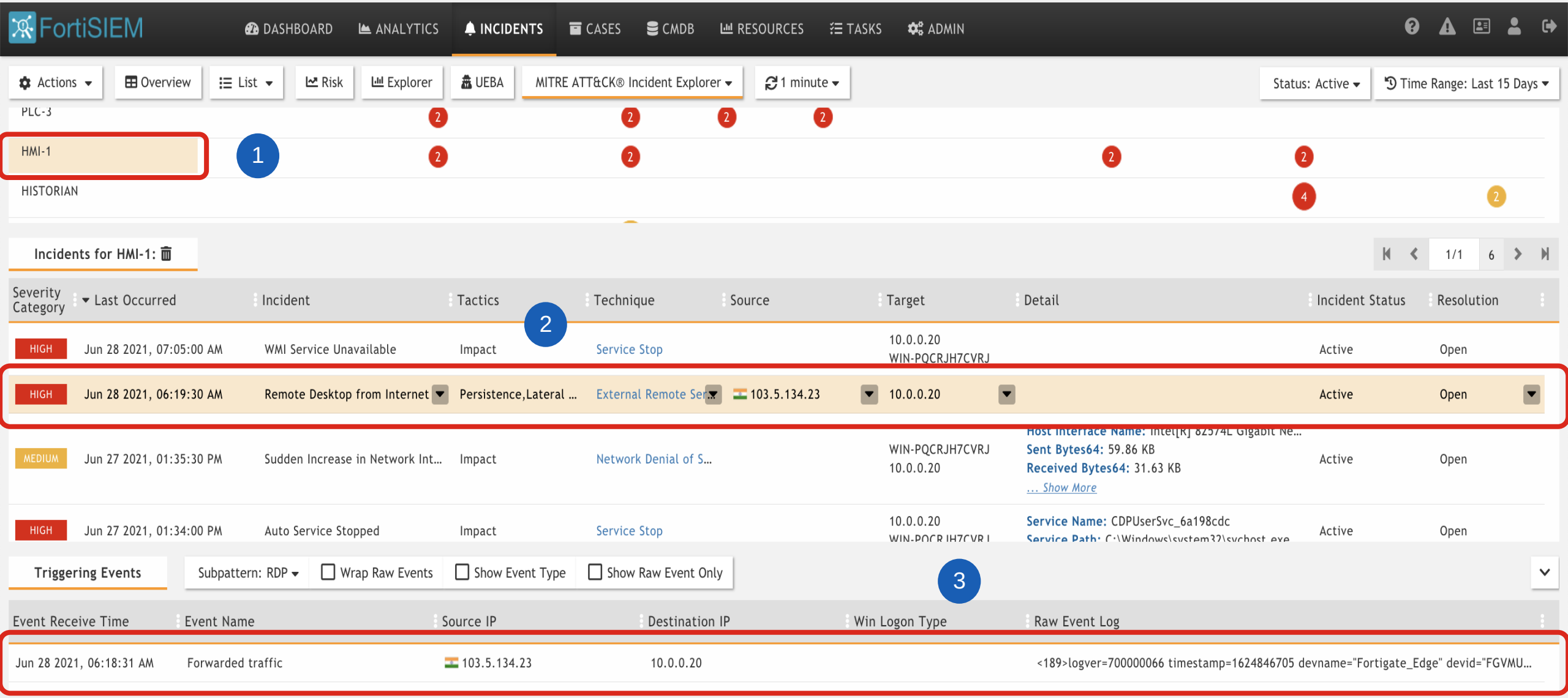
Вывод данных



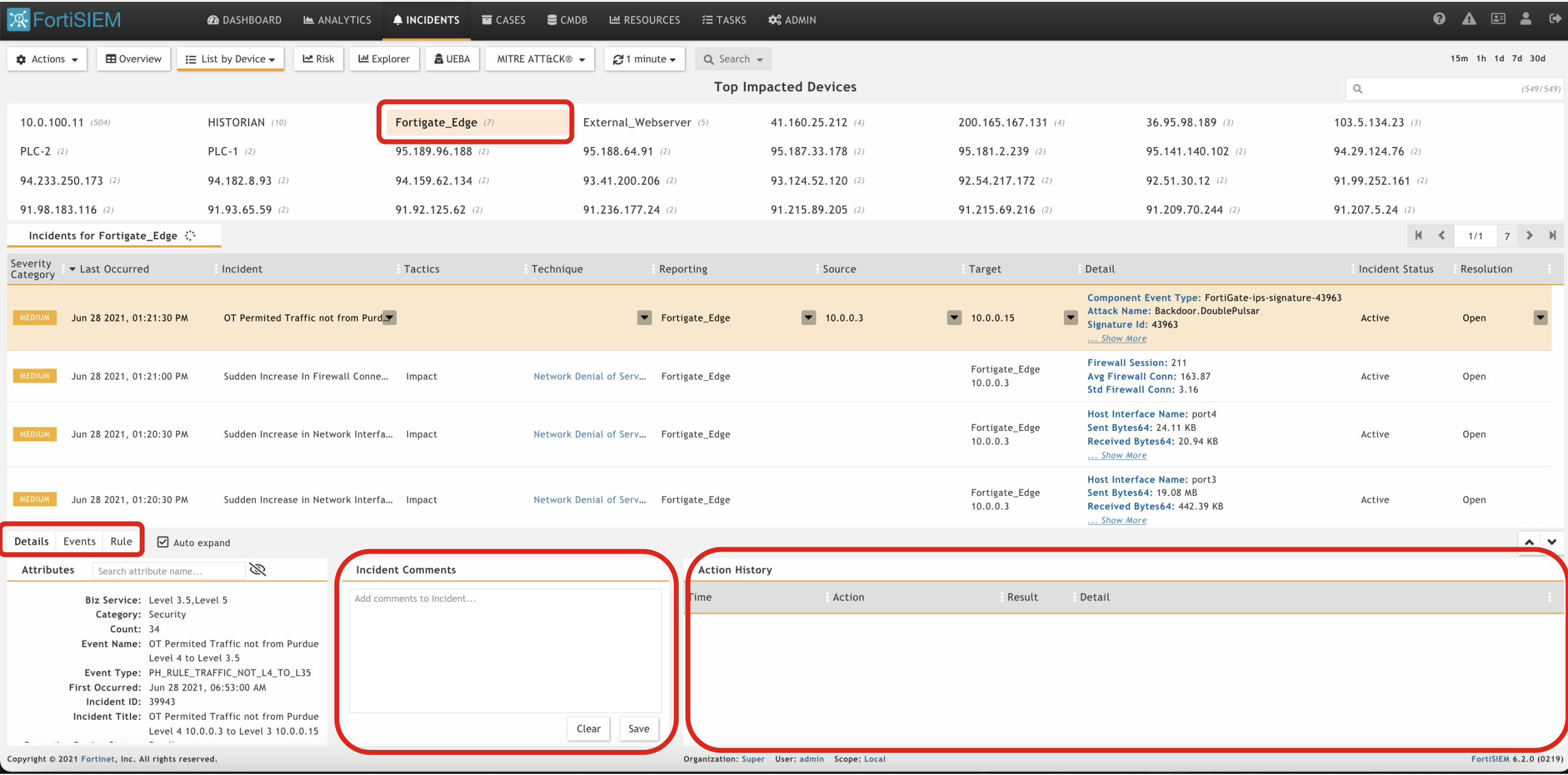
Выполнение миссии



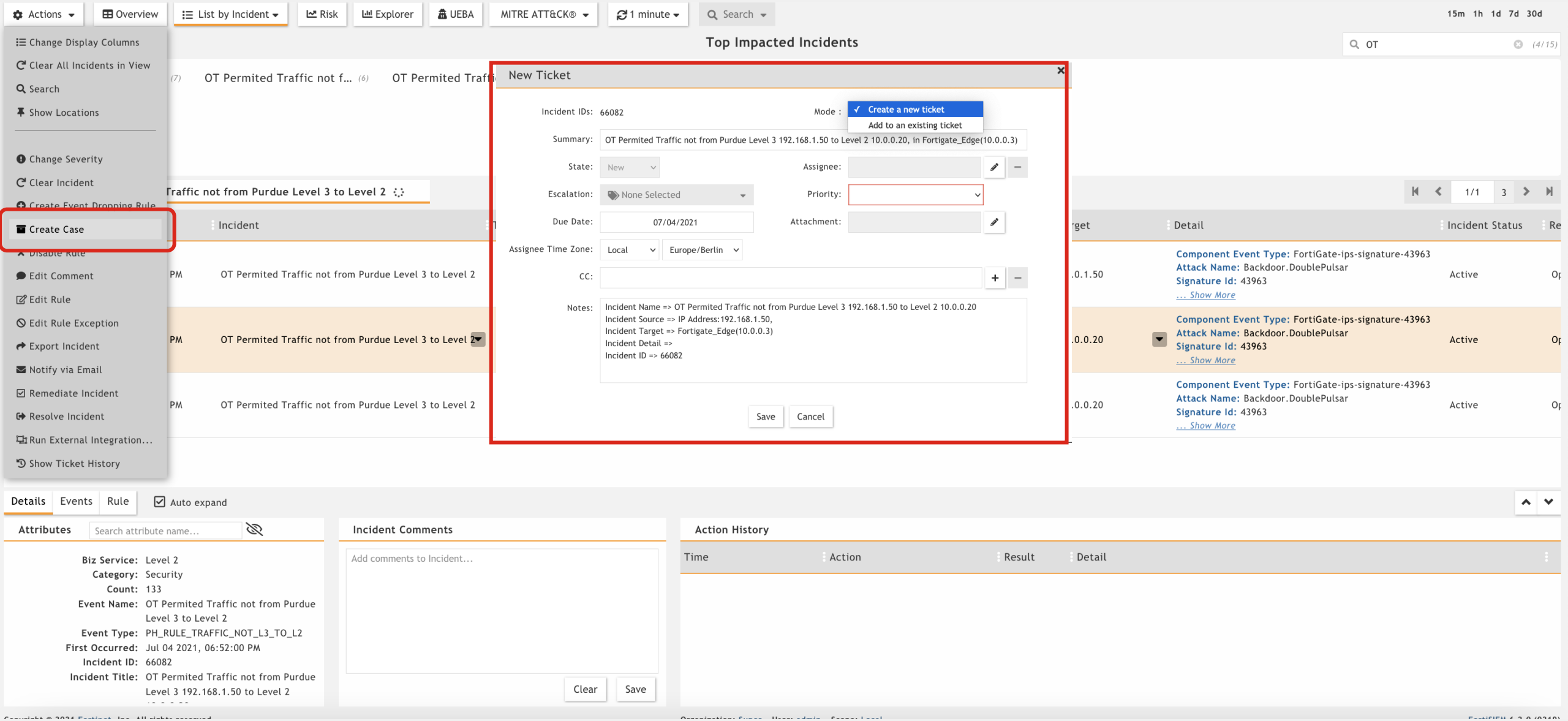
Расследование инцидента



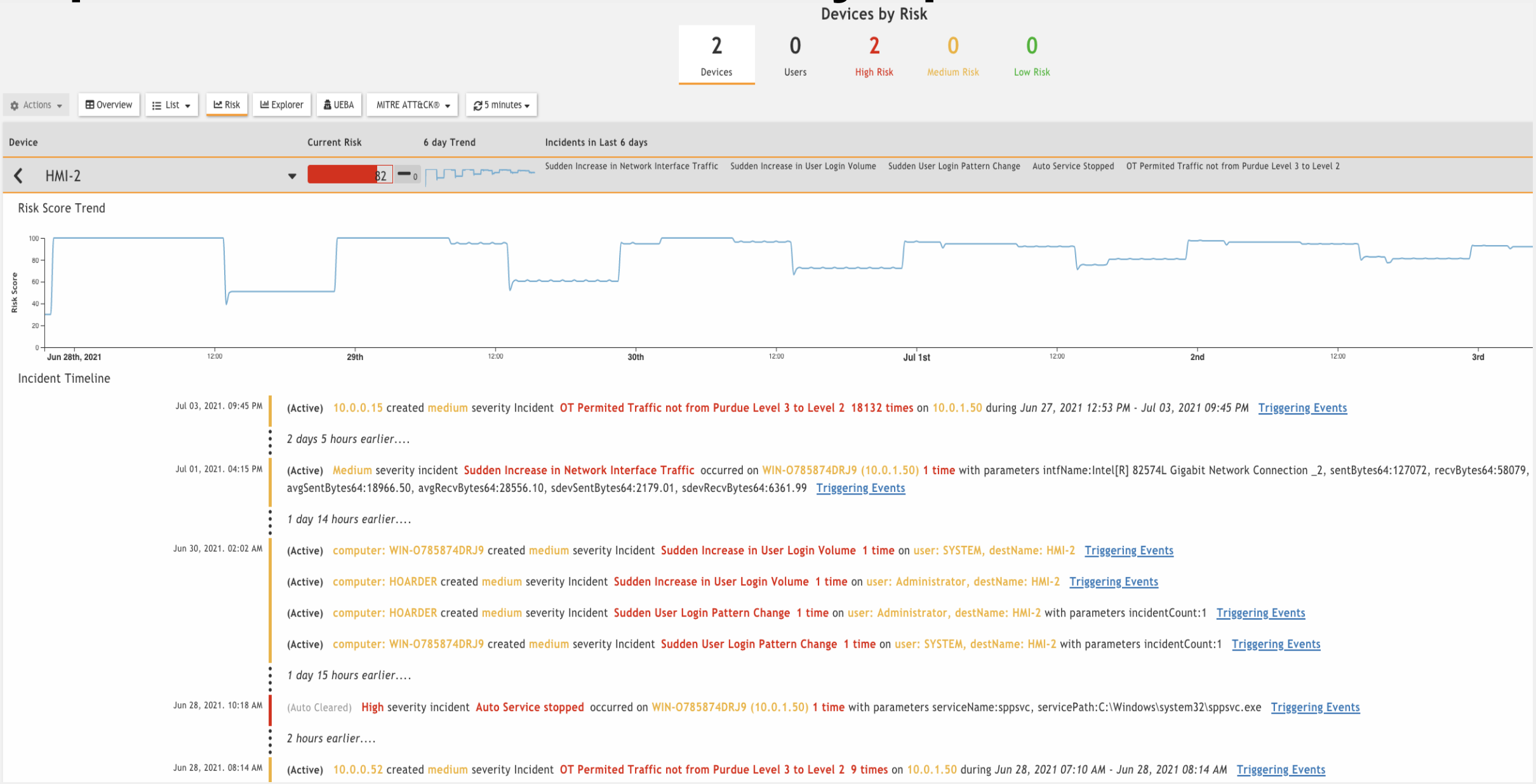
Расследование инцидента (Device View)



Расследование инцидента(Case)



Хронология инцидентов по устройствам



Метрики производительности

Health for HMI-2

Availability Status: Up

Performance Status: Normal

Uptime: 41d 2h Uptime % (30 d): 100%

Events Per Second (Avg): 2.81

Ping Round Trip: 1 ms

Incidents (Last 24 hrs): High: 0 Medium: 6 Low: 0

Monitor Status

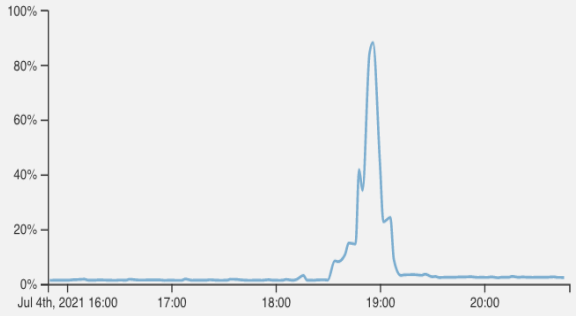
Metric	Last Successful	Status
Uptime	1m 27s ago	Normal
Service Status	1m 51s ago	Normal
Disk Space Util	3s ago	Normal
Net Intf Stat	1m 33s ago	Normal
Mem Util	23s ago	Normal
CPU Util	2m 20s ago	Normal
Virtual Mem Util	23s ago	Normal
Pagefile usage	41s ago	Normal

Incident Status for 24 Hours

Severity	Event Name	COUNT(Matched Events)
HIGH	Server Disk Latency Critical	1
MEDIUM	OT Permited Traffic not from Purd...	1
MEDIUM	OT Permited Traffic not from Purd...	1

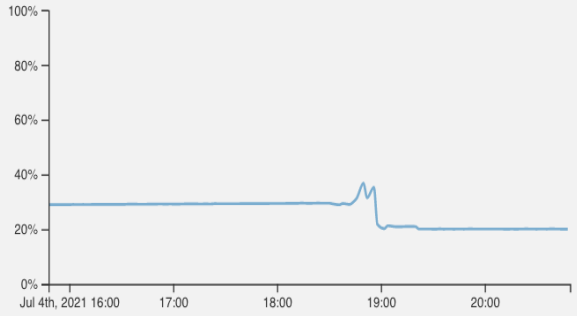
System CPU

1h | 5h | 12h | 1d | 7d



System Memory

1h | 5h | 12h | 1d | 7d



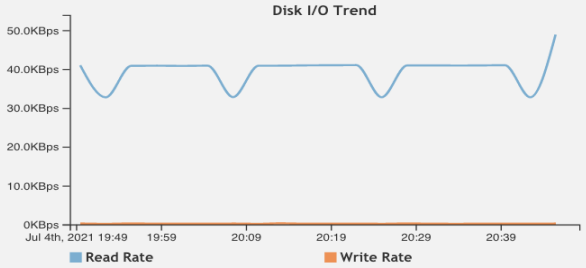
Top Application Status

1h | 5h | 12h | 1d | 7d

Application Name	Software Name	Software Param	CPU Util	Memory Util	Disk Read Rate	Disk Write Rate	Uptime
svchost.exe-k Loc...	svchost.exe	-k LocalServiceNe...	0.19%	0.06%	40KBps	200Bps	41d 2h
Microsoft Networ...	svchost.exe	-k netsvcs -p -s W...	0.05%	0.10%	200Bps	10Bps	41d 2h
FortiClient.exe	FortiClient.exe	--type=renderer -...	0.01%	0.42%	0KBps	0KBps	1h 54m
FortiProxy.exe	FortiProxy.exe	-s FC_{73EFB30F-...	0.01%	1.45%	20Bps	0KBps	1h 54m
Microsoft RPC ser...	svchost.exe	-k RPCSS -p	0.01%	0.04%	0KBps	0KBps	41d 2h
Microsoft Networ...	svchost.exe	-k netsvcs -p -s w...	0.00%	0.17%	0KBps	0KBps	41d 2h
svchost.exe-k utc...	svchost.exe	-k utcsvc -p	0.00%	0.24%	0KBps	0KBps	41d 2h
				0.07%	0KBps	0KBps	38d 4h

Disk Utilization

Disk I/O Trend

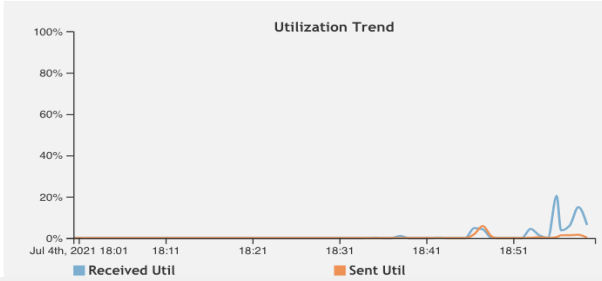


Top 10 Interface Utilization

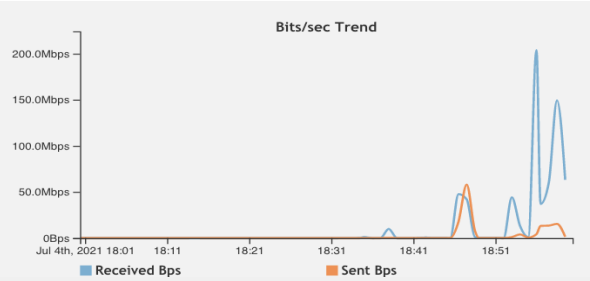
1h | 5h | 12h | 1d | 7d

Name	Received Util	Sent Util	Received Bps	Sent Bps
Intel[R] 82574L Gigabit Network Connection _2	1.05%	0.21%	11Mbps	2Mbps
Intel[R] 82574L Gigabit Network Connection	0.71%	0.32%	7Mbps	3Mbps
Intel[R] 82574L Gigabit Network Connection _3	0.31%	0.22%	3Mbps	2Mbps

Utilization Trend



Bits/sec Trend



Технологические партнеры и интеграторы

OT TECHNOLOGY PARTNERS

Visibility & Threat Intelligence

CYBERX BATTLE-TESTED INDUSTRIAL CYBERSECURITY
DRAGOS
NOZOMI NETWORKS
CLAROTY
INDUSTRIAL DEFENDER
SCADAfence
tenable

Operations, Orchestration Automation

OTORIO
splunk>
tdi
rubrik
np network perception
SKYBOX SECURITY
BACKBOX
servicenow

Other

SIEMENS RUGGEDCOM INDUSTRIAL STRENGTH NETWORKS
FORESCOUT
radiflow
RAD
DARKTRACE
OWL Cyber Defense

SOLUTION VENDORS AND SYSTEMS INTEGRATORS

Control Vendors

Schneider Electric
GE
ABB
YOKOGAWA
SIEMENS
HIRSCHMANN A BELDEN BRAND
EMERSON
Rockwell Automation
Honeywell
SEL SCHWEITZER ENGINEERING LABORATORIES

Global System Integrators

Hewlett Packard Enterprise
Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING
Orange Cyberdefense
HCL
IBM
NTT
accenture
Atos

Other(s)

Baker Hughes
T-Systems
Johnson Controls
Cognizant
World Wide Technology, Inc.
Eleven Paths A Telefónica COMPANY

FORTINET FABRIC-READY

Пример внедрения

Крупнейший в мире производитель сжиженного газа

15 изолированных заводов

Ключевые моменты

Модернизация безопасности
Обеспокоенность ЛПР по поводу эффективности безопасности
Экспертиза в области ОТ привнесена в ИТ-безопасность
Опасения по поводу операционного воздействия

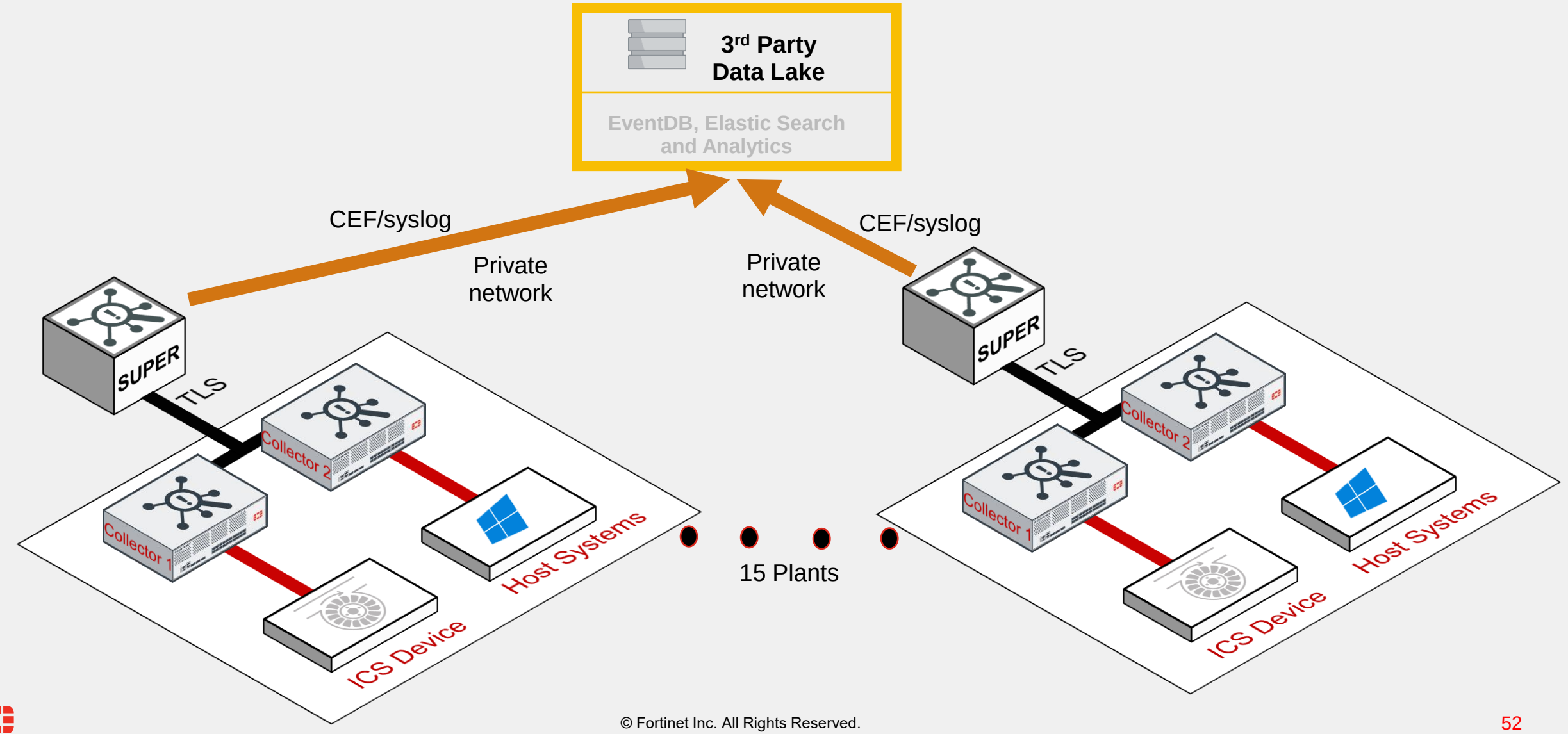
Потребности заказчика

- Осведомленность, сегментация
- Простота настройки и внедрения
- Экспертиза безопасности в доменах ОТ и IT
- Мультивендорная консолидация логов с возможностью осведомленности, как операционной, так и безопасности

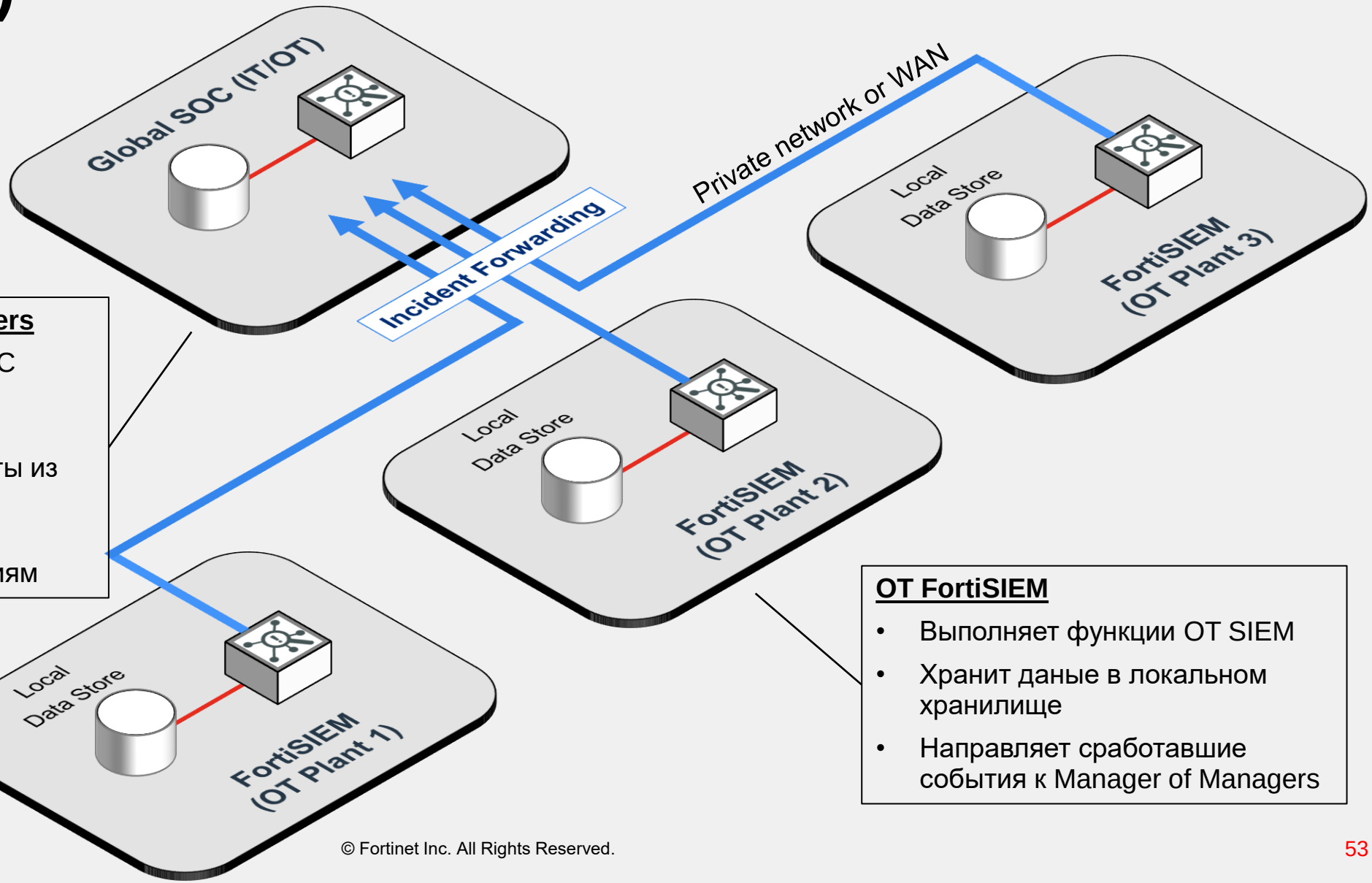
FORTINET РЕШЕНИЕ

- Патнер с ведущими производителями контроля ОТ
- Fortinet FortiSIEM 1 Supervisor, 2 Collectors на каждый завод(1 для IT и 1 для ОТ)
- «Сырые» логи направлялись в Elastic Data Lake

FortiSIEM изолированная архитектура



Архитектура Менеджер над Менеджерами(Global SOC IT/OT)



FortiSIEM Manager-of-Managers

- Внедрен в глобальном SOC (IT/OT)
- Получает и хранит переправленные инциденты из OT FortiSIEM
- Не имеет доступа к детализированным событиям

OT FortiSIEM

- Выполняет функции OT SIEM
- Хранит даные в локальном хранилище
- Направляет сработавшие события к Manager of Managers


FORTINET