



**Check Point**<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD

# ТРЕНДЫ И ТЕХНОЛОГИИ ДЛЯ ЗАЩИТЫ АСУ ТП 2020

Березовский Антон | Check Point Russia  
Эксперт по информационной безопасности  
[antonb@checkpoint.com](mailto:antonb@checkpoint.com)

# Автоматизированные системы управления



Водоподготовка



Энергетика



Транспорт



Промышленность



Автоматизация



Нефть и газ



Управление зданиями

... используются нами **каждую секунду** для повседневных вещей и операций

## Встроенные уязвимости промышленного оборудования



Устаревшее ПО



Отсутствует встроенная защита



Отсутствуют исправления  
невозможно исправить



Слабые пароли по умолчанию

## Вектор атаки



Целевой фишинг



Индивидуальные АРТ  
атаки



Традиционное вредоносное ПО



Шифровальщики  
Вымогатели

# Факты и реальность



Check Point  
SOFTWARE TECHNOLOGIES LTD.

Март 2019

Атака шифровальщиком LockerGoga на Norsk Hydro

# Атака на завод Norsk Hydro

Целевая фишинговая  
рассылка

Распространение  
вредоносного  
кода используя  
групповые  
политики AD

Шифрование как  
документов так и  
системных файлов

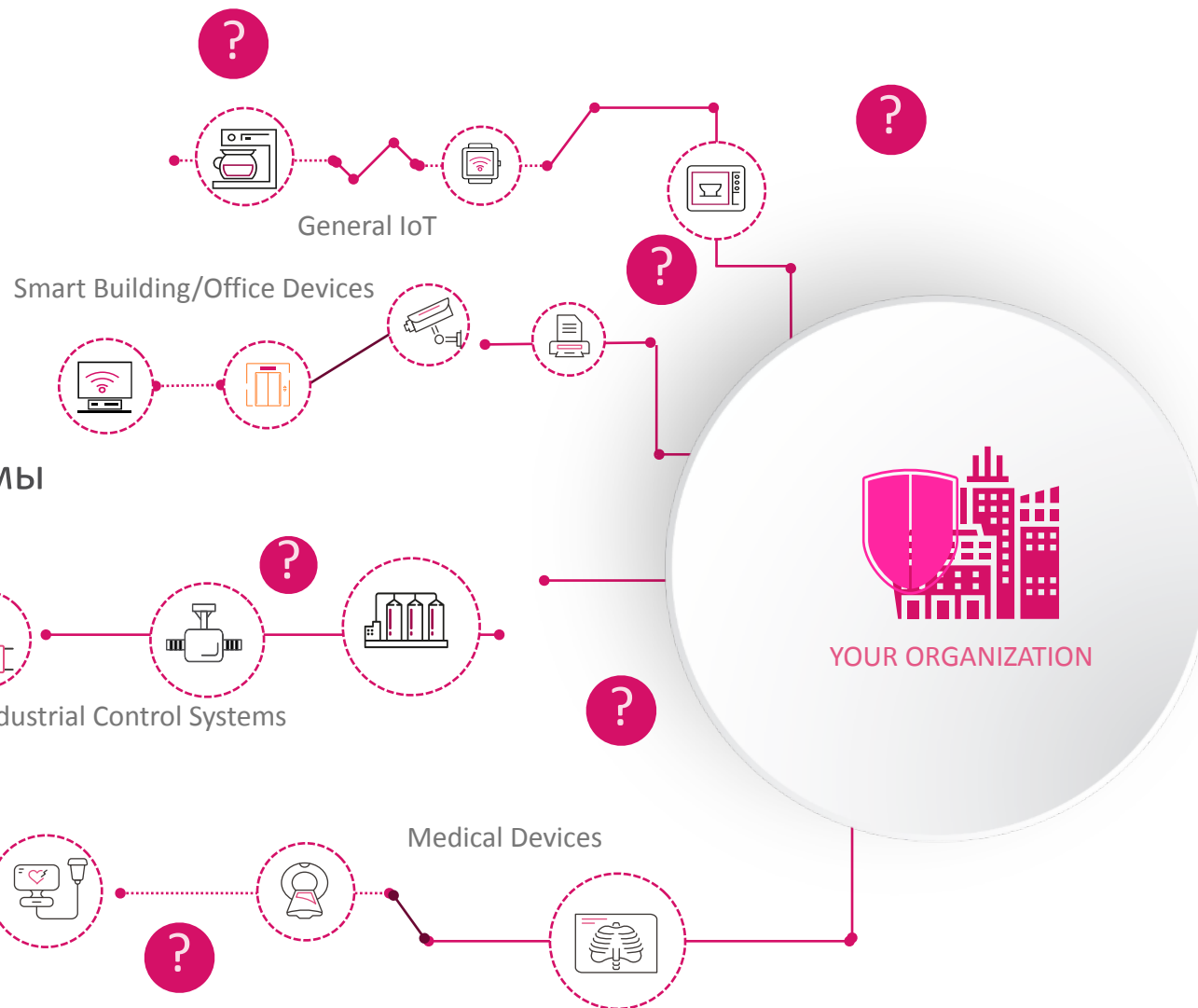
Частичная  
остановка бизнес  
процессов

LockerGoga

# Современное окружение в компании

Различные типы устройств и производителей

---



Различные протоколы и операционные системы

---

Кто управляет этими устройствами ?

---

# Эволюция угроз

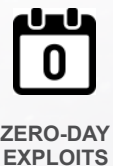
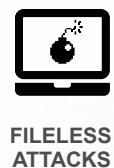
## Мотивированные и финансируемые



## Человеческий фактор

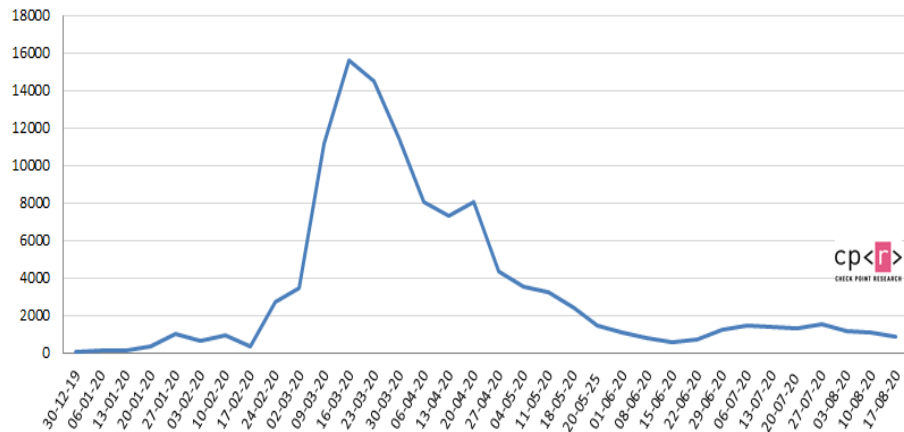


## Сложные и направленные атаки

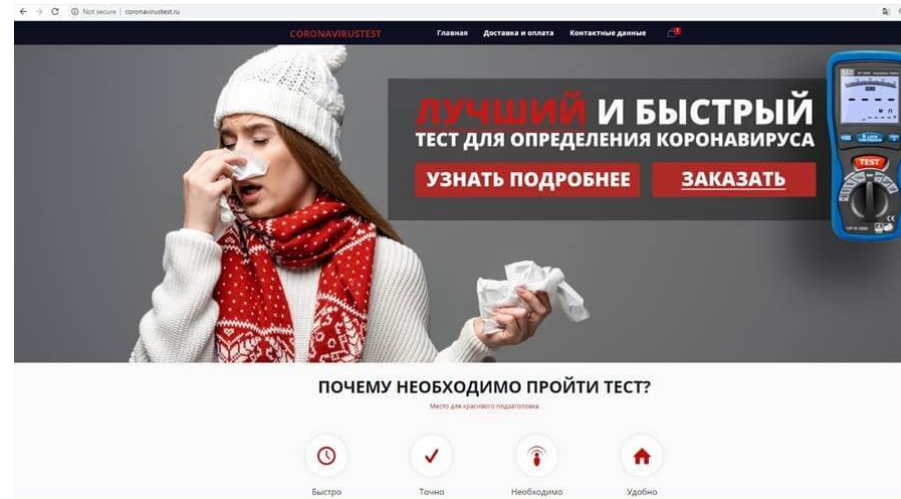
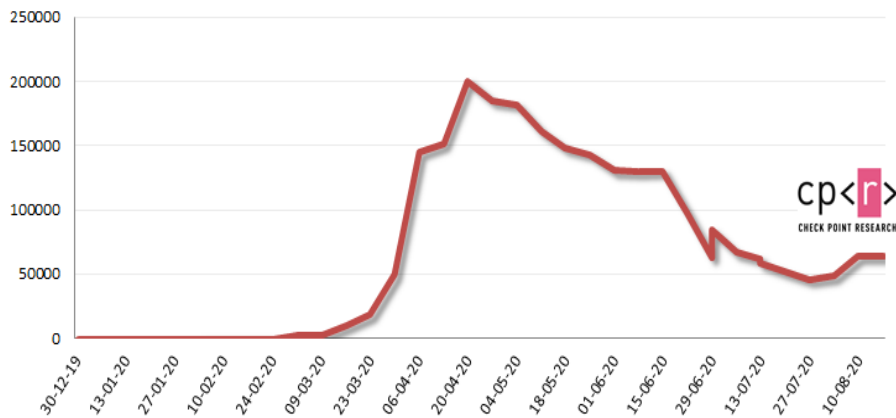


# Злоумышленники пользуются ситуацией

Coronavirus Domains Registered Weekly



Weekly Coronavirus Related Cyber Attacks



До 17% новых веб-сайтов, посвященных коронавирусу в период начала эпидемии, вредоносные/подозрительные

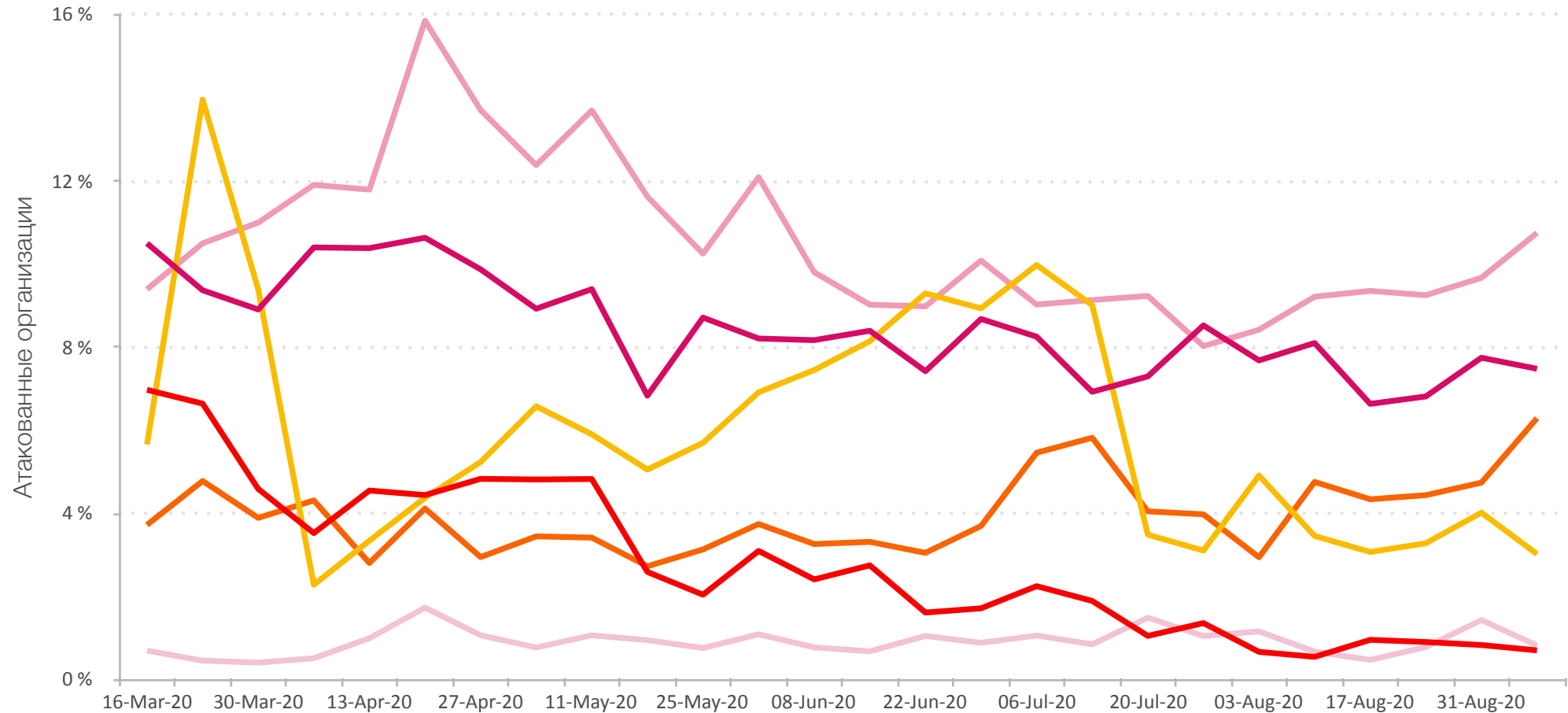
<https://blog.checkpoint.com/2020/04/02/coronavirus-update-in-the-cyber-world-the-graph-has-yet-to-flatten/>

<https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/>



# Тренды кибер-угроз в СНГ за последние 6 месяцев

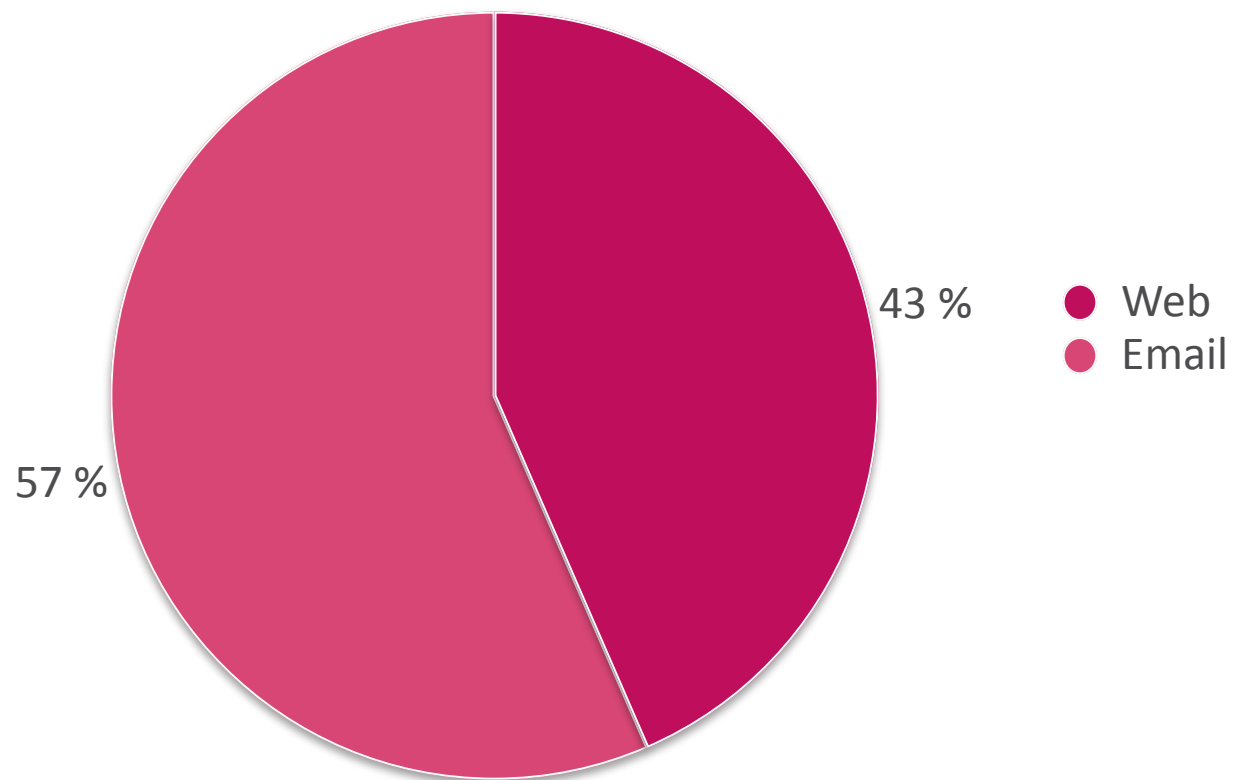
— Майнеры — Мобильные — InfoStealer — Банкеры — Ботнеты — Вымогатели



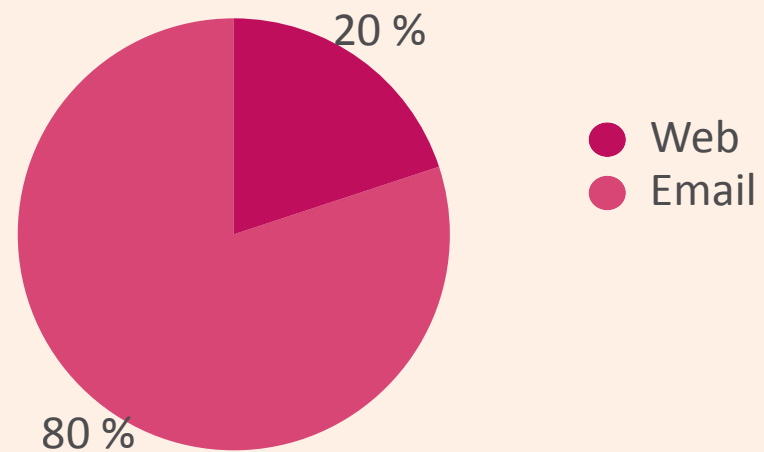
# Вектор атаки доставки вредоносных файлов

За последние 30 дней

## СНГ - Энергетическая отрасль



## All Industries





**Check Point**<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD

# КАКИМ ОБРАЗОМ МЫ МОЖЕМ ОСТАВАТЬСЯ НА ШАГ ВПЕРЕДИ УГРОЗ?

# Лучшие практики защиты КИИ

Обеспечить  
безопасность ИТ- и  
ОТ-окружений

Защитить корпоративную сеть  
предприятия от угроз

Обеспечить четкое разделение  
между ИТ- и ОТ-инфраструктурами

Внедрить специализированные  
системы защиты для КИИ

**CHECK POINT'S**

**РЕШЕНИЯ ПО ЗАЩИТЕ**

**критических информационных инфраструктур**

**CYBER DEFENSE**

**Контроль  
SCADA-трафика**

**Анализ  
событий  
безопасности**

**Специализиро-  
ванная защита  
от угроз**

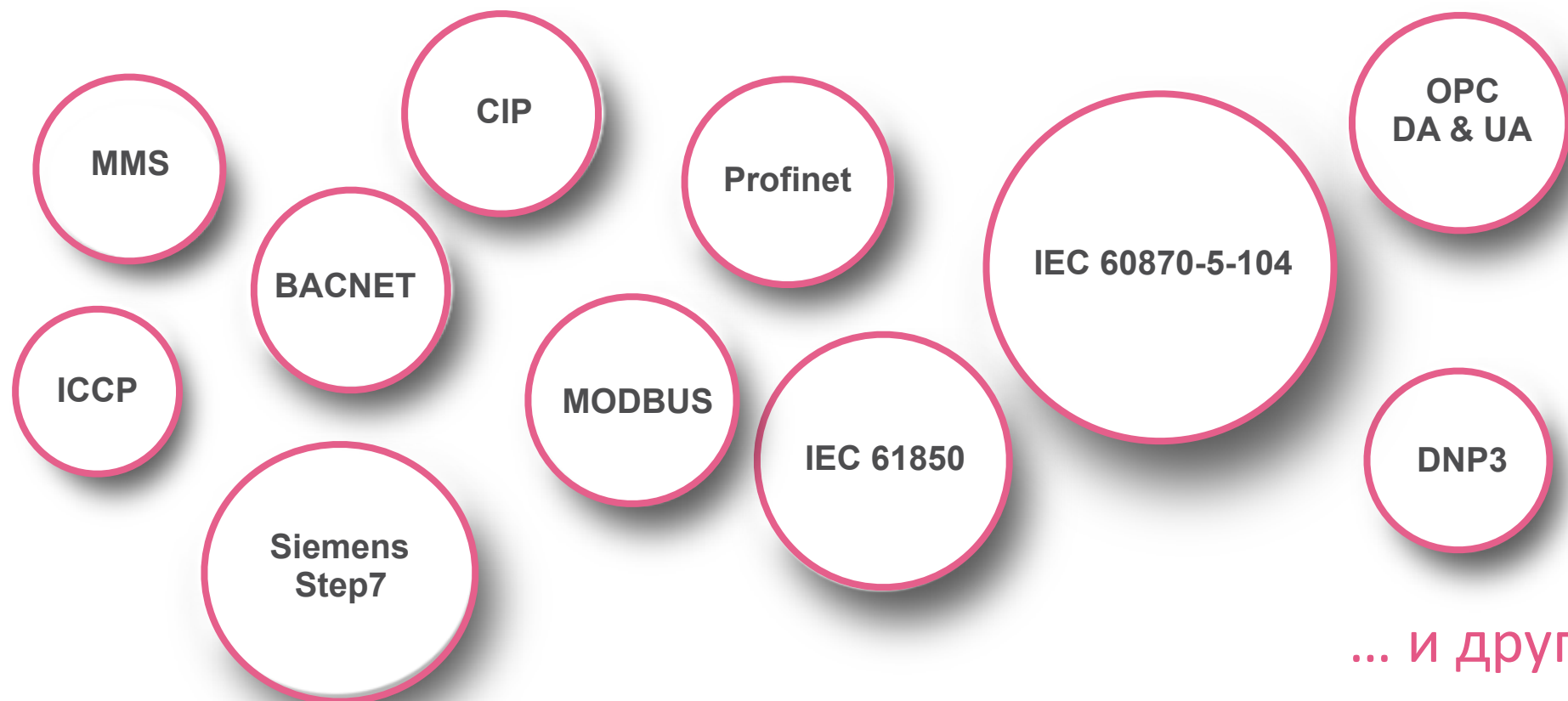
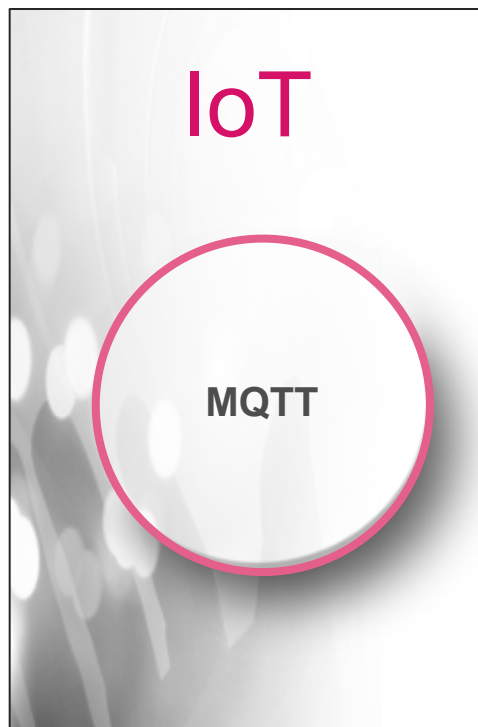
**Надежные  
устройства для  
агрессивной среды**

**SCADA**

# Контроль SCADA-трафика



# Поддержка специализированных протоколов



... и другие

Более **1500 SCADA и IoT** команд  
в Check Point Application Control

Полный перечень: <https://appwiki.checkpoint.com>

## CHECK POINT

РЕШЕНИЯ ПО ЗАЩИТЕ  
критических информационных инфраструктур

## CYBER DEFENSE

Контроль  
SCADA-трафика

Анализ  
событий  
безопасности

Специализиро-  
ванная защита  
от угроз

Надежные  
устройства для  
агрессивной среды

SCADA

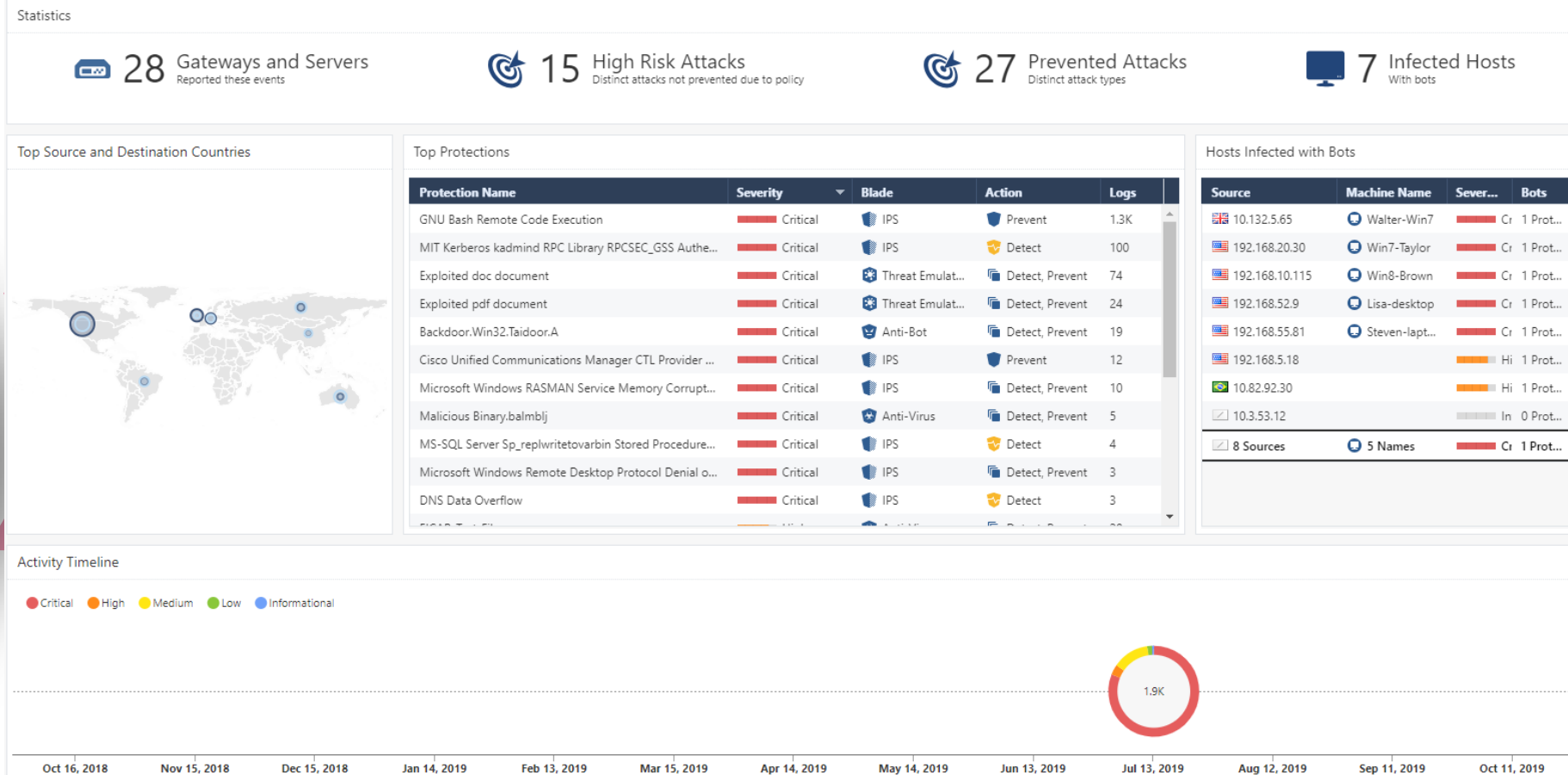


# Детальное журналирование трафика

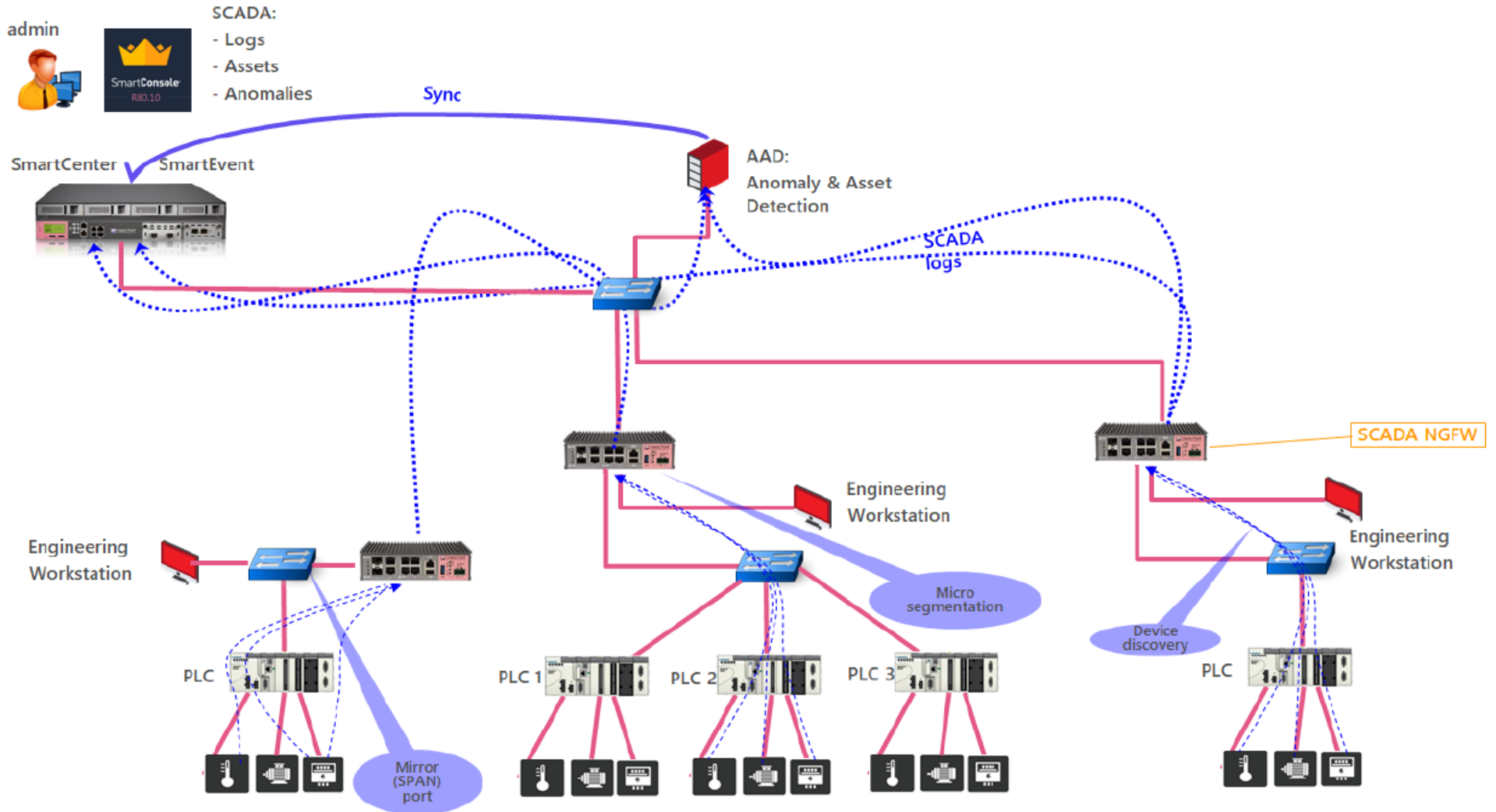
## СГРУППИРОВАНО

Детальная информация для расследования инцидентов

CHECK POINT  
SMARTLOG &  
SMARTEVENT



# Архитектура Check Point AAD



# Информация об устройстве

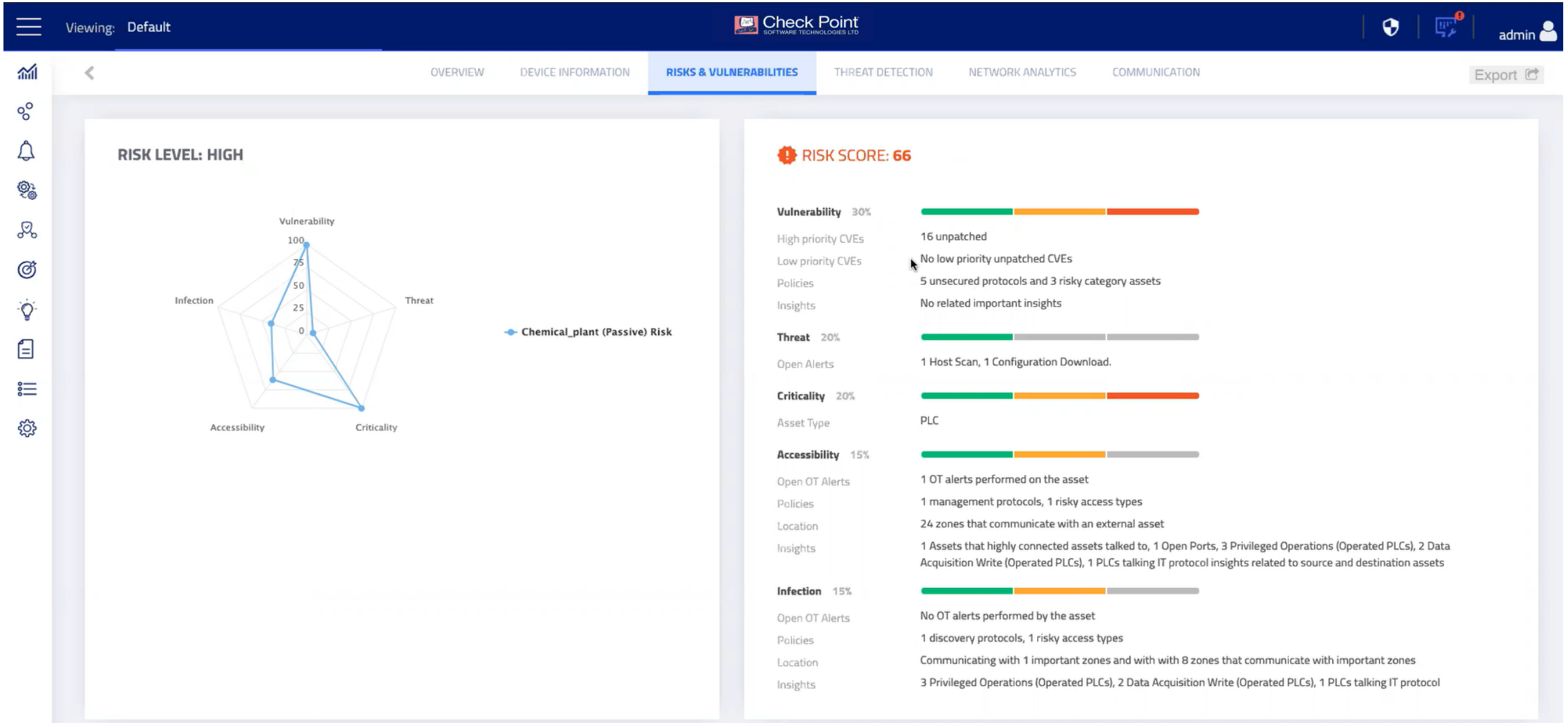
Детальная информация об устройстве – тип, производитель, версия прошивки и прочее

The screenshot displays the 'Assets View' interface in the Check Point management console. The top navigation bar includes the 'Viewing: Default' status, the Check Point logo, and a user profile for 'admin'. Below the navigation bar, there are filters for Class, Type, Vendor, Protocol, and Criticality, along with a search bar. The main area shows a table of 516 results, with the following columns: NAME, IP, MAC, CLASS, TYPE, CRITICALITY, RISK LEVEL, VENDOR, NETWORK, and LAST SEEN. The table lists various devices, including PLCs and OT devices from Rockwell Automation and Siemens.

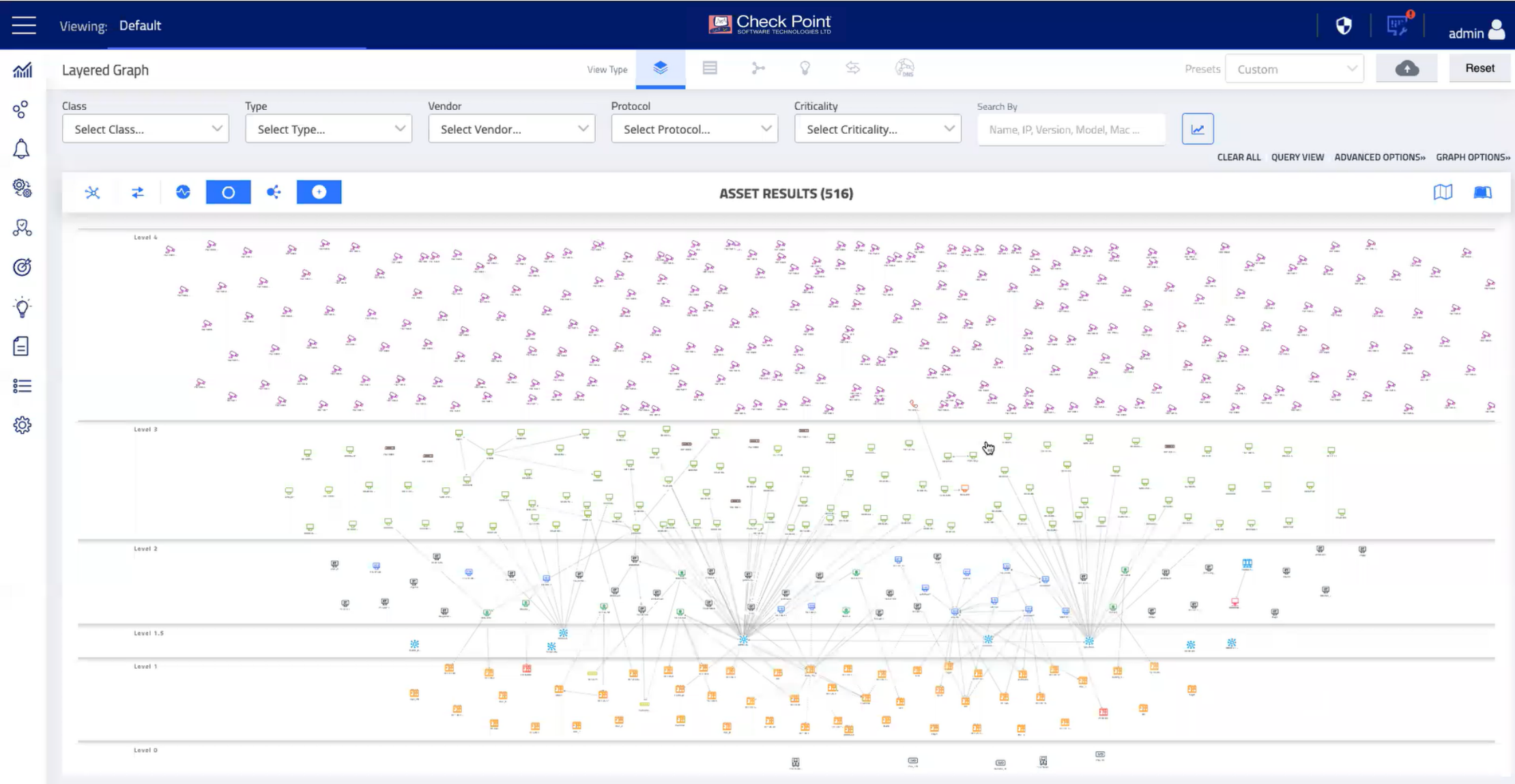
NAME	IP	MAC	CLASS	TYPE	CRITICALITY	RISK LEVEL	VENDOR	NETWORK	LAST SEEN
10.1.30.3	10.1.30.3	F4:54:33:92:89:96	OT	PLC	High	High	Rockwell Automation	Default	07/05/20, 14:25
10.1.30.6	10.1.30.6	00:1D:9C:A1:60:4E	OT	PLC	High	High	Rockwell Automation	Default	07/05/20, 14:25
10.1.30.5	10.1.30.5	00:00:BC:03:44:C0	OT	PLC	High	High	Rockwell Automation	Default	07/05/20, 14:25
Chemical_plant (Active)	10.1.30.1	00:1D:9C:C0:04:9D, 00:1D:9C:CF:3D:FD	OT	PLC	High	High	Rockwell Automation	active	07/05/20, 13:25
Chemical_plant (Passive)	10.1.0.40, 10.1.30.1	00:1D:9C:C0:04:9D	OT	PLC	High	High	Rockwell Automation	Default	07/05/20, 15:37
10.1.0.10	10.1.0.10, 10.1.30.4	E4:90:69:A7:70:0F	OT	PLC	High	High	Rockwell Automation	Default	07/05/20, 14:25
Data_Transfer	10.1.0.41, 10.1.30.2, 10.1.30.30	00:00:BC:C7:8F:06, 00:1D:9C:BD:A9:4F, 00:1D:9C:C3:88:9E	OT	PLC	High	High	Rockwell Automation	Default	07/05/20, 15:37
Oil-Gas	10.1.31.5	00:0E:8C:84:9C:5C	OT	PLC	High	Medium	Siemens	Default	07/05/20, 12:55
Suger	10.1.31.3	28:63:36:38:FE:9D	OT	PLC	High	Medium	Siemens	Default	07/05/20, 14:55
RO	10.1.31.1	28:63:36:26:F0:74	OT	PLC	High	Medium	Siemens	Default	07/05/20, 15:55
10.1.31.16	10.1.31.16	08:00:06:93:8C:DA	OT	PLC	High	Medium	Siemens	Default	07/05/20, 12:55

# Информация об устройстве

Детальная информация об устройстве – тип, производитель, версия прошивки и прочее



# Информация об устройстве – иерархическая карта



# Оповещения на базе поведенческого анализа

The screenshot displays the Check Point Insights View interface. At the top, there is a navigation bar with the Check Point logo and user information (admin). Below this, the 'Insights View' section is active, showing a list of 21 insights. The interface includes filters for Class, Type, Vendor, Protocol, and Criticality, along with a search bar. The insights are listed as follows:

- 6 assets were communicating with 5 external IPs
- 17 assets are using 4 unsecured protocols: FTP, SCHNEIDER-NETMANAGE, SMB, SNMP
- 1 asset has 149 unpatched vulnerabilities - Windows Full Match
- 52 assets have 79 unpatched vulnerabilities - Full Match
- Top 7 Risky Assets
- 5 OT-assets performed privileged OT operations on 3 PLCs/Controllers/RTUs/IEDs
- 9 assets are using default passwords
- 4 assets using IT protocols: EPM, PHYSICAL, RDP , with 10 PLCs/Controllers/RTUs/IEDs
- 7 assets have 26 unpatched vulnerabilities - Vendor and Model Match
- 1 asset managed 1 asset remotely using protocol: RDP
- 12 assets have multiple network interfaces
- 11 OT-assets performed data-acquisition write operations on 8 PLCs/Controllers/RTUs/IEDs
- 4 USB devices were connected to 1 asset

# Автоматическое добавление устройств и создание политики

The screenshot displays the Check Point SmartConsole interface. On the left, a navigation pane shows the hierarchy: GATEWAYS & SERVERS, SECURITY POLICIES, LOGS & MONITOR, and MANAGE & SETTINGS. Under SECURITY POLICIES, the 'Access Control' section is expanded to show 'Policy', 'NAT', 'Threat Prevention', and 'HTTPS Inspection'. The 'Shared Policies' section includes 'Geo Policy', 'Gateways', and 'Exceptions'. The 'Access Tools' section includes 'VPN Communities', 'Updates', 'UserCheck', 'Client Certificates', 'Application Wiki', and 'Installation History'. The main workspace shows a table with columns 'No.', 'Name', 'Source', 'Destination', and 'VPN'. A row is highlighted with '1', 'Cleanup', 'New IoT Discovery Service', and '\* Any'. A modal dialog box is open over this row, titled 'CTD' with the subtitle 'Enter Object Comment'. The dialog has a yellow warning banner that says 'Changes will be applied after publish.' Below this, there are input fields for 'Hostname' (192.168.101.3), 'Port' (9000), and 'Pre-shared Key' (masked with three dots). A 'Test Connection' button shows a green 'Connected' status. At the bottom of the dialog are 'OK' and 'Cancel' buttons. The background interface shows a search bar at the top right, an 'Object Categories' list on the right, and a status bar at the bottom with 'No tasks in progress', the IP address '192.168.101.2', and 'No changes | admin'.

No.	Name	Source	Destination	VPN
1	Cleanup	New IoT Discovery Service		* Any

**Object Categories**

- Network Objects: 19
- Services: 547
- Applications/Categories: 7508
- VPN Communities: 2
- Data Types: 62
- Users: 1
- Servers: 1
- Time Objects: 3
- UserCheck Interactions: 13
- Limit: 4

# Автоматическое добавление устройств и создание политики

The screenshot displays the Check Point management console interface. The main window shows a policy configuration table with the following data:

No.	Name	Source	Destination	VPN
1	Cleanup rule	* Any	* Any	* Any

Below the table, a 'Recent Tasks' window is open, showing the progress of an IoT layer update:

- Updating IoT Layer** (10% Arranging rules structure) - 08:38
- Updating IoT Layer** (Finished Updating IoT Layer) - 4/6/2020 07:47
- Policy installation - Standard** (Installation succeeded on check-point-gateway)

On the right side, the 'Object Categories' list includes:

- Network Objects: 19
- Services: 547
- Applications/Categories: 7508
- VPN Communities: 2
- Data Types: 62
- Users: 1
- Servers: 1
- IoT Controllers: 1
- Time Objects: 3
- UserCheck Interactions: 13
- Limit: 4
- IoT Assets: 4**

The bottom status bar shows the IP address 192.168.101.2, the user 'admin', and the system state 'Published'.



# Автоматическое добавление устройств и создание политики

The screenshot displays the Check Point SmartConsole interface. On the left, a navigation sidebar includes sections for Gateways & Servers, Security Policies, Logs & Monitor, and Manage & Settings. The main window shows a table of security policy rules under the 'Standard' tab. Rule 6.1 is selected, and a search for 'mod' is performed, resulting in a list of Modbus-related protocols. The details for 'Common Industrial Protocol - RMW (Read/Modify/Write)' are shown on the right, including its primary category as 'SCADA Protocols' and a match-by configuration for 'tcp/44818'.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
3.2	Cleanup	* Any	* Any	* Any	* Any	Accept	Accounting, Detailed Log, Accounting
4		Function=SCADA Client: Cl...	* Any	* Any	* Any	from SCADA Client: C	N/A
5		Function=Engineering Stati...	* Any	* Any	* Any	from Engineering Sta	N/A
6		Function=HMI: Rockwell - ...	* Any	* Any	* Any	from HMI: Rockwell -	N/A
6.1		* Any	Function=OT: Rockwell - P	* Any	tcp-44818	Accept	Detailed Log

Search results for 'mod':

- Common Industrial Protocol - RMW (Read/Modify/Wri
- udp-dhcp-rep-localmodule
- udp-dhcp-req-localmodule
- ftp-pasv
- ftp-port
- LDAP-modify
- Modbus
- Modbus Protocol
- Modbus Protocol - CANOpen General Reference
- Modbus Protocol - diagnostic
- Modbus Protocol - encapsulated interface transport
- Modbus Protocol - get com event counter
- Modbus Protocol - get com event log

Details for Common Industrial Protocol - RMW (Read/Modify/Wri):

Primary Category: **SCADA Protocols**

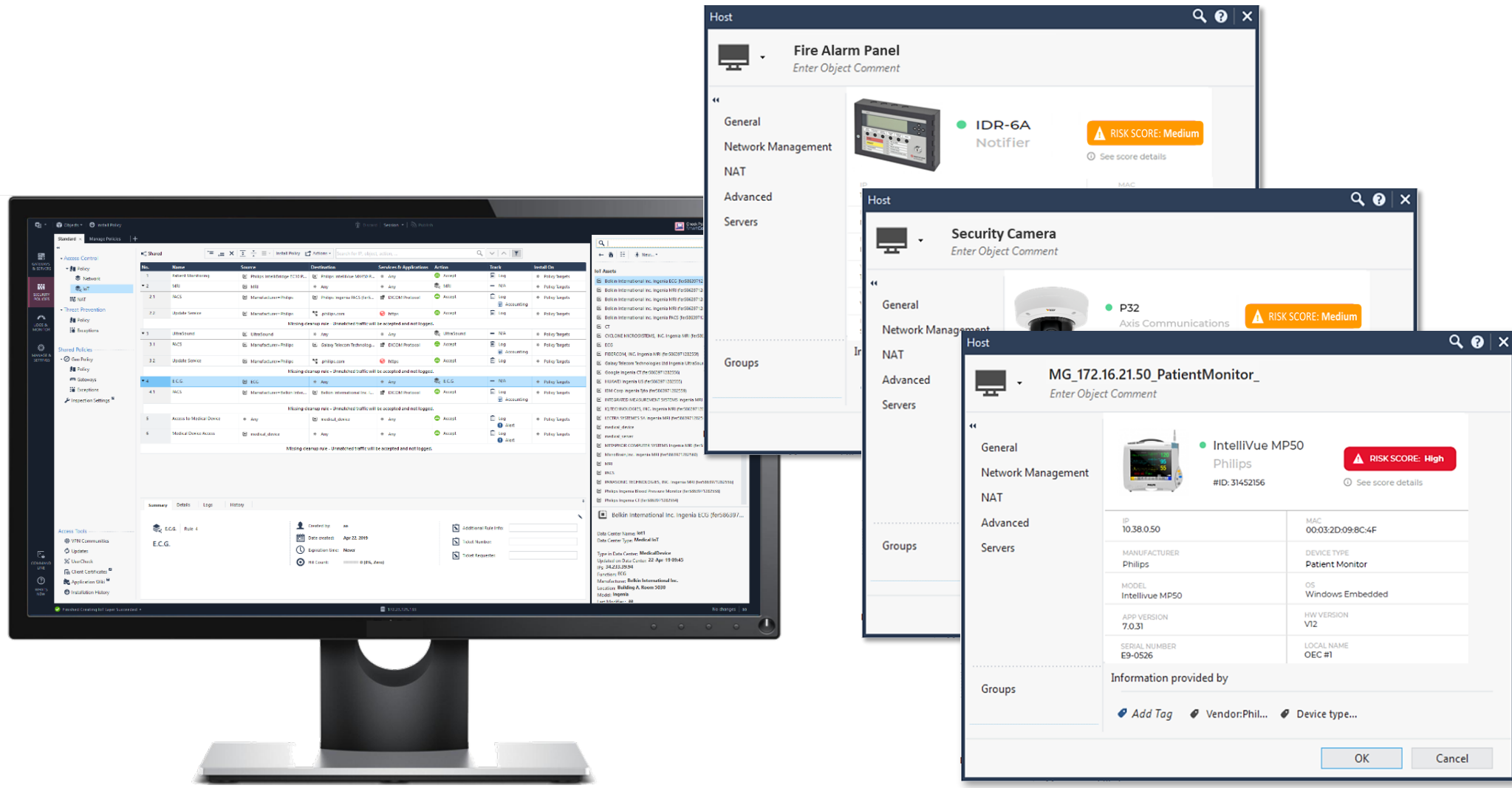
The Common Industrial Protocol (CIP) is a protocol for industrial applications. It is supported by ODVA. This protocol supports the Read/Modify/Write (RMW) command.

Match By:

- Application Signature
- Services:
  - tcp/44818

More Info

# Автоматическое добавление устройств и создание политики



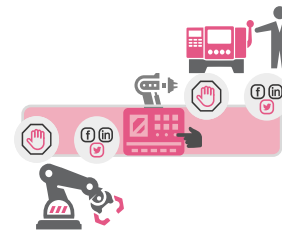
The image displays the Check Point management console interface. The main window shows a table of policies with columns for Name, Source, Destination, Services/Ports/Applications, Action, and Threat ID. Below the table, there are sections for Summary, Details, and Log. Overlaid on the console are three pop-up windows for device discovery:

- Fire Alarm Panel:** IDR-6A Notifier, RISK SCORE: Medium.
- Security Camera:** P32 Axis Communications, RISK SCORE: Medium.
- MG\_172.16.21.50\_PatientMonitor\_:** IntelliVue MP50 Philips, #ID: 31452156, RISK SCORE: High.

The third pop-up window provides detailed information for the Philips IntelliVue MP50 Patient Monitor:

IP	10.38.0.50	MAC	00:03:2D:09:8C:4F
MANUFACTURER	Philips	DEVICE TYPE	Patient Monitor
MODEL	IntelliVue MP50	OS	Windows Embedded
APP VERSION	7.0.31	HW VERSION	V12
SERIAL NUMBER	E9-0526	LOCAL NAME	OEC #1

Information provided by: Add Tag, Vendor:Phil..., Device type...



## CHECK POINT

РЕШЕНИЯ ПО ЗАЩИТЕ  
критических информационных инфраструктур

## CYBER DEFENSE

Контроль  
SCADA-трафика

Анализ  
событий  
безопасности

Специализиро-  
ванная защита  
от угроз

Надежные  
устройства для  
агрессивной среды

SCADA

# Компоненты КИИ редко обновляются



Siemens Global Website

### ProductCERT Security Advisories

Siemens ProductCERT is the central team for responding to security incidents and vulnerabilities related to Siemens solutions and services. In the following, Siemens security bulletins issued by ProductCERT are listed.

**2016**

- > SSA-751155 (Last Update 2016-04-08): Denial-of-Service Vulnerability
- > SSA-623229 (Last Update 2016-04-08): DROWN Vulnerability in Indu
- > SSA-301706 (Last Update 2016-04-08): GNU C Library Vulnerability i
- > SSA-151221 (Last Update 2016-03-18): Incorrect File Permissions in
- > SSA-833048 (Last Update 2016-03-14): Vulnerability in SIMATIC S7-1
- > SSA-253230 (Last Update 2016-02-08): Vulnerabilities in SIMATIC S7
- > SSA-743465 (Last Update 2016-01-15): Cross-Site Scripting Vulnerab

OZW772

**2015**

- > SSA-472334 (Last Update 2015-12-18): NTP Vulnerabilities in RUGG
- > SSA-763427 (Last Update 2016-04-29): Vulnerability in Communicatio
- > SSA-921524 (Last Update 2016-04-29): Incorrect Frame Padding in F
- > SSA-720081 (Last Update 2015-09-01): IP Forwarding in RUGGEDC
- > SSA-134003 (Last Update 2015-08-27): Web Vulnerability in S7-1200

Life Is On Schneider Electric

all the site

Solutions Products a

## Support

You are here: Home > Support > Cybersecurity > Vuln

### Security

World presence	Date (dd/mm/yyyy)
Customer Care Centre	14/03/2016
Contact	12/03/2016
Cybersecurity	29/02/2016
News	17/02/2016
Report an incident	04/02/2016
Substitution tool	25/01/2016
Counterfeiting	20/01/2016
Definitions	11/01/2016
Report a counterfeit	10/12/2015
Idea Submission	25/11/2015

HOME • ABOUT • TECHNOLOGY • CYBER SECURITY • ALERTS AND NOTIFICATIONS

GLOBAL SITE - ENGLISH

Power and productivity for a better world™ ABB

## Cyber security alerts and notifications

We are committed to providing our customers with products, systems and services that clearly address cyber security. Proper and timely handling of cyber security incidents and software vulnerabilities is one important factor in helping our customers minimize risks associated with cyber security.

Latest alerts and notifications

Archived alerts and notifications

Subscribe to email alerts

Report a vulnerability

2015-12-10: POODLE Vulnerability in RTU500 Series  
 2015-12-10: POODLE Vulnerability in Relion 650 series Ver. 1.3.0  
 2015-12-10: POODLE Vulnerability in MicroSCADA Pro SYS600  
 2015-12-10: POODLE Vulnerability in SDM600 Ver. 1.1  
 2015-12-10: POODLE Vulnerability in AFx series  
 2015-12-10: POODLE Vulnerability in ETL600 series  
 2015-12-10: POODLE Vulnerability in ESP630 series  
 2015-12-10: POODLE Vulnerability in FOX660 series  
 2015-12-10: POODLE Vulnerability in Relion 615 series v5.0  
 2015-12-10: POODLE Vulnerability in COM600  
 2015-12-10: POODLE Vulnerability in Protection and Control IED Manager PCM600

2015-02-11: Security Bulletin for ABB 3rd Party Device Type Library HART DTM  
 2014-10-30: Advisory for ABB RobotStudio  
 2014-10-30: Advisory for ABB Test Signal Viewer  
 2014-04-24: (updated 2014-06-30): OpenSSL Heartbleed Vulnerability in Relion 650 series Ver. 1.3.0  
 2014-02-19: CMT 1000 Vulnerability bug fix  
 2013-11-08: Remote code execution vulnerability in CAP 501 / CAP 505 / SMS 510  
 2013-11-08: Remote code execution vulnerabilities in MicroSCADA  
 2013-10-17: Advisory for Test Signal Viewer on Windows for Robotics  
 2012-04-30: Advisory for AC500 web server  
 2012-03-23: Advisory for WebWare Components and Related Products  
 2012-02-28: Buffer Overflow in Robot Communications Runtime on Windows

Date	Product	Vulnerability	Action	Reference
20/01/2016	Altivar Drives	Modification of Drive Parameters	See disclosure	ST03406
11/01/2016	MiCOM C264	Integer Overflow	See disclosure	SEVD-2016-011-01
10/12/2015	M340 PLC	Buffer Overflow	See disclosure	SEVD-2015-344-01
25/11/2015	ProClima SW	Remote Code Execution	ProClima, all versions prior to V6.2	SEVD-2015-329-01

# Виртуальный патчинг Более 350 специализированных IDS/IPS сигнатур

Защита от уязвимостей  
и обнаружение  
аномального трафика



Protection	Severity
Citect SCADA ODBC Overflow Attempt	Medium
Rockwell RSLogix Denial of Service Vulnerability	Critical
SCADA Engine OPC Client Buffer Overflow Vulnerability	High
Schneider Electric UnitelWay Windows Device Driver Buffer Overflow	Critical
<b>Siemens Tecnomatix FactoryLink Stack Overflow Vulnerability</b>	<b>Critical</b>
Siemens Automation License Manager Multiple Vulnerabilities	Critical
ScadaTEC SCADAPhone and ModbusTagServer Buffer Overflow	High
RealWin HMI Service Buffer Overflow 2	High
Automated Solutions Modbus/TCP Master OPC server Modbus TCP Header	High
RealWin INFOTAG/SET_CONTROL Packet Processing Buffer Overflow	High
Unauthorized Miscellaneous Request to a PLC	Critical
Broadcast Request from an Authorized Client	Critical
IGSS SCADARMS Report Template WriteFile Command Buffer Overflow	Critical
IGSS SCADA STDREP Request Buffer Overflow	High
Iconics Genesis SCADA Freeing of Uninitialized Memory Trigger	High
<b>Rockwell RNA Message Negative Header Length</b>	<b>Critical</b>
Intellicom NetBiter Config HICP Hostname Buffer Overflow	Medium
WonderWare SuiteLink DOS Attempt	High



NSS Labs  
Highest Rating

## CHECK POINT

# РЕШЕНИЯ ПО ЗАЩИТЕ критических информационных инфраструктур

## CYBER DEFENSE

Контроль  
SCADA-трафика

Анализ  
событий  
безопасности

Специализиро-  
ванная защита  
от угроз

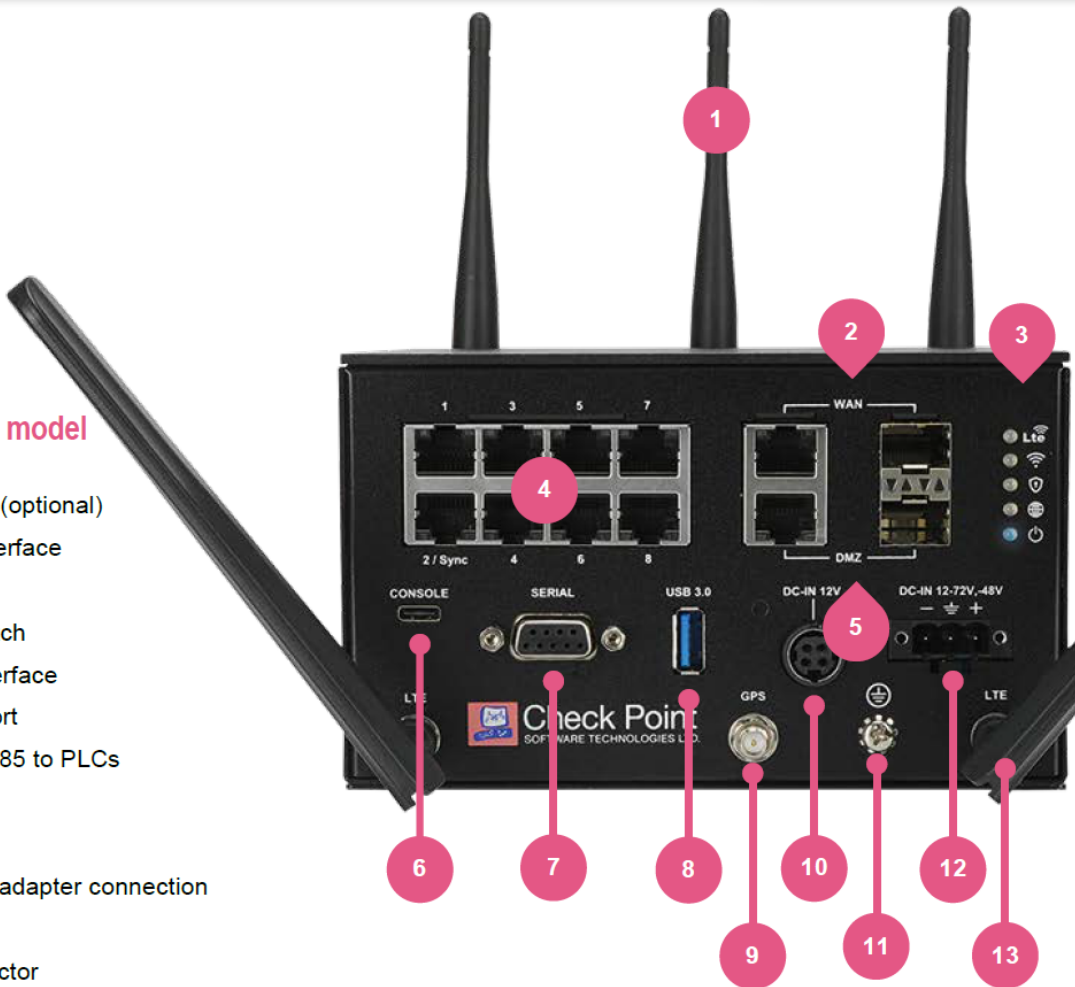
Надежные  
устройства для  
агрессивной среды

SCADA

# Check Point 1570R

## 1570R Wi-Fi, LTE model

- 1. 802.11 n/ac Wi-Fi (optional)
- 2. 1x 1GbE WAN interface
- 3. LED tower
- 4. 8x 1GbE LAN switch
- 5. 1x 1GbE DMZ interface
- 6. USB-C console port
- 7. DB9 RS232/422/485 to PLCs
- 8. USB 3.0 port
- 9. GPS connector
- 10. AC to DC power adapter connection
- 11. Ground screw
- 12. DC power connector
- 13. Embedded LTE modem (optional)

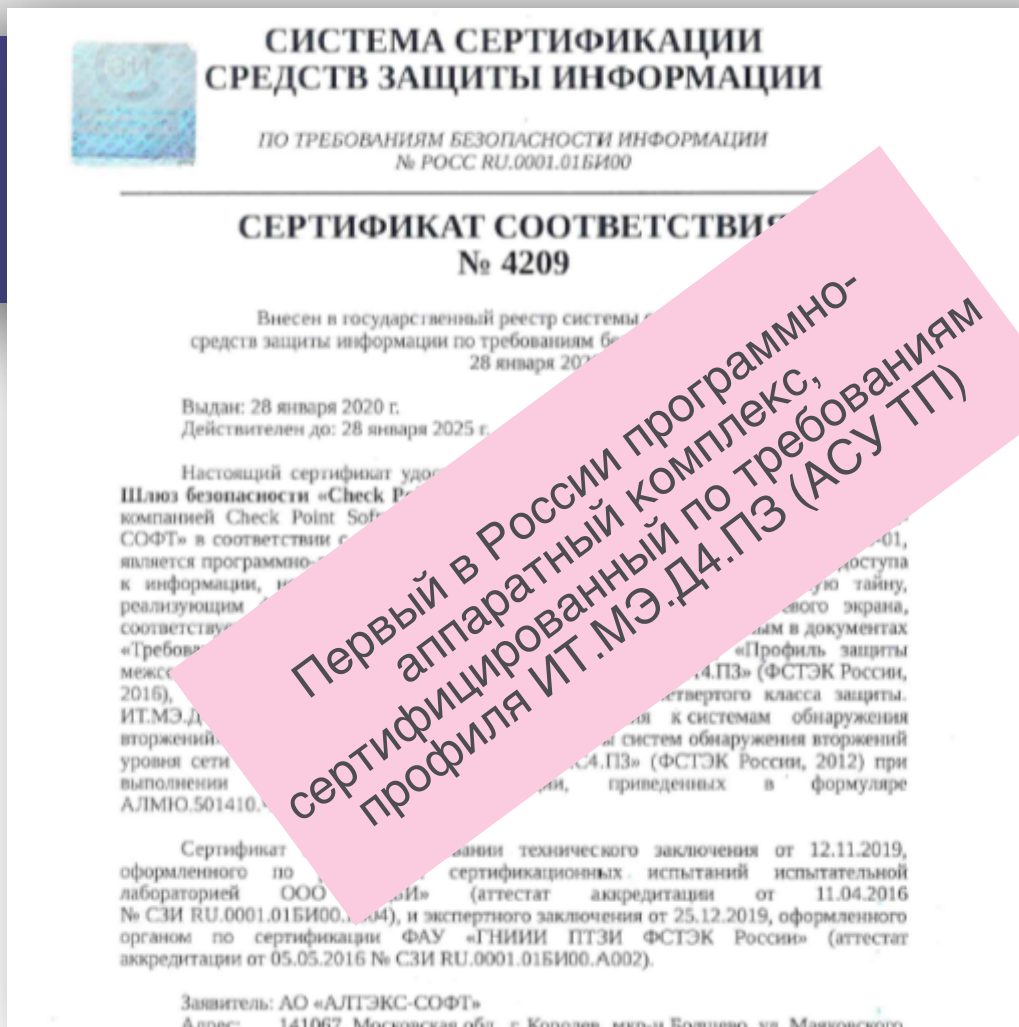


8x1GbE ports

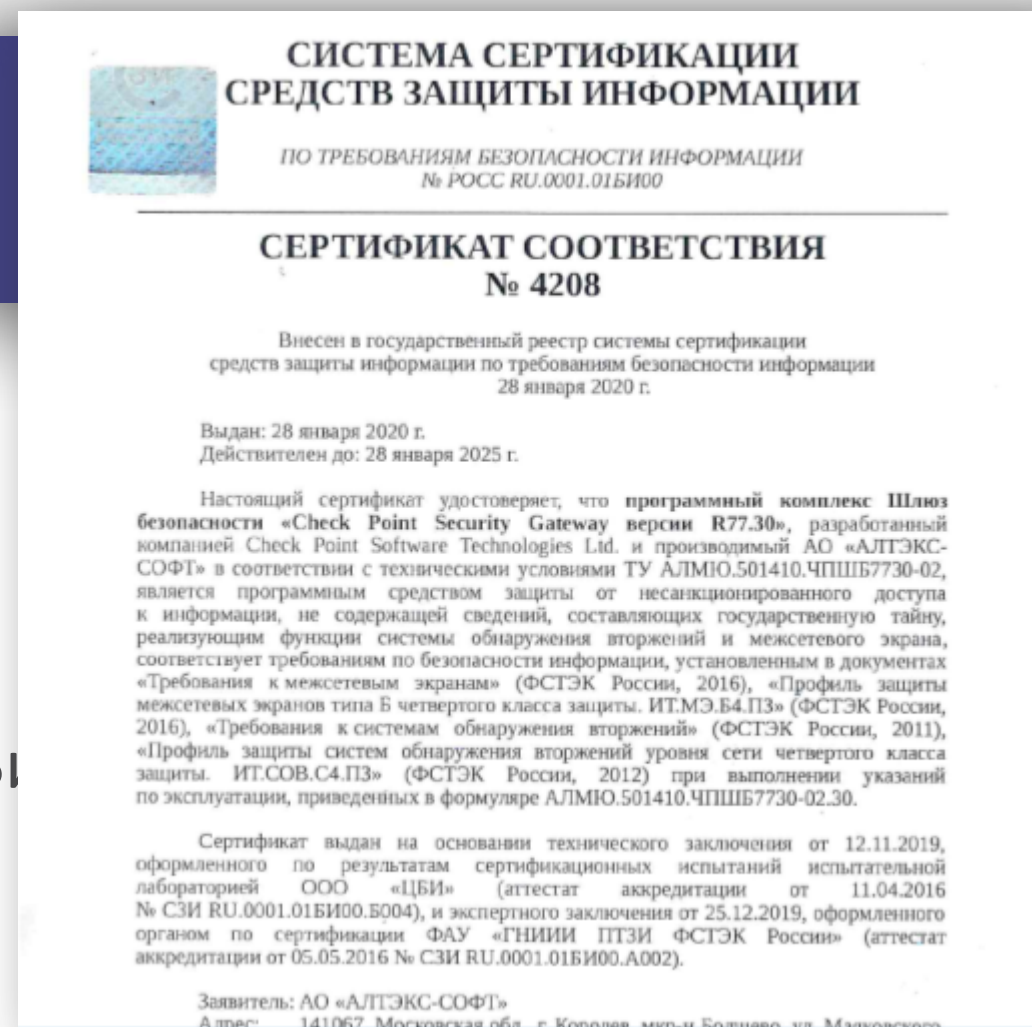
Dual band 802.11ac 3X3 MIMO

400 Mbps Threat Prevention

# Государственный реестр сертифицированных средств защиты информации



Первый в России программно-аппаратный комплекс, сертифицированный по требованиям профиля ИТ.МЭ.Д4.ПЗ (АСУ ТП)



В



# Государственный реестр сертифицированных средств защиты информации

4208		28.01.2020	28.01.2025	программный комплекс безопасности «Check Point Security Gateway версии R77.30» Шлюз	Соответствует требованиям документам: Требования к МЭ, Профиль защиты МЭ(Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ), Требования к СОВ, Профили защиты СОВ(сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ)	серия	ООО «ЦБИ»	ФАУ ПТЗИ России»	«ГНИИИ ФСТЭК	АО «АЛТЭК-СОФТ»	141067, Московская обл., г. Королев, мкр-н Болшево, ул. Маяковского, д. 10А, пом. VII, (495) 543-3101	31.12.2023
4209	28.01.2020	28.01.2025	программно-аппаратный комплекс безопасности «Check Point Security Gateway версии R77.30» Шлюз	Соответствует требованиям документам: Требования к МЭ, Профиль защиты МЭ(А четвертого класса защиты. ИТ.МЭ.А4.ПЗ), Профиль защиты МЭ(Д четвертого класса защиты. ИТ.МЭ.Д4.ПЗ), Требования к СОВ, Профили защиты СОВ(сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ)	серия	ООО «ЦБИ»	ФАУ ПТЗИ России»	«ГНИИИ ФСТЭК	АО «АЛТЭК-СОФТ»	141067, Московская обл., г. Королев, мкр-н Болшево, ул. Маяковского, д. 10А, пом. VII, (495) 543-3101	31.12.2023	

# Срок действия сертификата

Срок действия

Потребитель, не являющийся заявителем

Срок действия сертификата заявителя

Может ли сертификат

- за
- пр
- ин
- се
- Ре



Общество с ограниченной ответственностью «ЧЕК ПОЙНТ СОФТ

Исх. №: 20.01.20-0  
Дата: 20 января

Настоящим письмом компания Check Point поддерживает прогн

1. Поддержка ПК версии R77.30 ФСТЭК на шлю
2. Поддержка П выходят только функционала.
3. Начиная с января будут привлечены стабилизиров

С уважением,  
Василий Широков  
Заместитель генерального директора  
ООО «Чек Пойнт Софт

## Product Support of R77.30 for Russia

[Rate This](#)

[My Favorites](#)

Solution ID	sk163301
Product	Security Gateway
Version	R77.30
OS	Gaia
Access Level	Internal
Date Created	28-Oct-2019
Last Modified	28-Oct-2019 by Vasily Shirokov
Status	Approved by TAC
SR #	WXB-194-52966
CR # / Jira #	
Originator	Vasily Shirokov
Editor	Vasily Shirokov
Technical Resource	Ricky Nissanov
Last Approver	rzeld@checkpoint.com

### Symptoms

- Russian FSTEC certification requirements

### Solution

Support Extension for R77.30 for Russia until December 2023 at the follow

явителя).

к по обращению

срока действия  
ОВИЙ:

ИЯМ по защите

Ю находятся в

# Решения ФСТЭК России о проведении сертификации Security Gateways R80.xx

## Федеральная служба по техническому и экспортному контролю

### РЕШЕНИЕ о проведении сертификации средства защиты информации

№ 6423 от 8 июня 2020 г.

Наименование средства защиты информации:	программно-аппаратный комплекс «Шлюз безопасности «Check Point Security Gateway версии R80.XX»
Назначение средства защиты информации:	для защиты информации, не содержащей сведения, составляющие государственную тайну, в ГИС 1 класса защищенности, в АСУ ТП 1 класса защищенности, на значимых объектах КИИ 1 категории, для обеспечения безопасности персональных данных 1 уровня защищенности
Заявитель:	Акционерное общество «АЛТЭК-СОФТ» (АО «АЛТЭК-СОФТ»)
Адрес местонахождения заявителя:	141067, Московская обл., г. Королев, мкр-н Болшево, ул. Маяковского, д. 10А, пом. VII
Испытательная лаборатория:	ООО «ЦБИ», 141090, Московская область, г. Королев, мкрн. Юбилейный, ул. Ленинская, дом 4, подвальное помещение 10
Орган по сертификации:	ФАУ «ГНИИИ ПТЗИ ФСТЭК России», 394030, г. Воронеж, ул. Студенческая, дом 36
Документы, на соответствие которым проводится сертификация:	Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (ФСТЭК России, 2018) - по 4 уровню доверия, Требования к межсетевым экранам (ФСТЭК России, 2016), Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ (ФСТЭК России, 2016), Профиль защиты межсетевых экранов типа Д четвертого класса защиты. ИТ.МЭ.Д4.ПЗ (ФСТЭК России, 2016), Требования к системам обнаружения вторжений (ФСТЭК России, 2011), Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ (ФСТЭК России, 2013)

## Федеральная служба по техническому и экспортному контролю

### РЕШЕНИЕ о проведении сертификации средства защиты информации

№ 6422 от 8 июня 2020 г.

Наименование средства защиты информации:	программный комплекс «Шлюз безопасности «Check Point Security Gateway версии R80.XX»
Назначение средства защиты информации:	для защиты информации, не содержащей сведения, составляющие государственную тайну, в ГИС 1 класса защищенности, в АСУ ТП 1 класса защищенности, на значимых объектах КИИ 1 категории, для обеспечения безопасности персональных данных 1 уровня защищенности
Заявитель:	Акционерное общество «АЛТЭК-СОФТ» (АО «АЛТЭК-СОФТ»)
Адрес местонахождения заявителя:	141067, Московская обл., г. Королев, мкр-н Болшево, ул. Маяковского, д. 10А, пом. VII
Испытательная лаборатория:	ООО «ЦБИ», 141090, Московская область, г. Королев, мкрн. Юбилейный, ул. Ленинская, дом 4, подвальное помещение 10
Орган по сертификации:	ФАУ «ГНИИИ ПТЗИ ФСТЭК России», 394030, г. Воронеж, ул. Студенческая, дом 36
Документы, на соответствие которым проводится сертификация:	Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (ФСТЭК России, 2018) - по 4 уровню доверия, Требования к межсетевым экранам (ФСТЭК России, 2016), Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ (ФСТЭК России, 2016), Требования к системам обнаружения вторжений (ФСТЭК России, 2011), Профиль защиты систем обнаружения



**Check Point**<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD

**СПАСИБО!**