



Кибербезопасность критически важных систем

Александр Чупрынин, системный инженер

25.11.2021

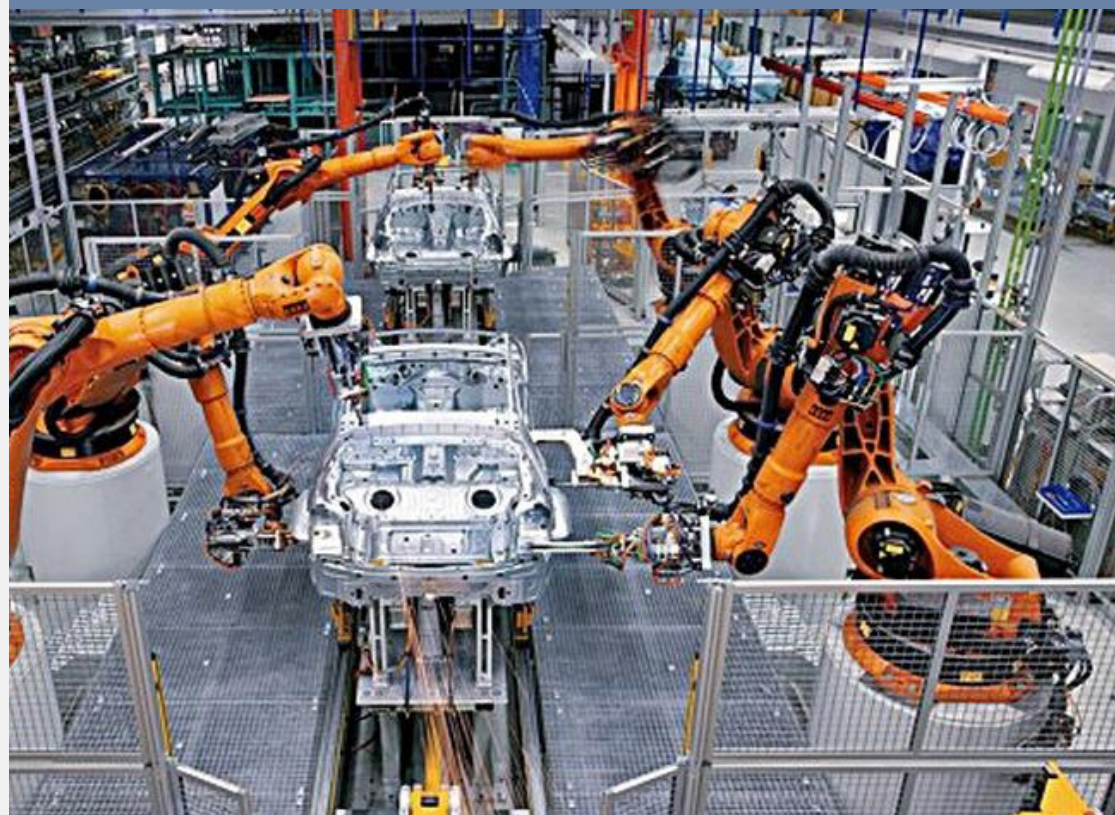
Операционные технологии (ОТ)

Используется для...

Мониторинг, управление, работа

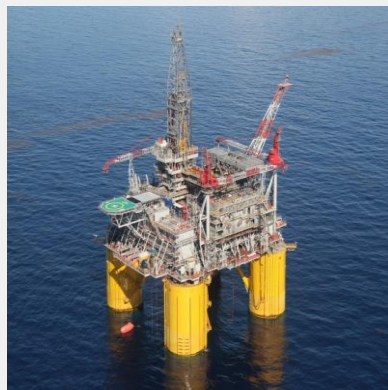


Индустриальная автоматизация



Операционные технологии (ОТ)

Применяются в ...

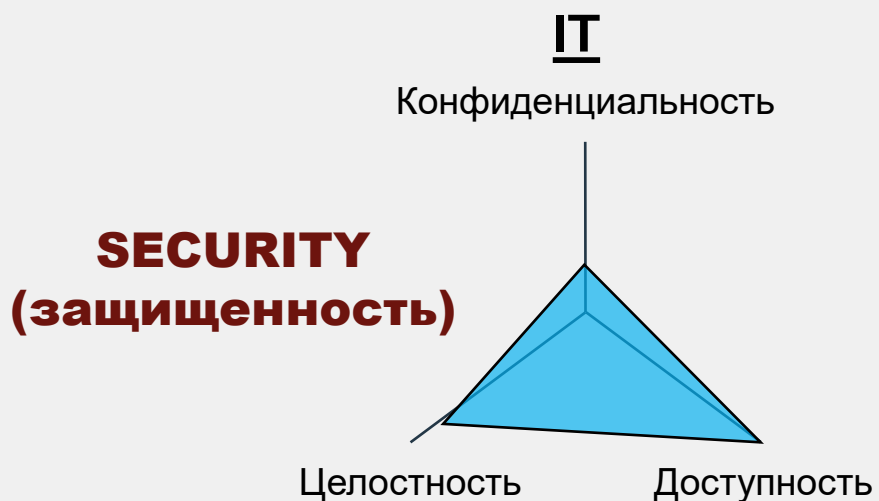


Разнообразные отрасли
Часто «критические»
инфраструктуры

В сложных условиях эксплуатации
(тепло, влажность, вибрация)



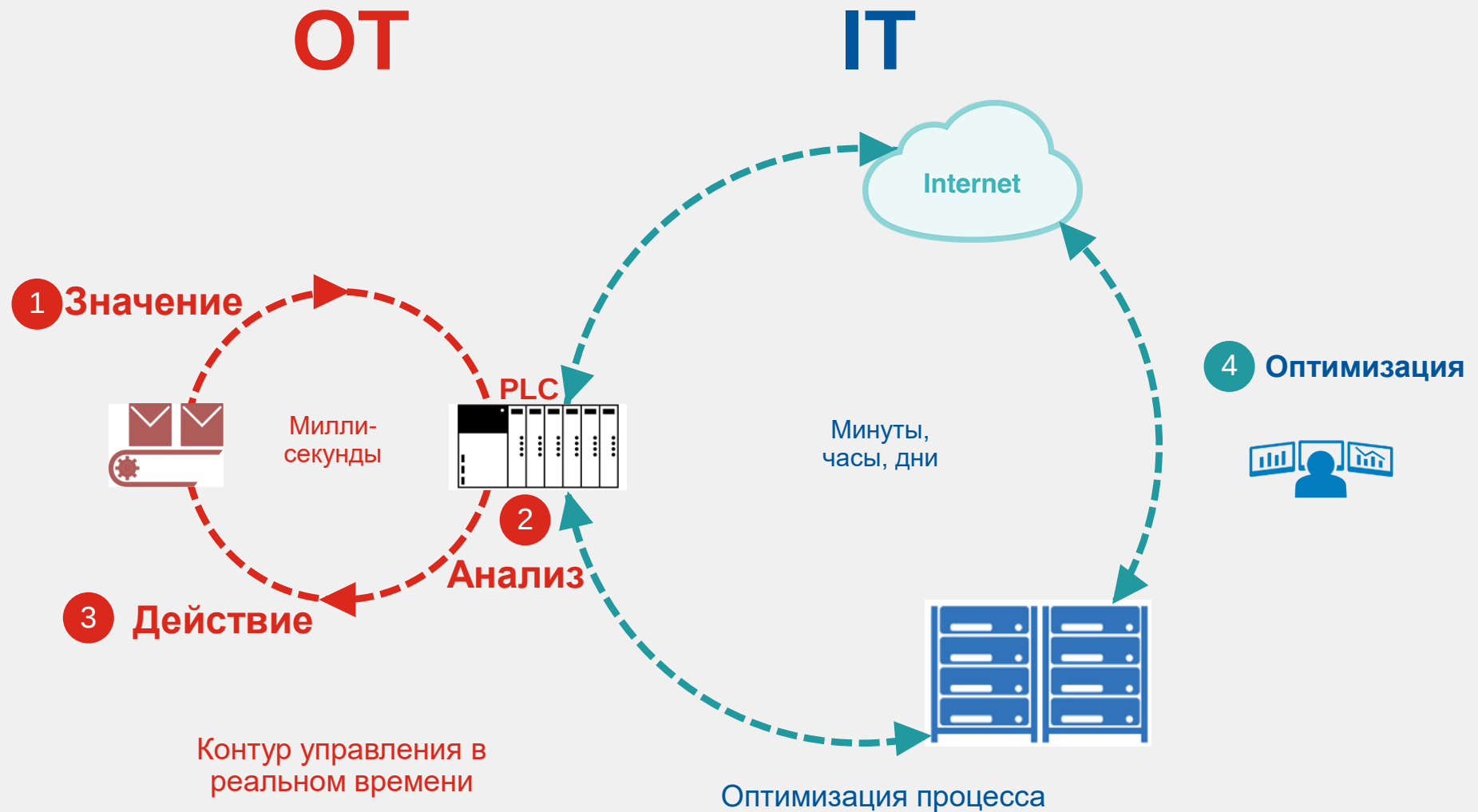
Чем отличаются IT от OT ?



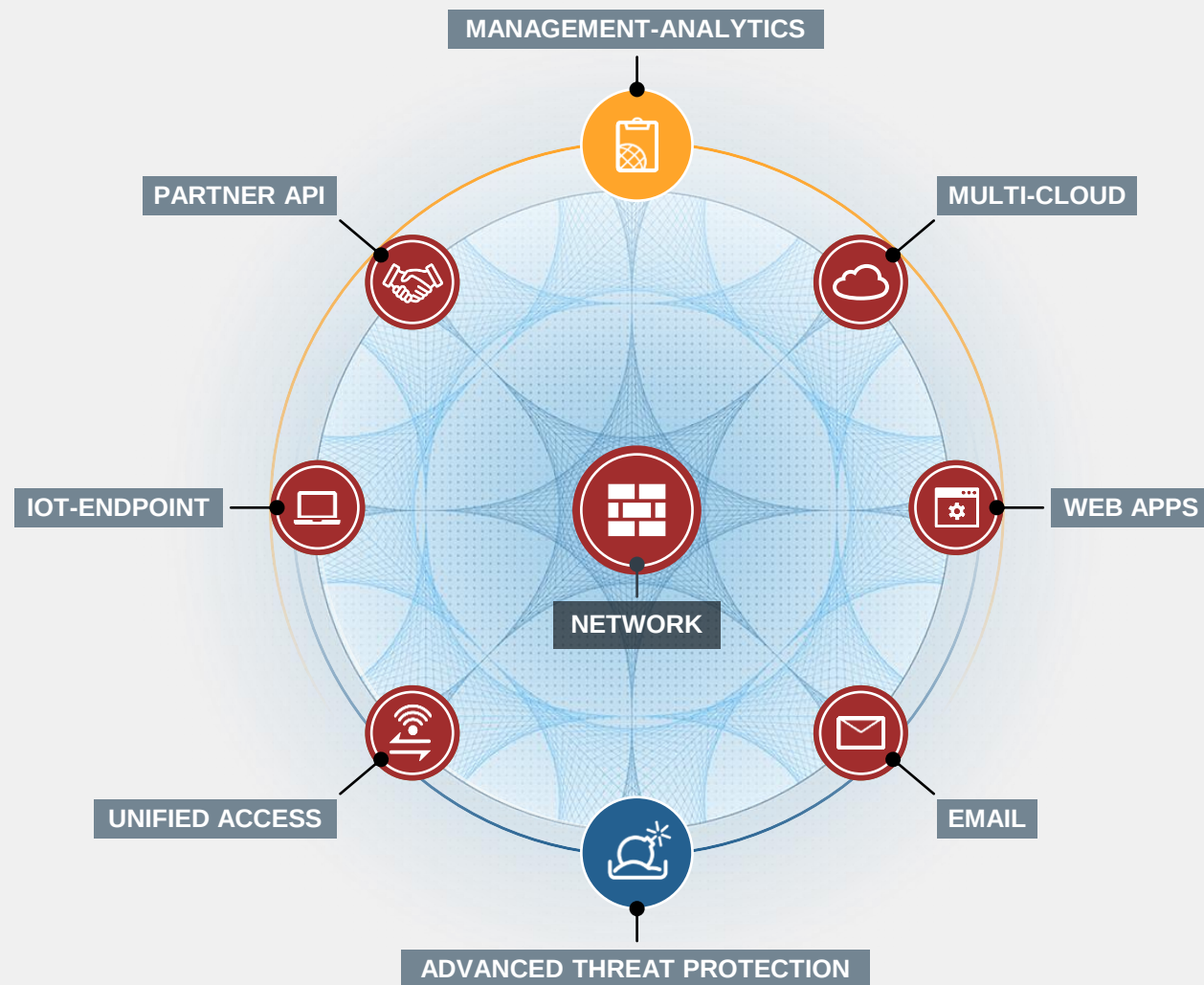
Характеристики Приоритеты

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



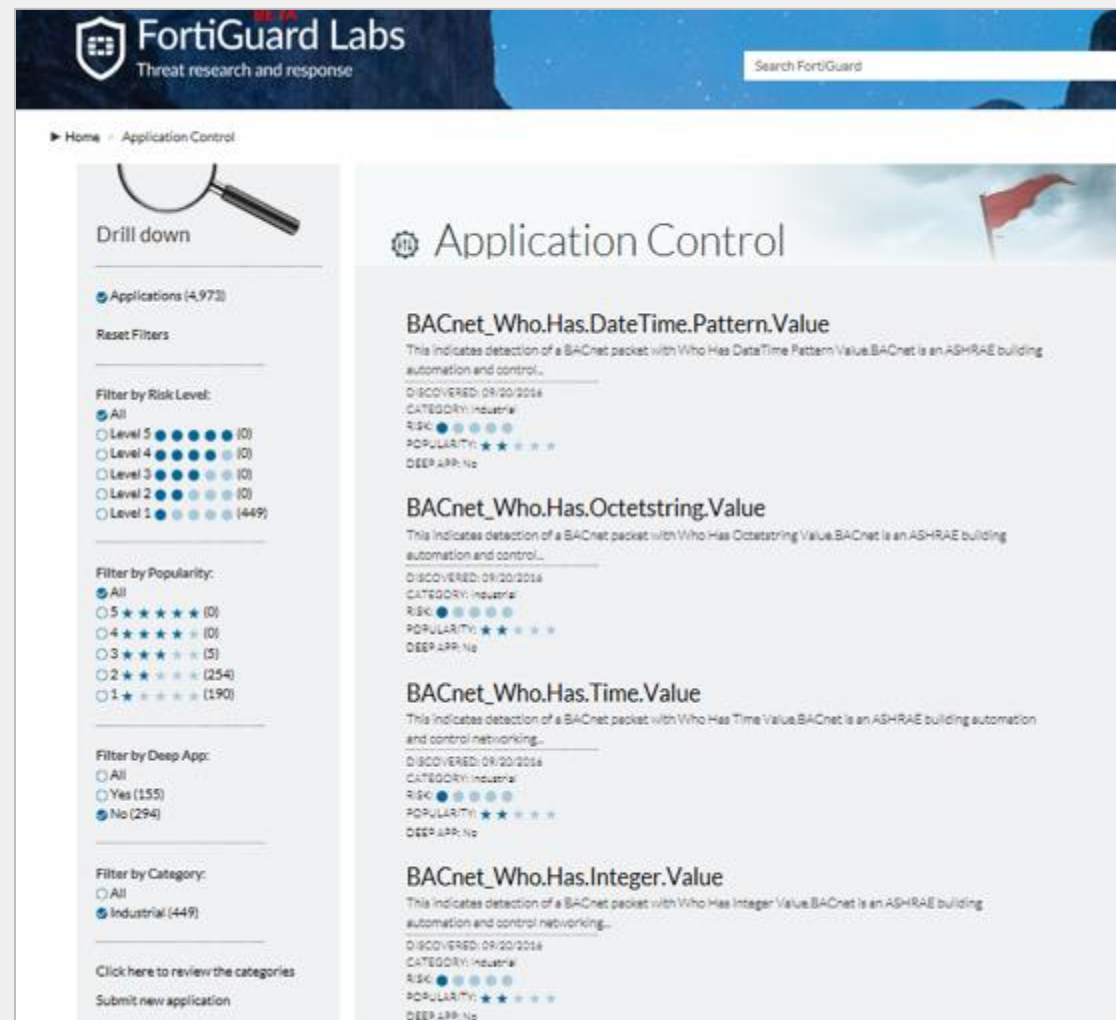
Fortinet Security Fabric для защиты ICS/SCADA



FortiGuard для OT

Специализация на OT

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



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 промышленных 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 промышленных 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





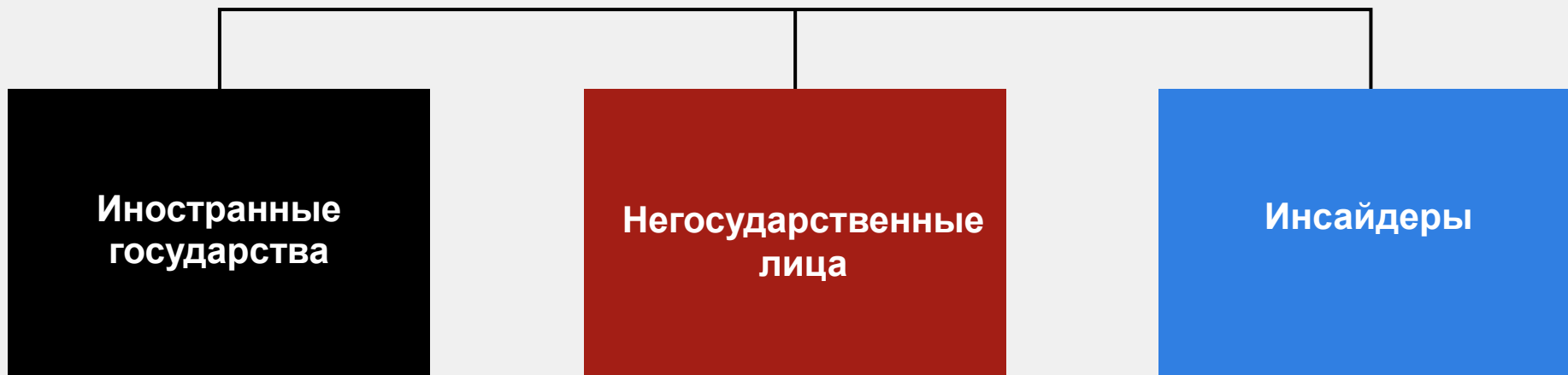
Какие решения Fortinet использовать для защиты ОТ ?



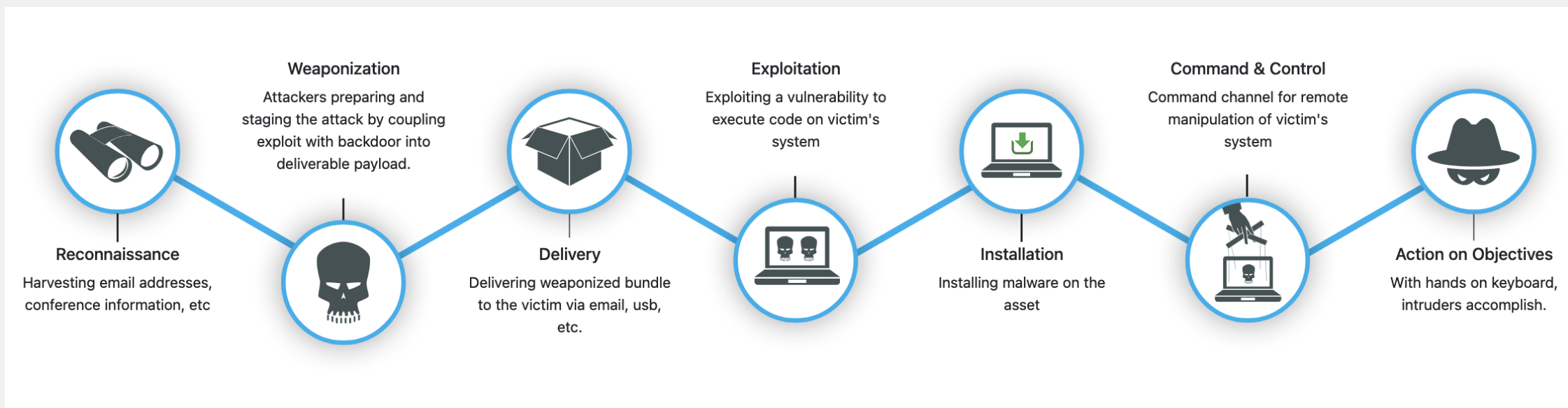
Кто атакует?



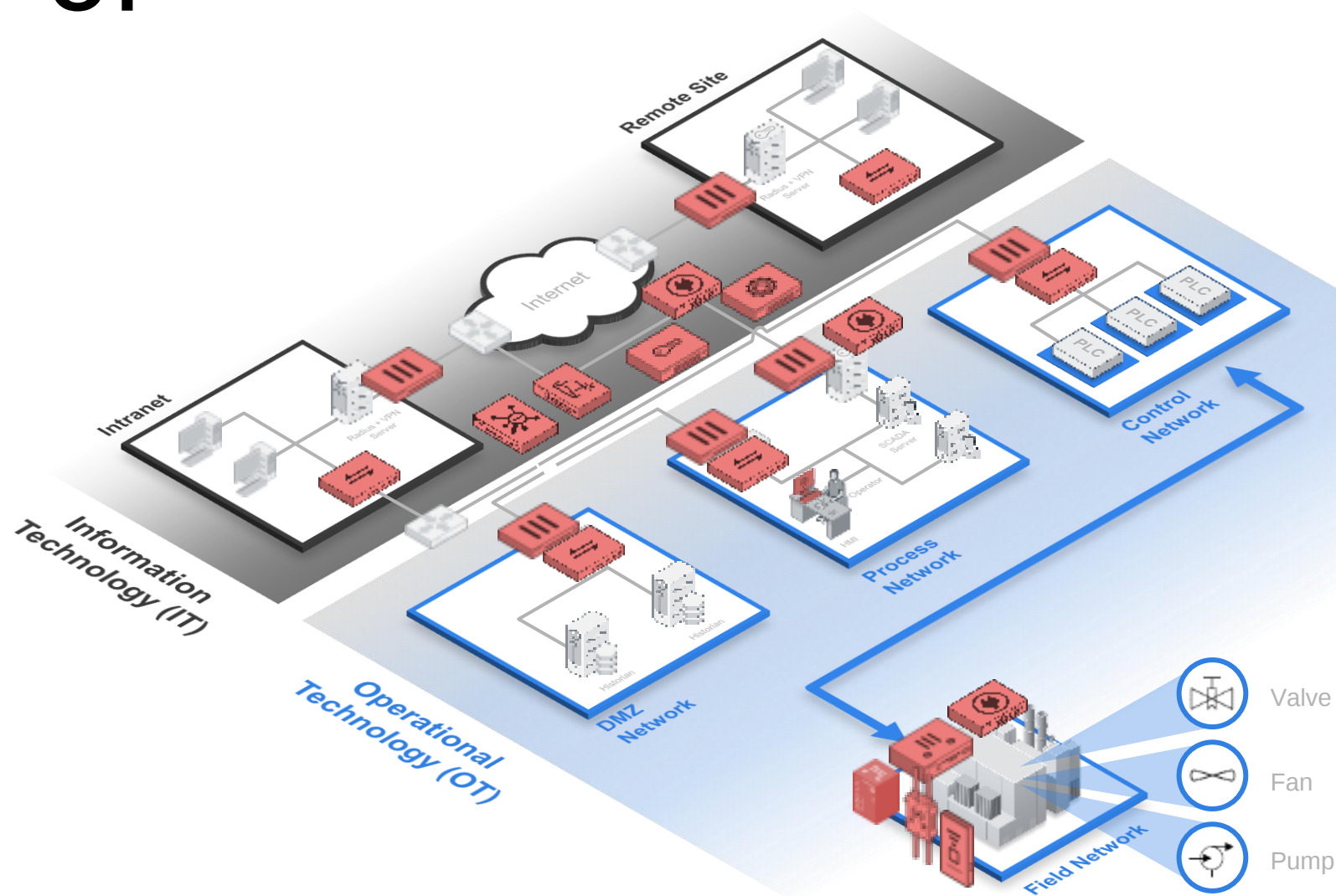
Носители угроз



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

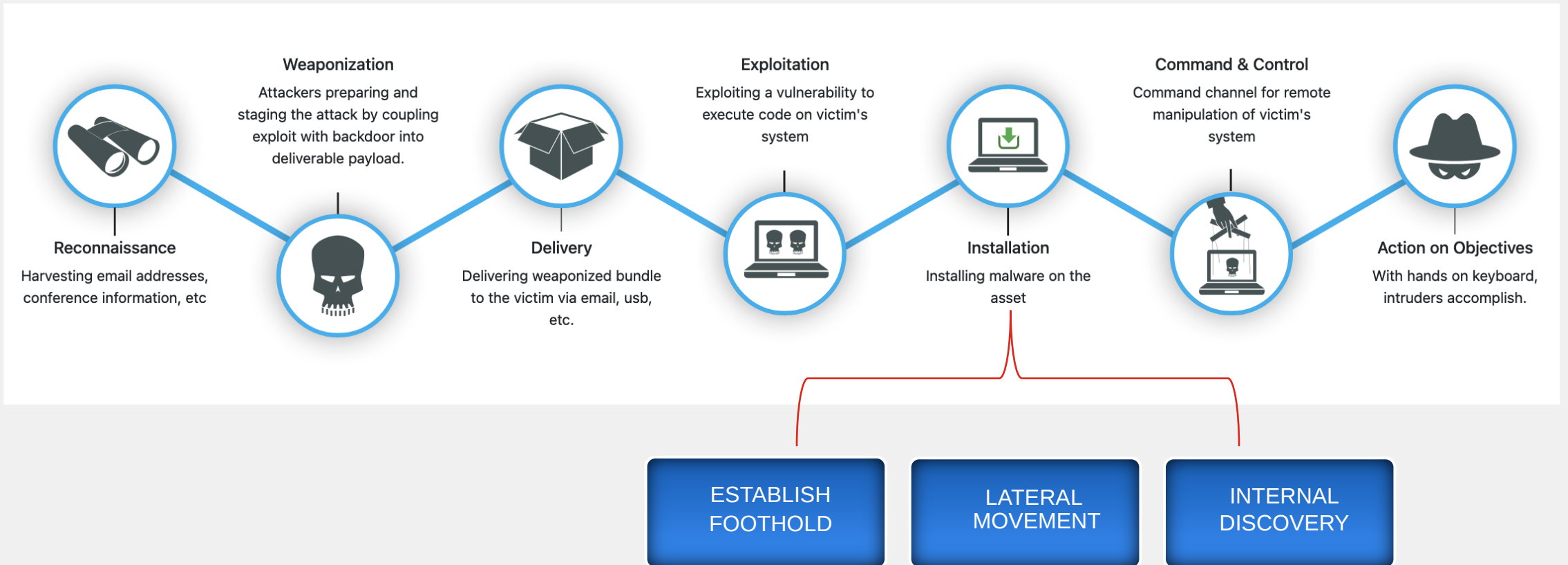
Сбор логов, корреляция и аудит и автоматическое реагирование (FortiAnalyzer, FortiSIEM/FortiSOAR)

Автоматизация выявления нарушителя и реагирование (FortiDeceptor)

На основе стандартного подхода и решения Fortinet Security Fabric



Cyber Kill Chain (APT)



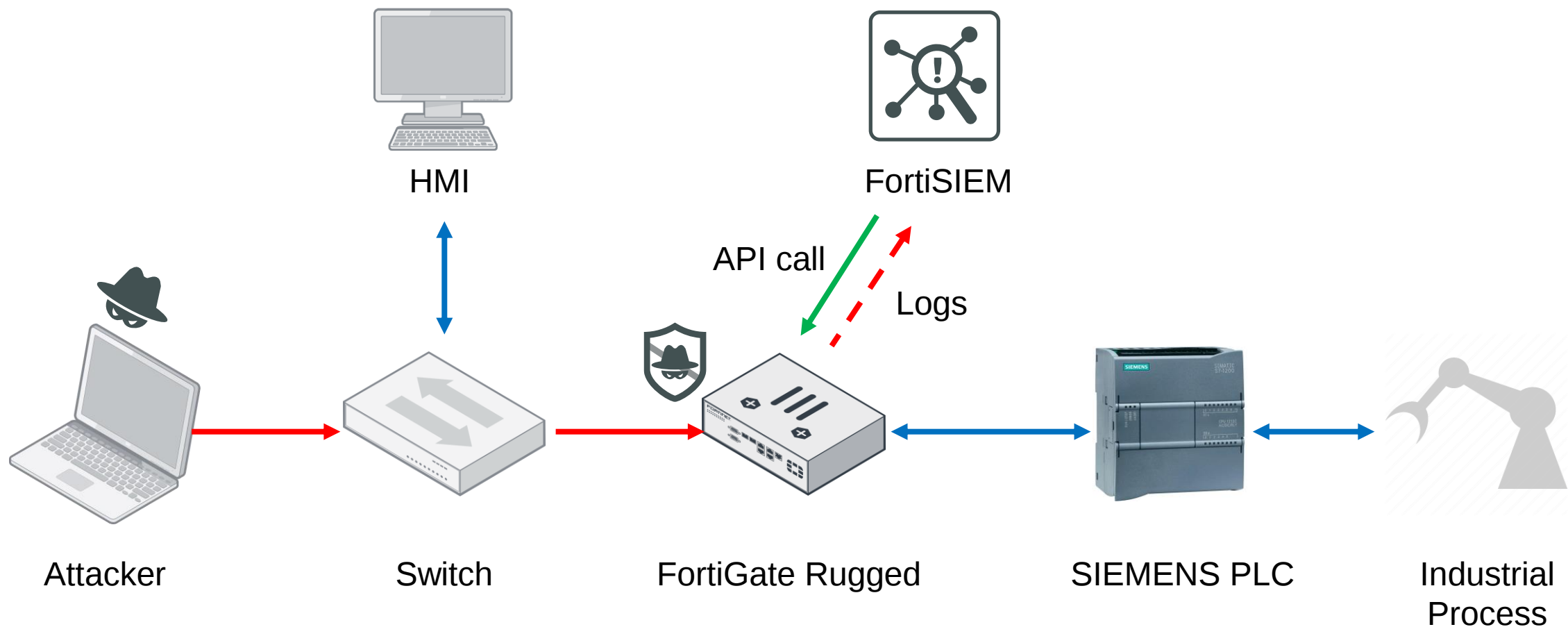


FortiSIEM

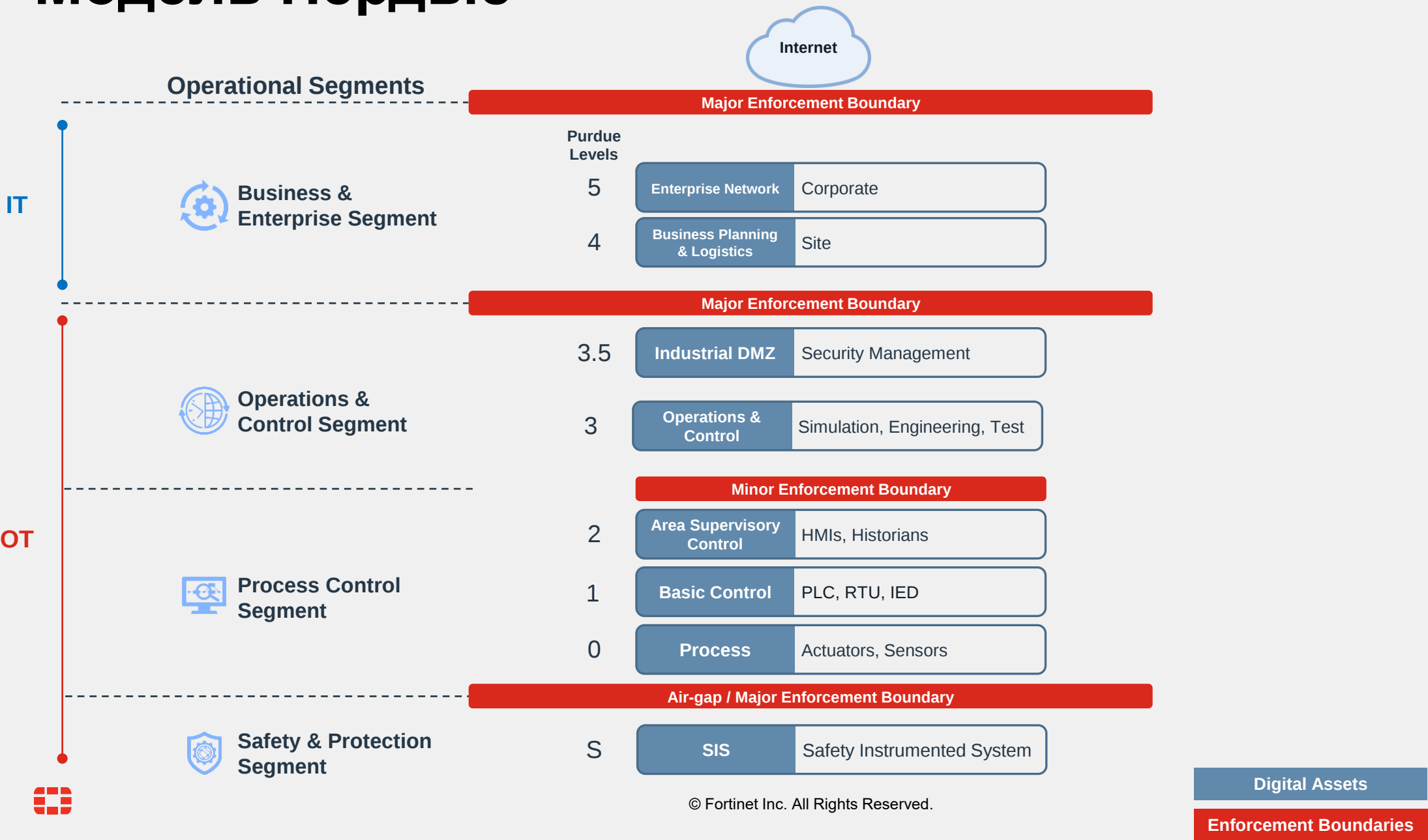
Мониторинг, обнаружение и разрушение атаки



Пример ОТ сети



Модель Пердю



Моделируйте Вашу инфраструктуру

Малпинг устройств к уровню Пердью

FortiSIEM

DASHBOARD ANALYTICS INCIDENTS CASES CMDB

Devices Applications Users Business Services IT Srvc Biz Srvc Compliance Operational Technology Ungrouped CMDB Reports

CMDB > Business Services > Operational Technology

New Edit Delete Discovered by All Search...

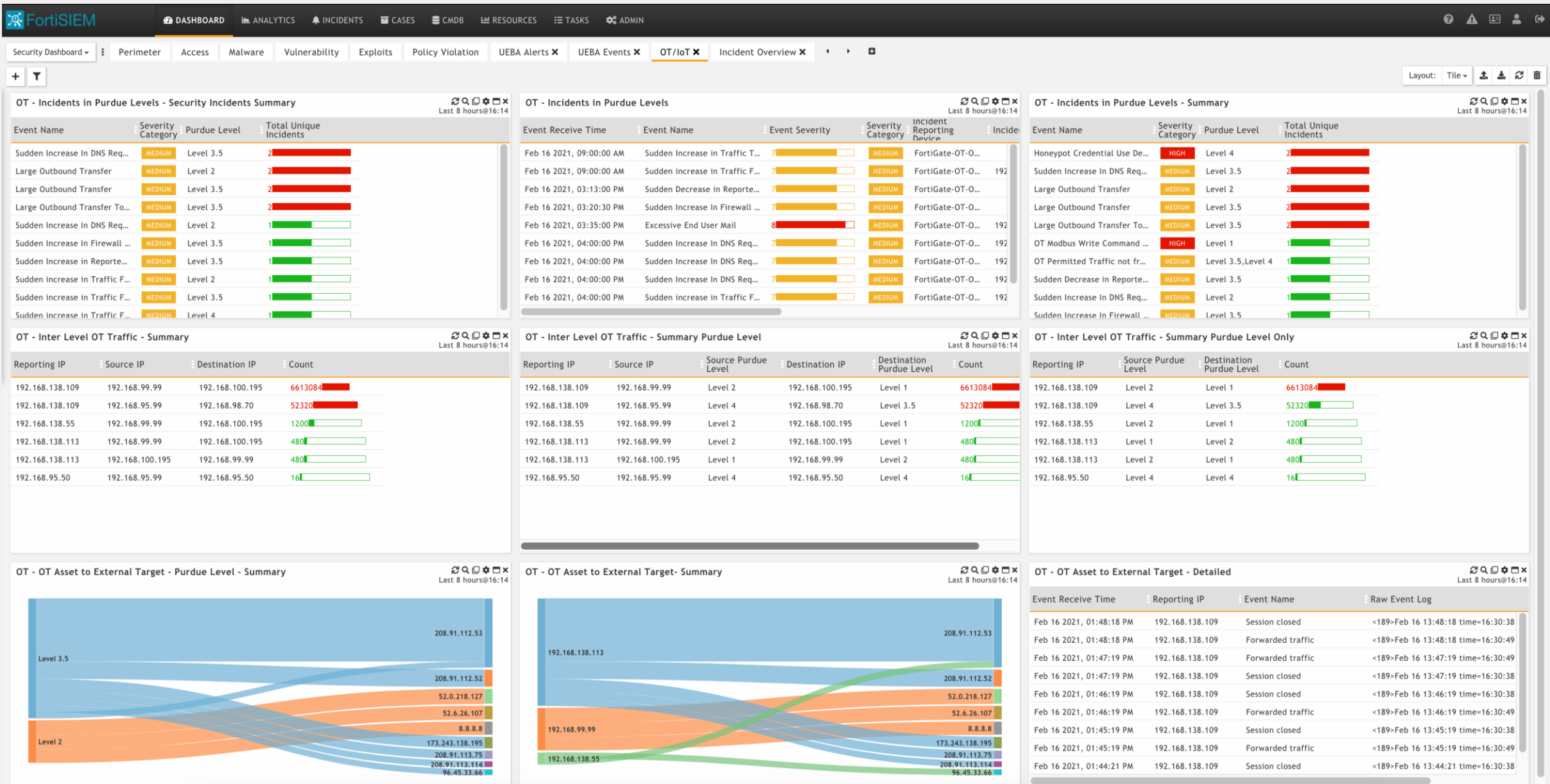
Name	Members
Level 5	0
Level 4	2
Level 3.5	1
Level 3	0
Level 2	1
Level 1	2
Level 0	0

Members Auto expand

Type	Name	Running On	Access IP
Device	PLC1-PCN-A2		192.168.100.197
Device	PLC1-PCN-A1		192.168.100.195



Панель управления



Инциденты

FortiSIEM

DASHBOARD

ANALYTICS

INCIDENTS

CASES

CMDB

RESOURCES

TASKS

ADMIN

Security Dashboard

Perimeter

Access

Malware

Vulnerability

Exploits

Policy Violation

UEBA AI Alerts

UEBA Events

OT/IoT

+

Y

Layout: Tile

📄

📥

🔄

🗑️

Last 30 days@6:15

OT: All Incident Summary

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 Permitted Traffic not from Purdue Level 4 to Level 3.5	MEDIUM	Level 3.5	6	
OT Permitted Traffic not from Purdue Level 3 to Level 2	MEDIUM	Level 2	4	
No logs from a device	MEDIUM	Level 1	2	
OT Permitted 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 Permitted Traffic not from Purdue Level 3 to Level 2	MEDIUM	Level 2,Level 3.5	1	

Деградация

Влияние

Обнаружение аномалий

Снижение защиты

Нарушение уровня Пердью

Первоначальный доступ или на постоянной основе

Передача C2 трафика



Финальные стадии

FortiSIEM

DASHBOARD

ANALYTICS

INCIDENTS

CASES

CMDB

RESOURCES

TASKS

ADMIN

Security Dashboard

Perimeter

Access

Malware

Vulnerability

Exploits

Policy Violation

UEBA AI Alerts

UEBA Events

OT/IoT

+

Y

Layout: Tile

🔄

📄

🔍

⌵

🗑

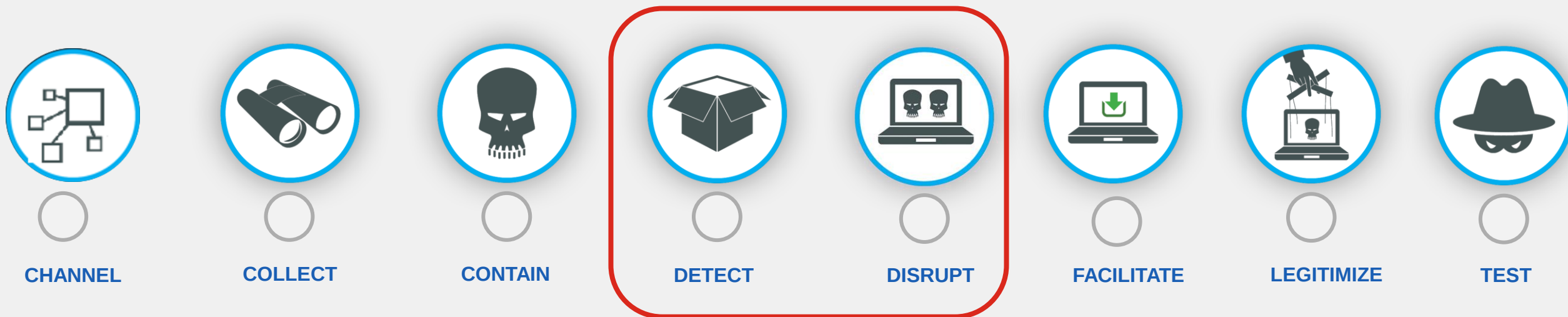
OT: All Incident Summary

Last 30 days@6:15

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 Permitted Traffic not from Purdue Level 4 to Level 3.5	MEDIUM	Level 3.5	6	
OT Permitted Traffic not from Purdue Level 3 to Level 2	MEDIUM	Level 2	4	
No logs from a device	MEDIUM	Level 1	2	
OT Permitted 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 Permitted 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

FortiSIEM DASHBOARD ANALYTICS INCIDENTS CASES CMDB RESOURCES TASKS ADMIN														
Actions Overview List Risk Explorer UEBA MITRE ATT&CK® Rule Coverage														
Search technique... (205/205) Show All 958 Rules - 76% Coverage Techniques														
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact	
12	0	42	113	152	131	290	121	63	37	38	57	39	202	
10 Tech 32 Sub-Tech	6 Tech 26 Sub-Tech	9 Tech 16 Sub-Tech	10 Tech 25 Sub-Tech	18 Tech 84 Sub-Tech	12 Tech 79 Sub-Tech	37 Tech 124 Sub-Tech	14 Tech 41 Sub-Tech	25 Tech 32 Sub-Tech	9 Tech 18 Sub-Tech	17 Tech 28 Sub-Tech	16 Tech 30 Sub-Tech	9 Tech 12 Sub-Tech	13 Tech 21 Sub-Tech	
Search Closed Sources	Compromise Infrastructure	Valid Accounts [23]	Software Deployment Tools	Office Application Startup [1]	Boot or Logon Initialization Scripts [2]	Masquerading [31]	Unsecured Credentials [8]	Software Discovery [2]	Remote Service Session Hijacking [2]	Data Staged [5]	Application Layer Protocol [9]	Exfiltration Over Physical Medium [1]	Endpoint Denial of Service [103]	
Phishing for Information [1]	Acquire Infrastructure	External Remote Services [4]	System Services [7]	Boot or Logon Initialization Scripts [2]	Access Token Manipulation [4]	Subvert Trust Controls	Steal or Forge Kerberos Tickets [6]	System Owner/User Discovery [5]	Software Deployment Tools	Man in the Browser	Encrypted Channel	Exfiltration Over Web Service [2]	Network Denial of Service [29]	
Search Open Technical Databases	Obtain Capabilities	Replication Through Removable Media [1]	User Execution [16]	Browser Extensions	Abuse Elevation Control Mechanism [16]	Obfuscated Files or Information [14]	Steal Web Session Cookie	Virtualization/Sandbox Evasion	Use Alternate Authentication Material [7]	Data from Removable Media [3]	Protocol Tunneling [4]	Automated Exfiltration [1]	Disk Wipe	
Active Scanning [11]	Develop Capabilities	Phishing [7]	Scheduled Task/Job [12]	Create Account [13]	Scheduled Task/Job [12]	Use Alternate Authentication Material [7]	Man-in-the-Middle [7]	Network Share Discovery [2]	Exploitation of Remote Services [4]	Man-in-the-Middle [7]	Non-Standard Port [2]	Exfiltration Over Alternative Protocol [9]	Resource Hijacking	
Search Victim-Owned Websites	Compromise Accounts	Hardware Additions [1]	Inter-Process Communication [2]	Scheduled Task/Job [12]	Process Injection [13]	Abuse Elevation Control Mechanism [16]	Network Sniffing [5]	System Network Connections Discovery [2]	Lateral Tool Transfer	Data from Network Shared Drive [1]	Communication Through Removable Media	Exfiltration Over Other Network Medium	Firmware Corruption	
Gather Victim Host Information [1]	Establish Accounts	Supply Chain Compromise [1]	Windows Management Instrumentation [11]	Traffic Signaling	Exploitation for Privilege Escalation [4]	Modify Authentication Process	Modify Authentication Process	Password Policy Discovery [2]	Remote Services [23]	Data from Configuration Repository [1]	Non-Application Layer Protocol [4]	Data Transfer Size Limits	Inhibit System Recovery [4]	
Search Open Websites/Domains		Trusted Relationship [1]	Exploitation for Client Execution [4]	BITS Jobs [2]	Group Policy Modification [2]	Process Injection [13]	Steal Application Access Token [3]	Cloud Service Dashboard	Replication Through Removable Media [1]	Data from Cloud Storage Object [1]	Traffic Signaling	Transfer Data to Cloud Account [1]	Service Stop [22]	
Gather Victim Org Information		Drive-by Compromise [1]	Native API [1]	Compromise Client Software Binary [1]	Valid Accounts [23]	Hide Artifacts [5]	Credentials from Password Stores [1]	Network Sniffing [5]	Internal Spearphishing	Data from Local System [2]	Proxy [9]	Scheduled Transfer	Defacement [1]	
Gather Victim Network Information [7]		Exploit Public-Facing Application [4]	Command and Scripting Interpreter [71]	Valid Accounts [23]	Hijack Execution Flow [17]	Impair Defenses [49]	Forced Authentication	Account Discovery [11]	Taint Shared Content	Input Capture [1]	Data Obfuscation [2]	Exfiltration Over C2 Channel [25]	Data Encrypted for Impact [2]	
Gather Victim Identity Information			Shared Modules [1]	Server Software Component [8]	Create or Modify System Process [9]	Valid Accounts [23]	OS Credential Dumping [44]	Network Service Scanning [12]		Screen Capture [1]	Web Service		Data Destruction [2]	
				Hijack Execution Flow [17]	Event Triggered Execution [17]	Hijack Execution Flow [17]	Two-Factor Authentication [1]	Cloud Infrastructure Discovery [2]		Data from Information [1]	Ingress Tool Transfer [14]		Data Manipulation [20]	



Сработавшие правила(покрытие инцидентов)

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 8 Days

🔍 Search technique... (23/23)

Show Triggered

4746 Incidents in Last 8 Days

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
3 2 Tech 4 Sub-Tech	0 0 Tech 0 Sub-Tech	62 2 Tech 2 Sub-Tech	4376 1 Tech 1 Sub-Tech	67 3 Tech 3 Sub-Tech	3 1 Tech 1 Sub-Tech	4 2 Tech 2 Sub-Tech	91 1 Tech 1 Sub-Tech	49 2 Tech 2 Sub-Tech	59 1 Tech 1 Sub-Tech	1 1 Tech 1 Sub-Tech	71 3 Tech 3 Sub-Tech	85 2 Tech 2 Sub-Tech	64 2 Tech 2 Sub-Tech
Active Scanning [3]		Valid Accounts [3]	User Execution [4376]	Valid Accounts [3]	Valid Accounts [3]	Impair Defenses [1]	Brute Force [91]	Network Service Scanning [46]	Remote Services [59]	Email Collection [1]	Application Layer Protocol [3]	Exfiltration Over Alternative Protocol [32]	Network Denial of Service [60]
Gather Victim Network Information [3]	External Remote Services [59]			Account Manipulation [5]		Valid Accounts [3]		Remote System Discovery [3]			Dynamic Resolution [9]	Exfiltration Over C2 Channel [53]	Service Stop [4]
				External Remote Services [59]							Remote Access Software [59]		

Исследование инцидента

FortiSIEM

DASHBOARDANALYTICSINCIDENTSCASESCMDBRESOURCESTASKSADMIN

Actions

OverviewListRiskExplorerUEBAMITRE ATT&CK® Incident Explorer1 minute

Status: ActiveTime Range: Last 15 Days

Tactics: AllSearch devices... (6685/6685)

Device	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
10.0.100.11			92		92					92		92	7	1
host-148.251.132.252								12					83	
ERP	3								49		1	4	1	2
_gateway								51						
[Empty]														51
external_webserver								8				1	25	
fdc-vm0000000000								34						
fortigate_edge							1	18						12

Related Incidents1/3426,839

Severity Category	Last Occurred	Incident	Tactics	Technique	Source	Target	Detail	Incident Status	Resolution
HIGH	Jun 28 2021, 12:38:30 PM	WMI Service Unavailable	Impact	Service Stop		10.0.0.20 WIN-PQCRJH7CVRJ		Active	Open
HIGH	Jun 28 2021, 12:38:30 PM	Backdoor Found	Execution	User Execution: Malicious Li...	46.70.155.2		Component Event Type: FortiGate-ips-signature-43963 Signature Id: 43963	Active	Open
HIGH	Jun 28 2021, 12:38:30 PM	Backdoor Found	Execution	User Execution: Malicious Li...	196.202.83.164		Component Event Type: FortiGate-ips-signature-43963 Signature Id: 43963	Active	Open
HIGH	Jun 28 2021, 12:38:30 PM	Backdoor Found	Execution	User Execution: Malicious Li...	110.38.1.13		Component Event Type: FortiGate-ips-signature-43963 Signature Id: 43963	Active	Open
HIGH	Jun 28 2021, 12:38:30 PM	Backdoor Found	Execution	User Execution: Malicious Li...	212.220.28.26		Component Event Type: FortiGate-ips-signature-43963 Signature Id: 43963	Active	Open
HIGH	Jun 28 2021, 12:38:30 PM	Suspicious logon attempt	Credential Access	Brute Force: Password Guess...	178.136.56.161	External_Webserver 10.0.0.6	Triggered Event Count: 1	Active	Open
HIGH	Jun 28 2021, 12:38:30 PM	Suspicious logon attempt	Credential Access	Brute Force: Password Guess...	171.226.29.78	External_Webserver 10.0.0.6	Triggered Event Count: 1	Active	Open
HIGH	Jun 28 2021, 12:38:30 PM	SNMP Service Unavailable	Impact	Service Stop		10.0.100.50 CP_443-1_EX40		Active	Open



Первоначальный доступ

FortiSIEM

DASHBOARD

ANALYTICS

INCIDENTS

CASES

CMDB

RESOURCES

TASKS

ADMIN

Actions

Overview

List

Risk

Explorer

UEBA

MITRE ATT&CK® Incident Explorer

1 minute

Tactics: All

Search devices...

(6689/6689)

1/335

6,689

Status: Active

Time Range: Last 15 Days

Device	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
10.0.100.11			91		91					91		91	7	1
host-148.251.132.252								12					83	
ERP	3								49		1	4	1	2
_gateway								51						
[Empty]														51
external_webserver								8				1	25	
fdc-vm0000000000								34						
fortigate_edge							1	18						12
102.5.124.22														

Initial Access Incidents for 10.0.100.11: 🗑️

1/5

91

Severity Category	Last Occurred	Incident	Tactics	Technique	Source	Target	Detail	Incident Status	Resolution
HIGH	Jun 28 2021, 12:47:30 PM	Remote Desktop from Internet	Persistence,Lateral Moveme...	External Remote Services, R...	🇺🇸 106.245.140.119	10.0.100.11		Active	Open
HIGH	Jun 28 2021, 12:21:30 PM	Remote Desktop from Internet	Persistence,Lateral Moveme...	External Remote Services, R...	🇺🇸 47.90.72.126	10.0.100.11		Active	Open
HIGH	Jun 28 2021, 11:18:30 AM	Remote Desktop from Internet	Persistence,Lateral Moveme...	External Remote Services, R...	🇺🇸 218.94.34.54	10.0.100.11		Active	Open
HIGH	Jun 28 2021, 11:06:30 AM	Remote Desktop from Internet	Persistence,Lateral Moveme...	External Remote Services, R...	🇺🇸 121.7.36.176	10.0.100.11		Active	Open
HIGH	Jun 28 2021, 10:06:30 AM	Remote Desktop from Internet	Persistence,Lateral Moveme...	External Remote Services, R...	🇺🇸 74.82.47.2	10.0.100.11		Active	Open
HIGH	Jun 28 2021, 10:06:30 AM	Remote Desktop from Internet	Remote Desktop from Internet	ernal Remote Services, R...	🇺🇸 137.135.96.145	10.0.100.11		Active	Open
HIGH	Jun 28 2021, 09:39:00 AM	Remote Desktop from Internet	Persistence,Lateral Moveme...	External Remote Services, R...	🇺🇸 195.78.54.230	10.0.100.11		Active	Open
HIGH	Jun 28 2021, 09:30:30 AM	Remote Desktop from Internet	Persistence,Lateral Moveme...	External Remote Services, R...	🇺🇸 195.78.54.73	10.0.100.11		Active	Open
HIGH	Jun 28 2021, 09:27:00 AM	Remote Desktop from Internet	Persistence,Lateral Moveme...	External Remote Services, R...	🇺🇸 185.202.2.147	10.0.100.11		Active	Open
HIGH	Jun 28 2021, 08:45:00 AM	Remote Desktop from Internet	Persistence,Lateral Moveme...	External Remote Services, R...	🇺🇸 13.213.66.119	10.0.100.11		Active	Open
HIGH	Jun 28 2021, 08:12:30 AM	Remote Desktop from Internet	Persistence,Lateral Moveme...	External Remote Services, R...	🇺🇸 185.252.145.204	10.0.100.11		Active	Open



Исполнение

🔍 Search technique... (23/23)

Show Triggered

4723 Incidents in Last 5 Days

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
3	0	61	4417	66	3	4	76	49	58	1	70	50	51
Active Scanning [3]		Valid Accounts [3]	User Execution [4417]	Valid Accounts [3]	Valid Accounts [3]	Impair Defenses [1]	Brute Force [76]	Network Service Scanning [46]	Remote Services [58]	Email Collection [1]	Application Layer Protocol [3]	Exfiltration Over Alternative Protocol [20]	Network Denial of Service [47]
Gather Victim Network Information [3]		External Remote Services [58]		Account Manipulation [5]		Valid Accounts [3]		Remote System Discovery [3]			Dynamic Resolution [9]	Exfiltration Over C2 Channel [30]	Service Stop [4]
				External Remote Services [58]							Remote Access Software [58]		

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

FortiSIEM

DASHBOARD

ANALYTICS

INCIDENTS

CASES

CMDB

RESOURCES

TASKS

ADMIN

?

⚠

📺

👤

➡

Actions

Overview

List

Risk

Explorer

UEBA

MITRE ATT&CK® Incident Explorer

1 minute

Tactics: All

Search devices...

(6685/6685)

Status: Active

Time Range: Last 15 Days

1/335

6,685

Device	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
10.0.100.11			92		92					92			7	1
host-148.251.132.252								12					83	
ERP	3								49		1	4	1	2
_gateway								51						
[Empty]														51
external_webserver								8				1	25	
fdc-vm0000000000								34						
fortigate_edge							1	18						12
102.5.124.22														

Related Incidents

1/342

6,839

Severity Category	Last Occurred	Incident	Tactics	Technique	Source	Target	Detail	Incident Status	Resolution
HIGH	Jun 28 2021, 12:38:30 PM	WMI Service Unavailable	Impact	Service Stop		10.0.0.20 WIN-PQCRJH7CVRJ		Active	Open
HIGH	Jun 28 2021, 12:38:30 PM	Backdoor Found	Execution	User Execution: Malicious Li...	46.70.155.2		Component Event Type: FortiGate-ips-signature-43963 Signature Id: 43963	Active	Open
HIGH	Jun 28 2021, 12:38:30 PM	Backdoor Found	Execution	User Execution: Malicious Li...	196.202.83.164		Component Event Type: FortiGate-ips-signature-43963 Signature Id: 43963	Active	Open
HIGH	Jun 28 2021, 12:38:30 PM	Backdoor Found	Execution	User Execution: Malicious Li...	110.38.1.13		Component Event Type: FortiGate-ips-signature-43963 Signature Id: 43963	Active	Open
HIGH	Jun 28 2021, 12:38:30 PM	Backdoor Found	Execution	User Execution: Malicious Li...	212.220.28.26		Component Event Type: FortiGate-ips-signature-43963 Signature Id: 43963	Active	Open
HIGH	Jun 28 2021, 12:38:30 PM	Suspicious logon attempt	Credential Access	Brute Force: Password Guess...	178.136.56.161	External_Webserver 10.0.0.6	Triggered Event Count: 1	Active	Open
HIGH	Jun 28 2021, 12:38:30 PM	Suspicious logon attempt	Credential Access	Brute Force: Password Guess...	171.226.29.78	External_Webserver 10.0.0.6	Triggered Event Count: 1	Active	Open
HIGH	Jun 28 2021, 12:38:30 PM	SNMP Service Unavailable	Impact	Service Stop		10.0.100.50 CP_443-1_EX40		Active	Open



Внутренняя разведка

FortiSIEM

DASHBOARD

ANALYTICS

INCIDENTS

CASES

CMDB

RESOURCES

TASKS

ADMIN

?

Actions

Overview

List

Risk

Explorer

UEBA

MITRE ATT&CK® Incident Explorer

1 minute

Status: Active

Time Range: Last 15 Days

Tactics: All

Search devices... (6689/6689)

1/335 6,689

Device	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
10.0.100.11			91		91					91		91	7	1
host-148.251.132.252								12					83	
ERP	3								49		1	4	1	2
_gateway								51						
[Empty]														51
external_webserver								8				1	25	
fdc-vm0000000000								34						
fortigate_edge							1	18						12
102.5.124.22														

Discovery Incidents for ERP: 49

Severity Category	Last Occurred	Incident	Tactics	Technique	Source	Target	Detail	Incident Status	Resolution
MEDIUM	Jun 28 2021, 07:16:30 AM	Heavy TCP Port Scan: Single Destination	Discovery	Network Service Scanning	10.0.0.52	10.0.100.39	Triggered Event Count: 30	Active	Open
MEDIUM	Jun 28 2021, 07:16:30 AM	Heavy TCP Port Scan: Single Destination	Discovery	Network Service Scanning	10.0.0.52	10.0.100.18	Triggered Event Count: 22	Active	Open
MEDIUM	Jun 28 2021, 07:16:30 AM	Heavy TCP Port Scan: Single Destination	Discovery	Network Service Scanning	10.0.0.52	10.0.100.22	Triggered Event Count: 24	Active	Open
MEDIUM	Jun 28 2021, 07:16:30 AM	Heavy TCP Port Scan: Single Destination	Discovery	Network Service Scanning	10.0.0.52	10.0.100.21	Triggered Event Count: 20	Active	Open
MEDIUM	Jun 28 2021, 07:16:30 AM	Heavy TCP Port Scan: Single Destination	Discovery	Network Service Scanning	10.0.0.52	10.0.100.44	Triggered Event Count: 28	Active	Open
MEDIUM	Jun 28 2021, 07:16:30 AM	Heavy TCP Port Scan: Single Destination	Discovery	Network Service Scanning	10.0.0.52	10.0.100.30	Triggered Event Count: 35	Active	Open
MEDIUM	Jun 28 2021, 07:16:30 AM	Heavy TCP Port Scan: Single Destination	Discovery	Network Service Scanning	10.0.0.52	10.0.100.29	Triggered Event Count: 31	Active	Open
MEDIUM	Jun 28 2021, 07:16:30 AM	Heavy TCP Port Scan: Single Destination	Discovery	Network Service Scanning	10.0.0.52	10.0.100.62	Triggered Event Count: 33	Active	Open
MEDIUM	Jun 28 2021, 07:16:30 AM	Heavy TCP Port Scan: Single Destination	Discovery	Network Service Scanning	10.0.0.52	10.0.100.40	Triggered Event Count: 33	Active	Open
MEDIUM	Jun 28 2021, 07:15:30 AM	Heavy TCP Port Scan: Multiple Destinations	Discovery	Network Service Scanning	10.0.0.52		Triggered Event Count: 40	Active	Open
MEDIUM	Jun 28 2021, 07:14:30 AM	Multiple IPS Detected Scans From Same Src	Discovery	Network Service Scanning	10.0.0.52		Triggered Event Count: 61	Active	Open
MEDIUM	Jun 28 2021, 07:14:30 AM	Heavy TCP Port Scan: Single Destination	Discovery	Network Service Scanning	10.0.0.52	10.0.100.31	Triggered Event Count: 50	Active	Open

Вывод данных

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	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
3	0	61	4417	66	3	4	76	49	58	1	70	50	51
Active Scanning [3]		Valid Accounts [3]	User Execution [4417]	Valid Accounts [3]	Valid Accounts [3]	Impair Defenses [1]	Brute Force [76]	Network Service Scanning [46]	Remote Services [58]	Email Collection [1]	Application Layer Protocol [3]	Exfiltration Over Alternative Protocol [20]	Network Denial of Service [47]
Gather Victim Network Information [3]		External Remote Services [58]		Account Manipulation [5]		Valid Accounts [3]		Remote System Discovery [3]			Dynamic Resolution [9]	Exfiltration Over C2 Channel [30]	Service Stop [4]
				External Remote Services [58]							Remote Access Software [58]		

Incidents related to Exfiltration Over Alternative Protocol

Columns: 7 Selected

1/120

Severity Category	Last Occurred	Event Name	Tactics	Technique	Target	Detail
MEDIUM	Jun 27 2021, 02:37:30 PM	Large Outbound Transfer	Exfiltration	Exfiltration Over Alternative Protocol: Exfi...	173.243.143.6	Sent Bytes64: 12.57 MB
HIGH	Jun 27 2021, 02:37:30 PM	Large Outbound Transfer To Outside My Country	Exfiltration	Exfiltration Over Alternative Protocol: Exfi...	173.243.143.6	Sent Bytes64: 12.57 MB
HIGH	Jun 27 2021, 02:10:00 PM	Large Outbound Transfer To Outside My Country	Exfiltration	Exfiltration Over Alternative Protocol: Exfi...	64.4.54.254	Sent Bytes64: 4.48 MB
HIGH	Jun 26 2021, 08:35:00 PM	Large Outbound Transfer To Outside My Country	Exfiltration	Exfiltration Over Alternative Protocol: Exfi...	173.243.140.6	Sent Bytes64: 3.16 MB
MEDIUM	Jun 26 2021, 07:29:30 PM	Large Outbound Transfer	Exfiltration	Exfiltration Over Alternative Protocol: Exfi...	208.184.237.67	Sent Bytes64: 8.62 MB
HIGH	Jun 26 2021, 07:29:30 PM	Large Outbound Transfer To Outside My Country	Exfiltration	Exfiltration Over Alternative Protocol: Exfi...	208.184.237.67	Sent Bytes64: 3.75 MB
HIGH	Jun 26 2021, 11:11:30 AM	Large Outbound Transfer To Outside My Country	Exfiltration	Exfiltration Over Alternative Protocol: Exfi...	173.243.138.69	Sent Bytes64: 4.88 MB
MEDIUM	Jun 26 2021, 11:11:00 AM	Large Outbound Transfer	Exfiltration	Exfiltration Over Alternative Protocol: Exfi...	173.243.138.69	Sent Bytes64: 9.64 MB
HIGH	Jun 26 2021, 10:15:00 AM	Large Outbound Transfer To Outside My Country	Exfiltration	Exfiltration Over Alternative Protocol: Exfi...	173.243.138.67	Sent Bytes64: 9.97 MB
MEDIUM	Jun 26 2021, 10:15:00 AM	Large Outbound Transfer	Exfiltration	Exfiltration Over Alternative Protocol: Exfi...	173.243.138.67	Sent Bytes64: 9.97 MB

© Fortinet Inc. All Rights Reserved.

32

Выполнение миссии

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

4727 Incidents in Last 5 Days

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
3	0	61	4419	66	3	4	78	49	58	1	70	50	51
Active Scanning [3]		Valid Accounts [3]	User Execution [4419]	Valid Accounts [3]	Valid Accounts [3]	Impair Defenses [1]	Brute Force [78]	Network Service Scanning [46]	Remote Services [58]	Email Collection [1]	Application Layer Protocol [3]	Exfiltration Over Alternative Protocol [20]	Network Denial of Service [47]
Gather Victim Network Information [3]		External Remote Services [58]		Account Manipulation [5]		Valid Accounts [3]		Remote System Discovery [3]			Dynamic Resolution [9]	Exfiltration Over C2 Channel [30]	Service Stop [4]
				External Remote Services [58]							Remote Access Software [58]		

Health for PLC-3

Incidents related to Service

Severity Category Last Occurred

HIGH Jun 28 2021, 12:51:00

HIGH Jun 28 2021, 12:50:00

HIGH Jun 28 2021, 10:18:00

HIGH Jun 27 2021, 01:34:00

Availability Status: Down

Performance Status:

Uptime: Uptime % (30 d):

Events Per Second (Avg): 0.02

Ping Round Trip: 1 ms

Incidents (Last 24 hrs): High: 1 Medium: 1 Low: 0

Monitor Status

Metric	Last Successful	Status
Uptime	15m 21s ago	Critical

Incident Status for 24 Hours

Severity	Event Name	COUNT(Matched Events)
HIGH	SNMP Service Unavailable	1

selected

1/1 4

ckSvcGroup

Расследование инцидента

FortiSIEM

DASHBOARD

ANALYTICS

INCIDENTS

CASES

CMDB

RESOURCES

TASKS

ADMIN

?

⚠

📄

👤

↔

⚙ Actions

📄 Overview

☰ List

📊 Risk

📊 Explorer

👤 UEBA

MITRE ATT&CK Incident Explorer

🔄 1 minute

Status: Active

🕒 Time Range: Last 15 Days

PLC-3

2

2

2

2

HMI-1

1

2

2

2

2

HISTORIAN

4

2

Incidents for HMI-1: 🗑

⏮ < 1/1 6 > ⏭

Severity Category	Last Occurred	Incident	Tactics	Technique	Source	Target	Detail	Incident Status	Resolution
HIGH	Jun 28 2021, 07:05:00 AM	WMI Service Unavailable	Impact	Service Stop		10.0.0.20 WIN-PQCRJH7CVRJ		Active	Open
HIGH	Jun 28 2021, 06:19:30 AM	Remote Desktop from Internet	Persistence,Lateral ...	External Remote Ser...	🇮🇳 103.5.134.23	10.0.0.20		Active	Open
MEDIUM	Jun 27 2021, 01:35:30 PM	Sudden Increase in Network Int...	Impact	Network Denial of S...		WIN-PQCRJH7CVRJ 10.0.0.20	Host Interface Name: Intel(R) 82574L Gigabit Ne... Sent Bytes64: 59.86 KB Received Bytes64: 31.63 KB ... Show More	Active	Open
HIGH	Jun 27 2021, 01:34:00 PM	Auto Service Stopped	Impact	Service Stop		10.0.0.20 WIN-PQCRJH7CVRJ	Service Name: CDPUserSvc_6a198cdc Service Path: C:\Windows\system32\svchost.exe	Active	Open

Triggering Events

Subpattern: RDP

☐ Wrap Raw Events

☐ Show Event Type

☐ Show Raw Event Only

Event Receive Time	Event Name	Source IP	Destination IP	Win Logon Type	Raw Event Log
Jun 28 2021, 06:18:31 AM	Forwarded traffic	🇮🇳 103.5.134.23	10.0.0.20		<189>logver=700000066 timestamp=1624846705 devname="Fortigate_Edge" devid="FGVMU...



Расследование инцидента (Device View)

FortiSIEM

DASHBOARD

ANALYTICS

INCIDENTS

CASES

CMDB

RESOURCES

TASKS

ADMIN

?

Actions

Overview

List by Device

Risk

Explorer

UEBA

MITRE ATT&CK

1 minute

Search

15m1h1d7d30d

Top Impacted Devices

10.0.100.11 (504)	HISTORIAN (10)	Fortigate_Edge (7)	External_Webserver (5)	41.160.25.212 (4)	200.165.167.131 (4)	36.95.98.189 (3)	103.5.134.23 (3)
PLC-2 (2)	PLC-1 (2)	95.189.96.188 (2)	95.188.64.91 (2)	95.187.33.178 (2)	95.181.2.239 (2)	95.141.140.102 (2)	94.29.124.76 (2)
94.233.250.173 (2)	94.182.8.93 (2)	94.159.62.134 (2)	93.41.200.206 (2)	93.124.52.120 (2)	92.54.217.172 (2)	92.51.30.12 (2)	91.99.252.161 (2)
91.98.183.116 (2)	91.93.65.59 (2)	91.92.125.62 (2)	91.236.177.24 (2)	91.215.89.205 (2)	91.215.69.216 (2)	91.209.70.244 (2)	91.207.5.24 (2)

Incidents for Fortigate_Edge

1/17

Severity Category	Last Occurred	Incident	Tactics	Technique	Reporting	Source	Target	Detail	Incident Status	Resolution
MEDIUM	Jun 28 2021, 01:21:30 PM	OT Permitted Traffic not from Purdue			Fortigate_Edge	10.0.0.3	10.0.0.15	Component Event Type: FortiGate-ips-signature-43963 Attack Name: Backdoor.DoublePulsar Signature Id: 43963 ... Show More	Active	Open
MEDIUM	Jun 28 2021, 01:21:00 PM	Sudden Increase In Firewall Connections	Impact	Network Denial of Service	Fortigate_Edge		Fortigate_Edge 10.0.0.3	Firewall Session: 211 Avg Firewall Conn: 163.87 Std Firewall Conn: 3.16	Active	Open
MEDIUM	Jun 28 2021, 01:20:30 PM	Sudden Increase in Network Interface Traffic	Impact	Network Denial of Service	Fortigate_Edge		Fortigate_Edge 10.0.0.3	Host Interface Name: port4 Sent Bytes64: 24.11 KB Received Bytes64: 20.94 KB ... Show More	Active	Open
MEDIUM	Jun 28 2021, 01:20:30 PM	Sudden Increase in Network Interface Traffic	Impact	Network Denial of Service	Fortigate_Edge		Fortigate_Edge 10.0.0.3	Host Interface Name: port3 Sent Bytes64: 19.08 MB Received Bytes64: 442.39 KB ... Show More	Active	Open

DetailsRule

Auto expand

Attributes

Search attribute name...

Biz Service: Level 3.5,Level 5

Category: Security

Count: 34

Event Name: OT Permitted Traffic not from Purdue

Level 4 to Level 3.5

Event Type: PH_RULE_TRAFFIC_NOT_L4_TO_L35

First Occurred: Jun 28 2021, 06:53:00 AM

Incident ID: 39943

Incident Title: OT Permitted Traffic not from Purdue

Level 4 10.0.0.3 to Level 3 10.0.0.15

Incident Comments

Add comments to Incident...

ClearSave

Action History

Time	Action	Result	Detail
------	--------	--------	--------

Copyright © 2021 Fortinet, Inc. All rights reserved.

Organization: Super User: admin Scope: Local

FortiSIEM 6.2.0 (0219)

Расследование инцидента(Case)

Actions

Overview

List by Incident

Risk

Explorer

UEBA

MITRE ATT&CK

1 minute

Search

Change Display Columns

Clear All Incidents in View

Search

Show Locations

Change Severity

Clear Incident

Create Event Dropping Rule

Create Case

Disable Rule

Edit Comment

Edit Rule

Edit Rule Exception

Export Incident

Notify via Email

Remediate Incident

Resolve Incident

Run External Integration...

Show Ticket History

15m 1h 1d 7d 30d

Q OT (4/15)

Top Impacted Incidents

Incident

OT Permitted Traffic not from Purdue Level 3 to Level 2

OT Permitted Traffic not from Purdue Level 3 to Level 2

OT Permitted Traffic not from Purdue Level 3 to Level 2

OT Permitted Traffic not from Purdue Level 3 to Level 2

OT Permitted Traffic not from Purdue Level 3 to Level 2

New Ticket

Incident IDs: 66082 Mode: Create a new ticket Add to an existing ticket

Summary: OT Permitted Traffic not from Purdue Level 3 192.168.1.50 to Level 2 10.0.0.20, in Fortigate_Edge(10.0.0.3)

State: New Assignee: []

Escalation: None Selected Priority: []

Due Date: 07/04/2021 Attachment: []

Assignee Time Zone: Local Europe/Berlin

CC: []

Notes: Incident Name => OT Permitted Traffic not from Purdue Level 3 192.168.1.50 to Level 2 10.0.0.20
Incident Source => IP Address:192.168.1.50,
Incident Target => Fortigate_Edge(10.0.0.3)
Incident Detail =>
Incident ID => 66082

Save Cancel

Target

Detail

Incident Status

Re

Component Event Type: FortiGate-ips-signature-43963
Attack Name: Backdoor.DoublePulsar
Signature Id: 43963
... Show More

Component Event Type: FortiGate-ips-signature-43963
Attack Name: Backdoor.DoublePulsar
Signature Id: 43963
... Show More

Component Event Type: FortiGate-ips-signature-43963
Attack Name: Backdoor.DoublePulsar
Signature Id: 43963
... Show More

Details

Events

Rule

Auto expand

Attributes

Search attribute name...

Biz Service: Level 2
Category: Security
Count: 133
Event Name: OT Permitted Traffic not from Purdue Level 3 to Level 2
Event Type: PH_RULE_TRAFFIC_NOT_L3_TO_L2
First Occurred: Jul 04 2021, 06:52:00 PM
Incident ID: 66082
Incident Title: OT Permitted Traffic not from Purdue Level 3 192.168.1.50 to Level 2

Incident Comments

Add comments to Incident...

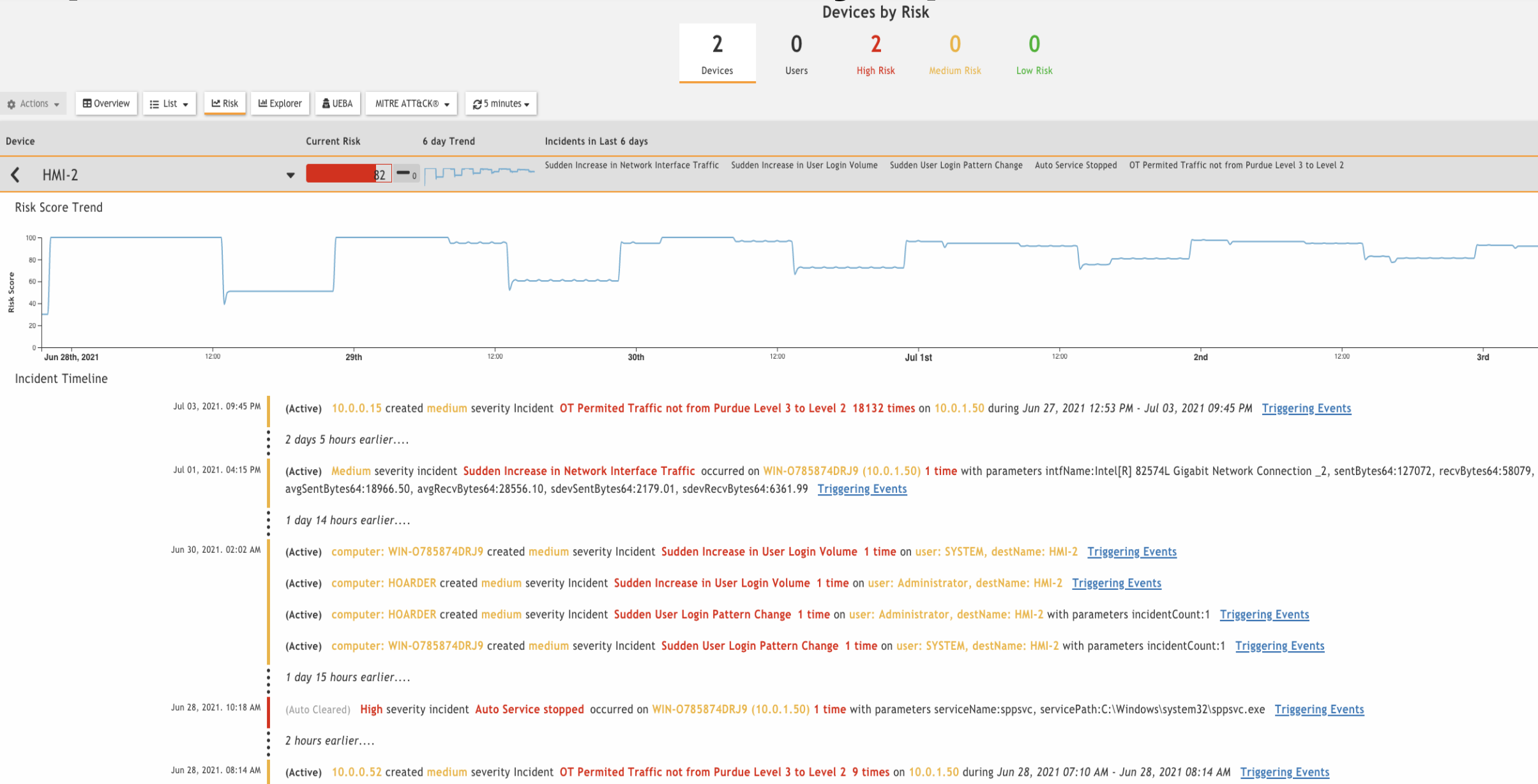
Clear Save

Action History

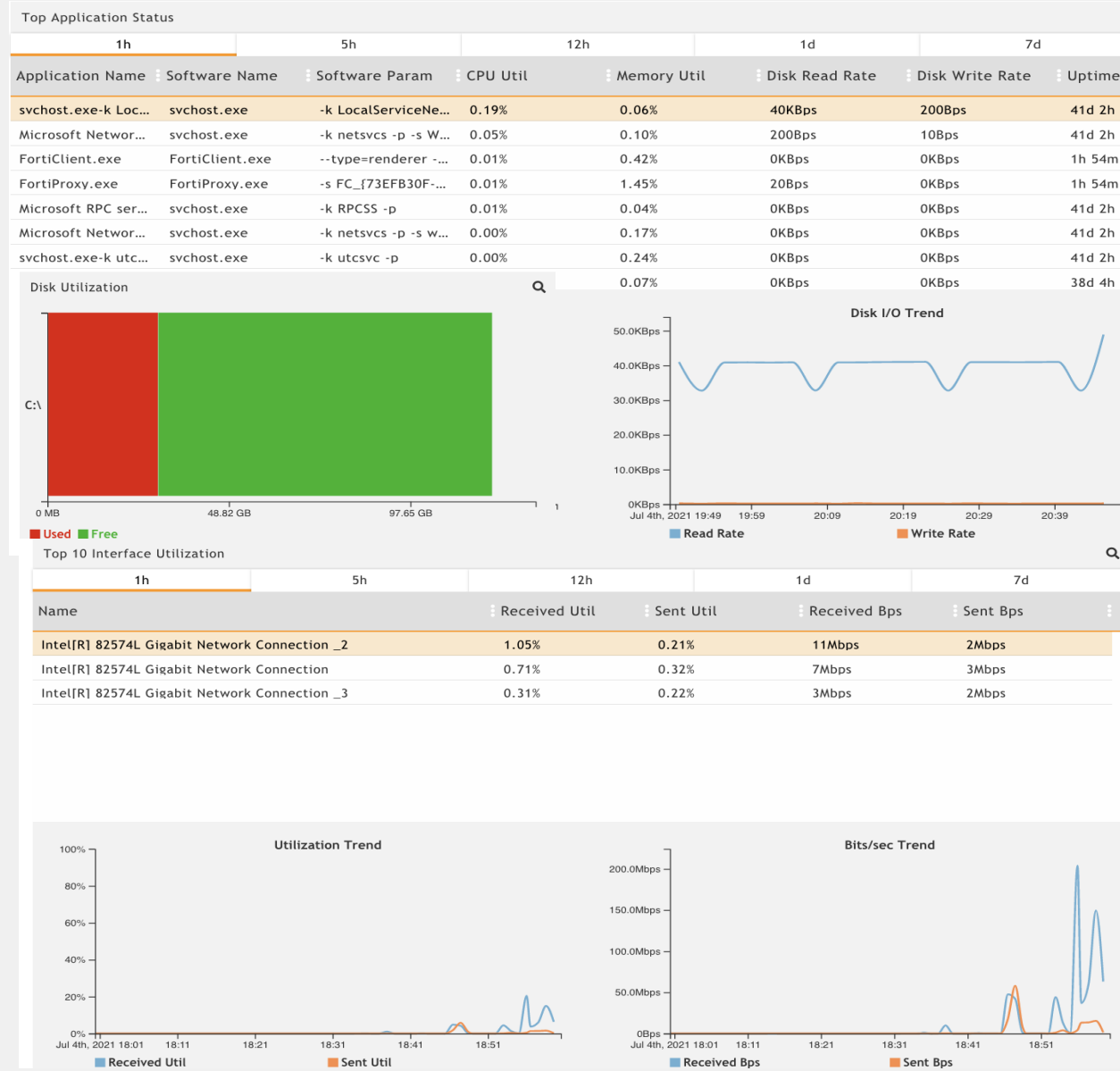
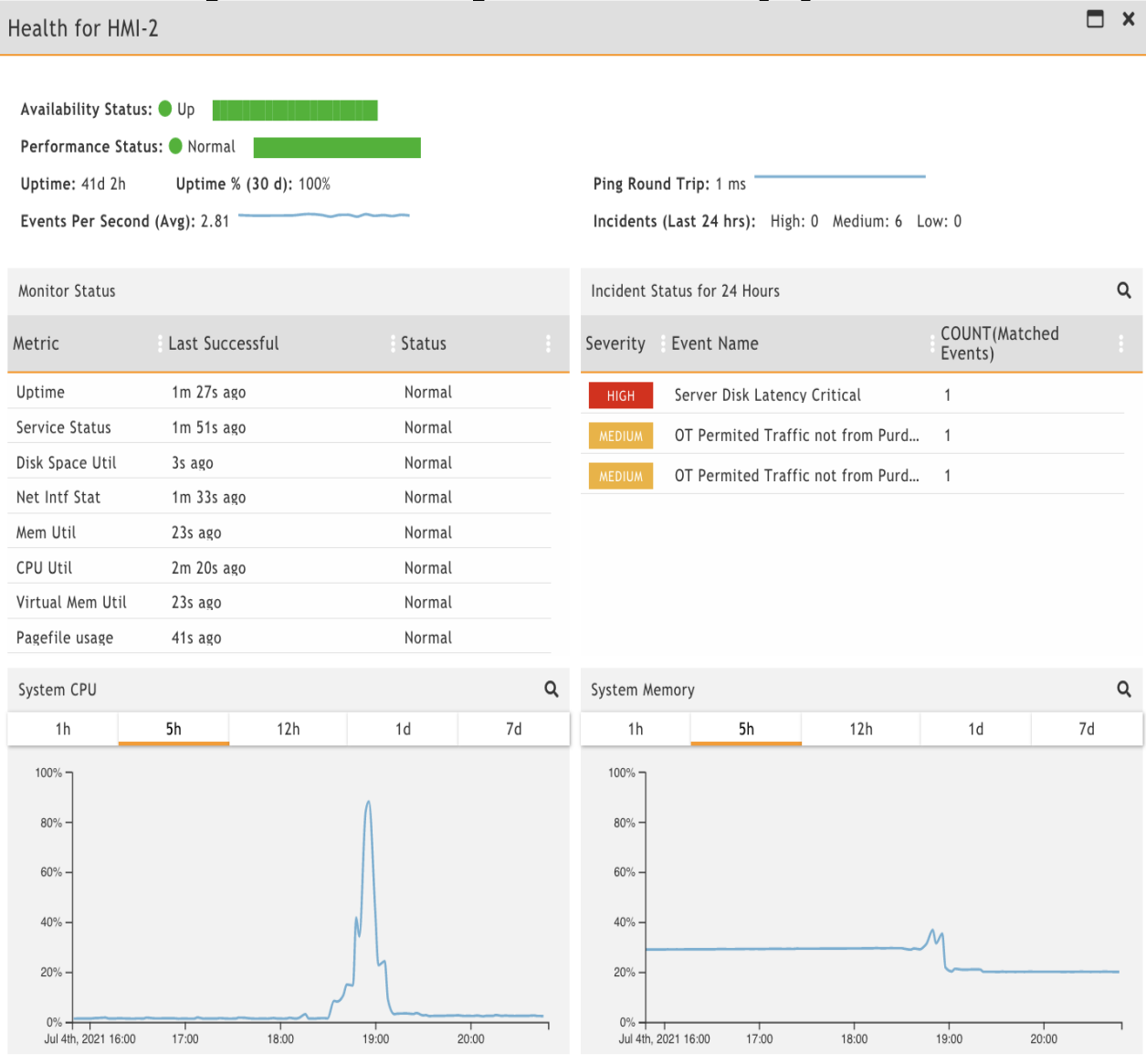
Time Action Result Detail



Хронология инцидентов по устройствам



Метрики производительности



Технологические партнеры и интеграторы

OT TECHNOLOGY PARTNERS

Visibility & Threat Intelligence



Operations, Orchestration Automation



Other



SOLUTION VENDORS AND SYSTEMS INTEGRATORS

Control Vendors



Global System Integrators



Other(s)



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

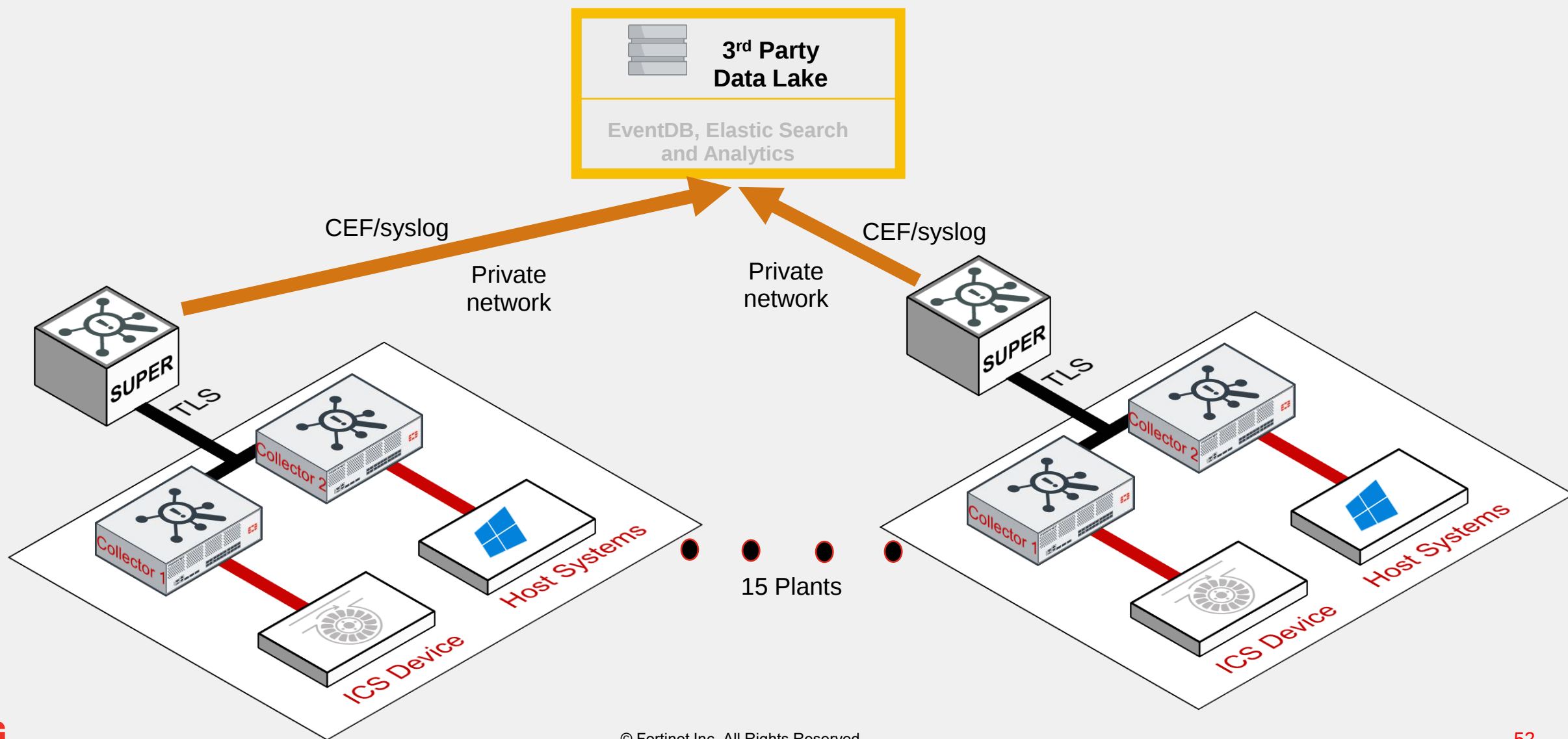
- Осведомленность, сегментация
- Простота настройки и внедрения
- Экспертиза безопасности в доменах ОТ и ИТ
- Мультивендорная консолидация логов с возможностью осведомленности, как операционной, так и безопасности

FORTINET РЕШЕНИЕ

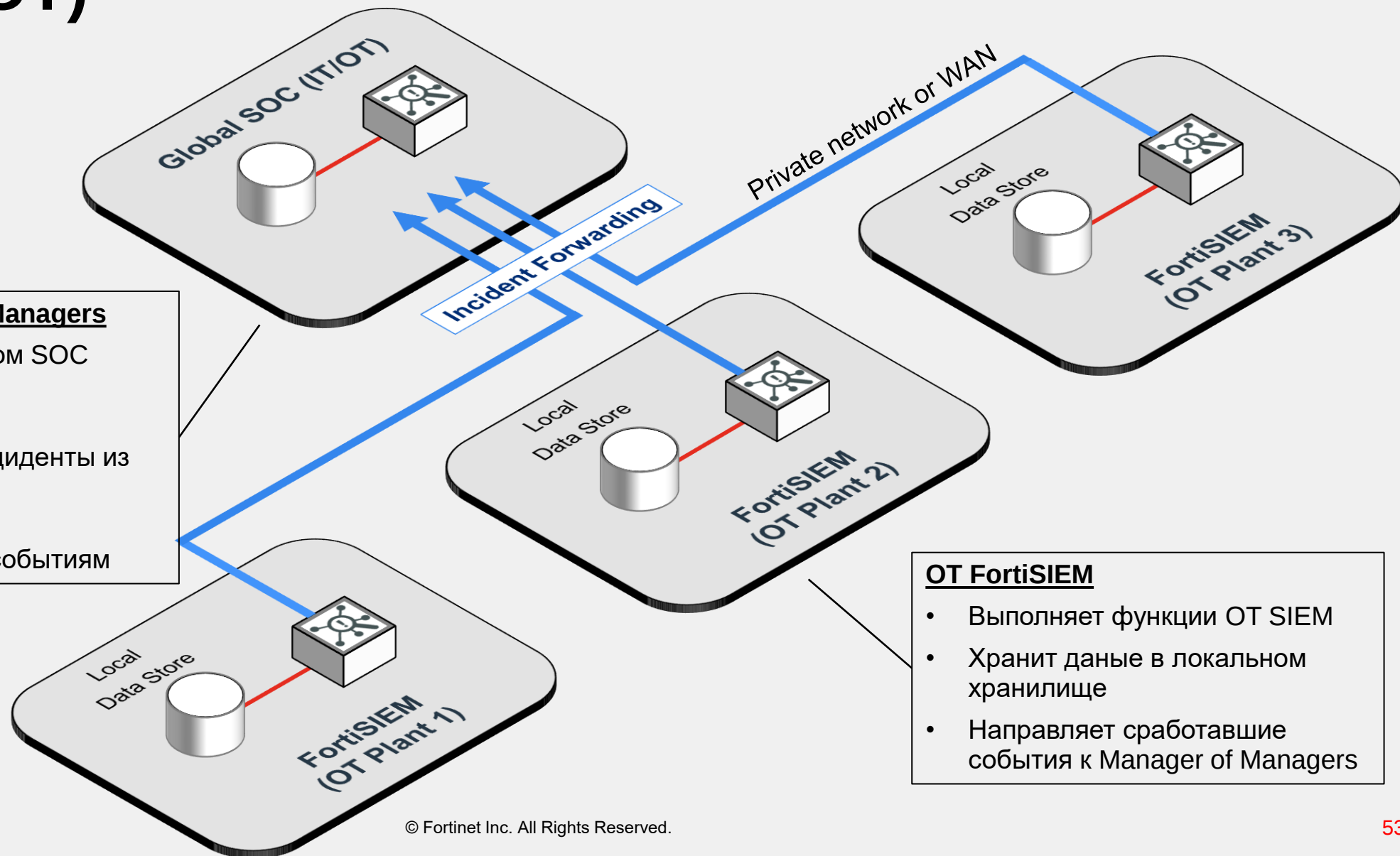
- Патнер с ведущими производителями контроля ОТ
- Fortinet FortiSIEM 1 Supervisor, 2 Collectors на каждый завод(1 для ИТ и 1 для ОТ)
- «Сырые» логи направлялись в Elastic Data Lake



FortiSIEM изолированная архитектура



Архитектура Менеджер над Менеджерами(Global SOC IT/OT)





FORTINET®