Check Point
SOFTWARE TECHNOLOGIES LTD

ТРЕНДЫ И ТЕХНОЛОГИИ ДЛЯ ЗАЩИТЫ АСУ ТП 2020

Березовский Антон | Check Point Russia
Эксперт по информационной безопасности
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 пороли по умолчанию

Вектор атаки

Целевой фишинг

Индивидуальные APT атаки

Традиционное вредоносное ПО

Шифровальщики

Вымогатели

Факты и реальность

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

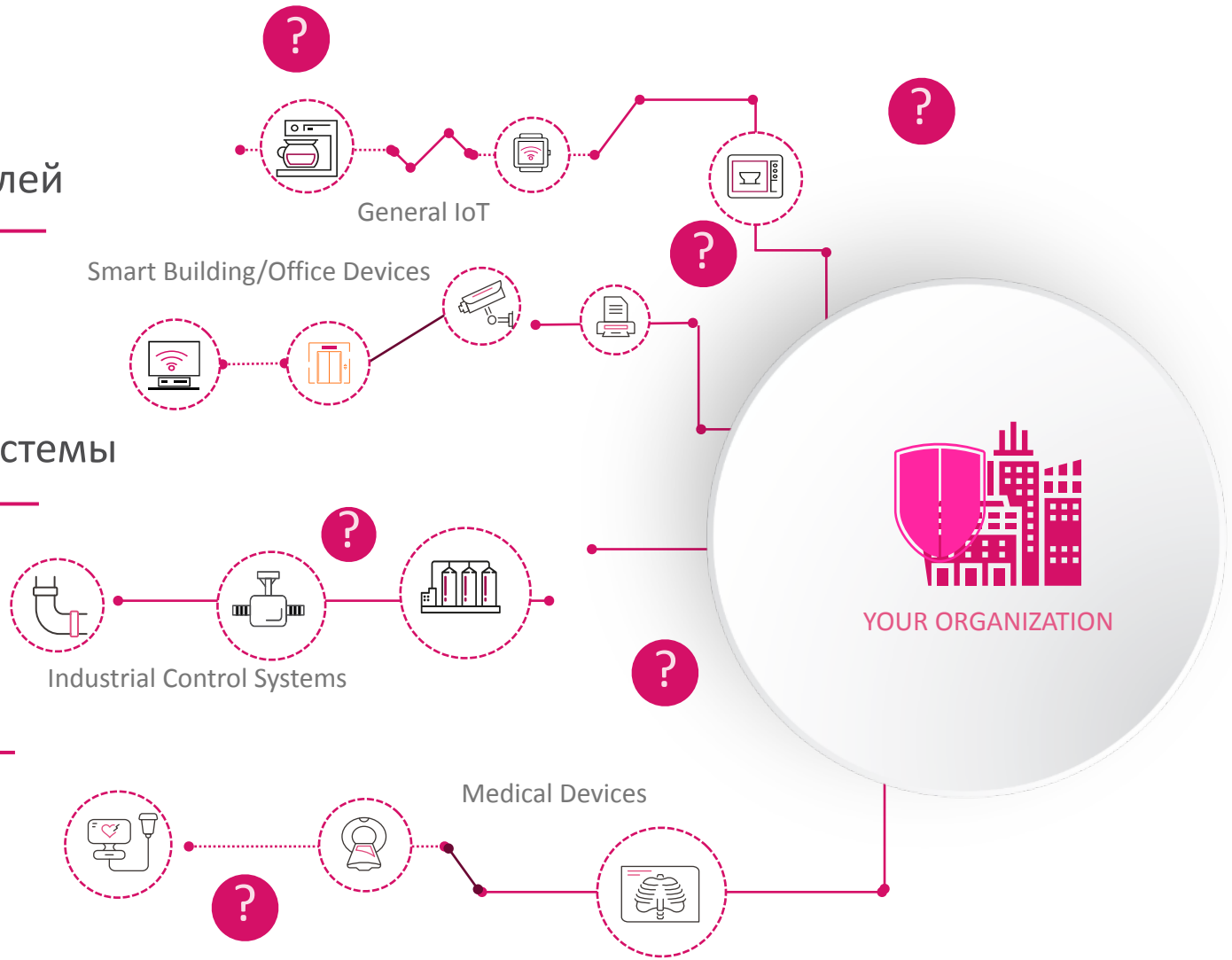
Частичная остановка бизнес процессов

Современное окружение в компании

Различные типа устройств и производителей

Различные протоколы и операционные системы

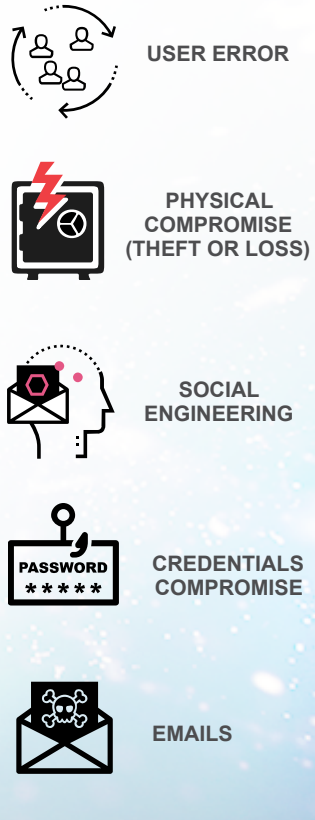
Кто управляет этими устройствами ?



Эволюция угроз

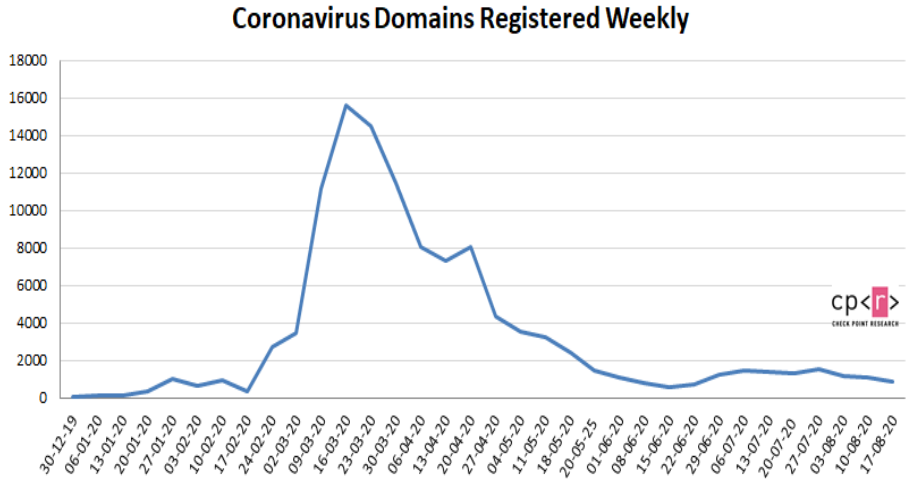
Мотивированные и финансируемые

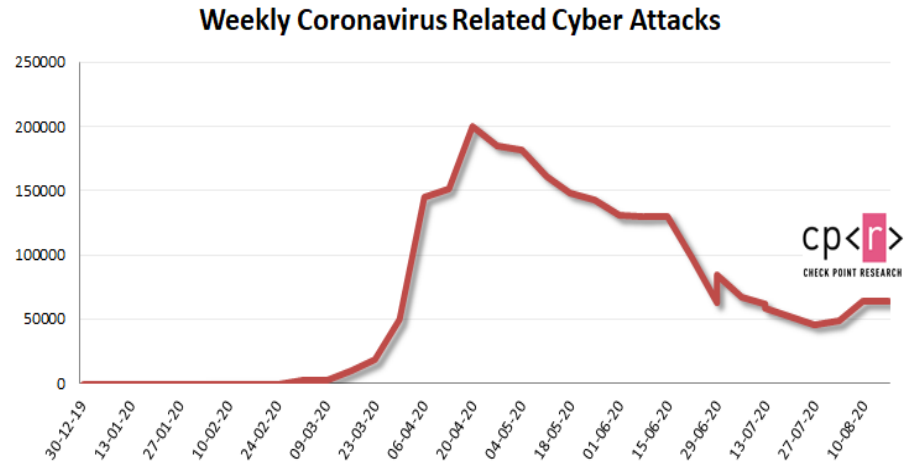
Человеческий фактор

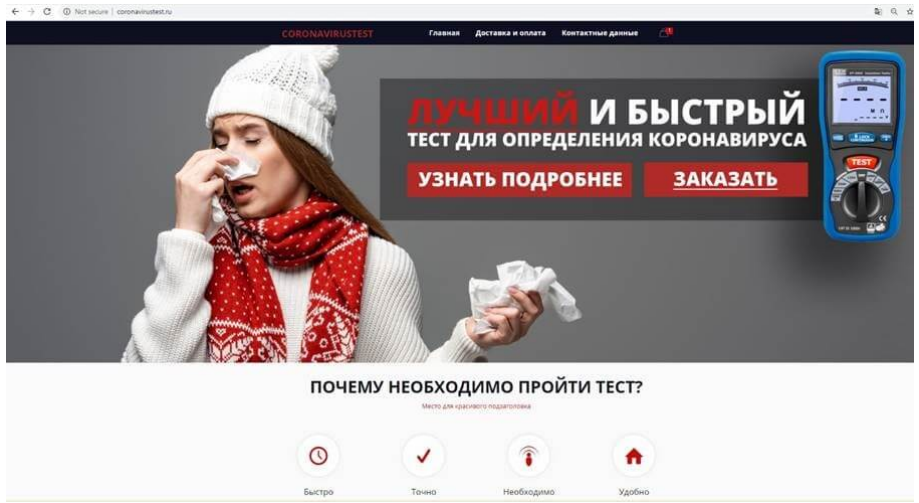


Сложные и направленные атаки

Злоумышленники пользуются ситуацией



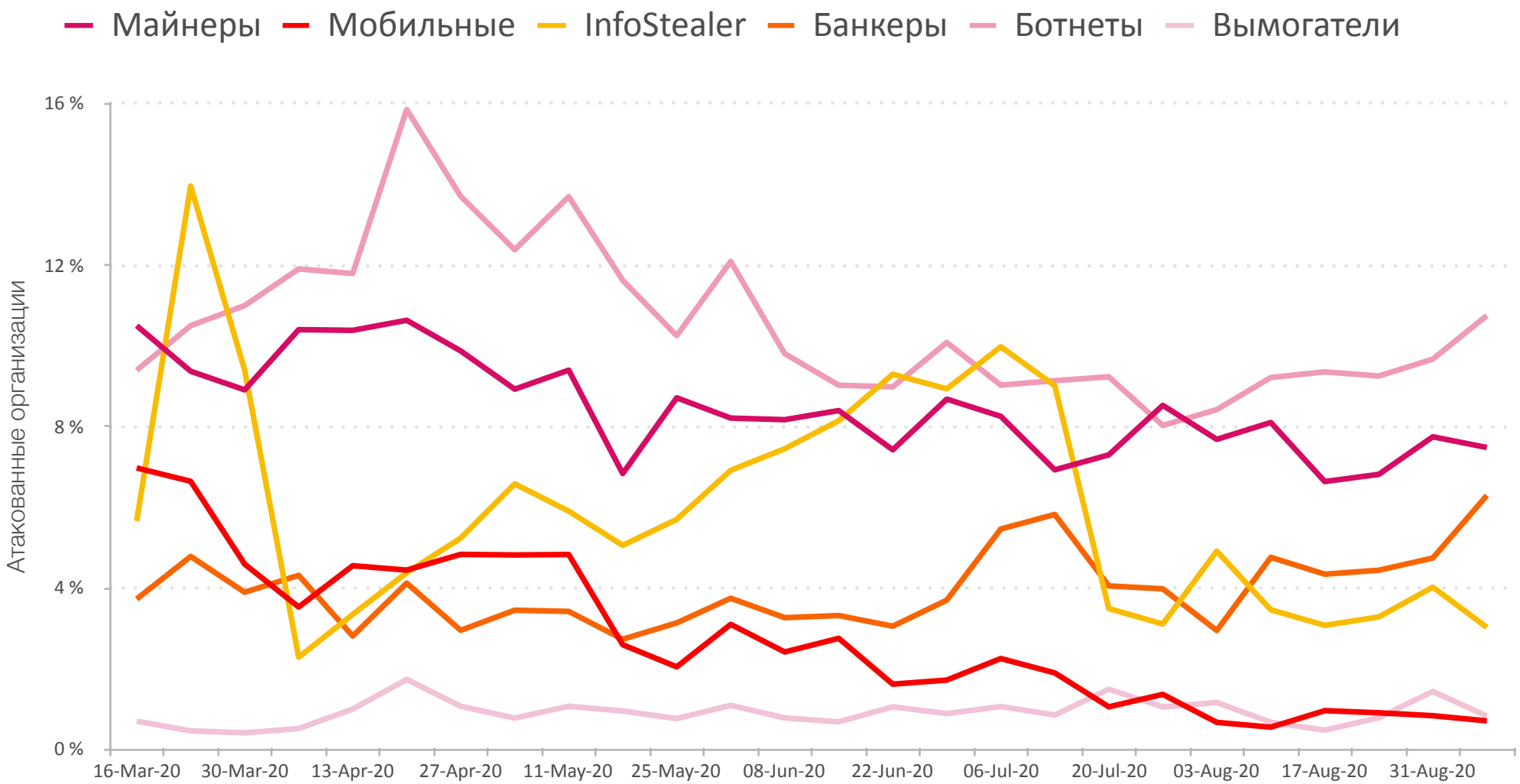




До 17% новых веб-сайтов, посвященных коронавирусу в период начала эпидеми, **вредоносные/подозрительные**

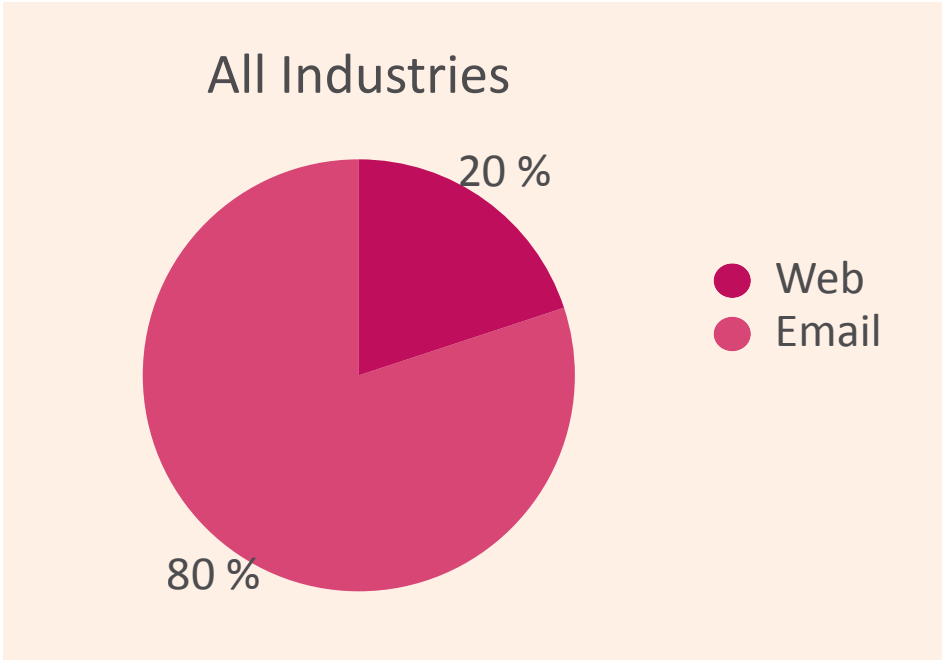
https://blog.checkpoint.com/2020/04/02/coronavirus-update-in-the-cyber-world-the-graph-has-yet-to-flatten/
https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/

Тренды кибер-угроз в СНГ за последние 6 месяцев



Вектор атаки доставки вредоносных файлов

За последние 30 дней



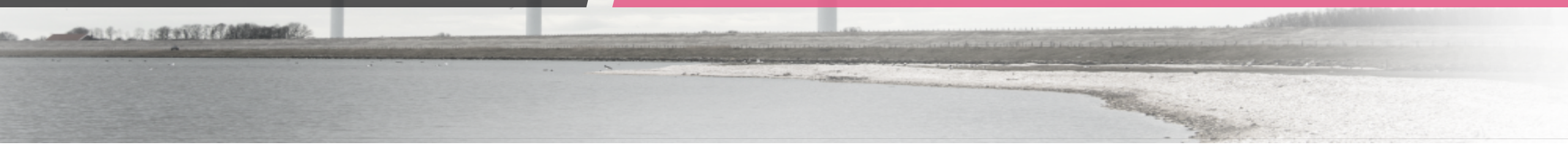
Check Point
SOFTWARE TECHNOLOGIES LTD

КАКИМ ОБРАЗОМ МЫ МОЖЕМ ОСТАВАТЬСЯ **НА ШАГ ВПЕРЕДИ** УГРОЗ?

Лучшие практики защиты КИИ

Обеспечить **безопасность IT- и OT-окружений**

- Защитить корпоративную сеть предприятия от угроз
- Обеспечить четкое разделение между IT- и OT-инфраструктурами
- Внедрить специализированные системы защиты для КИИ



CHECK POINT'S

РЕШЕНИЯ ПО ЗАЩИТЕ
критических информационных инфраструктур

CYBER DEFENSE

Контроль SCADA-трафика

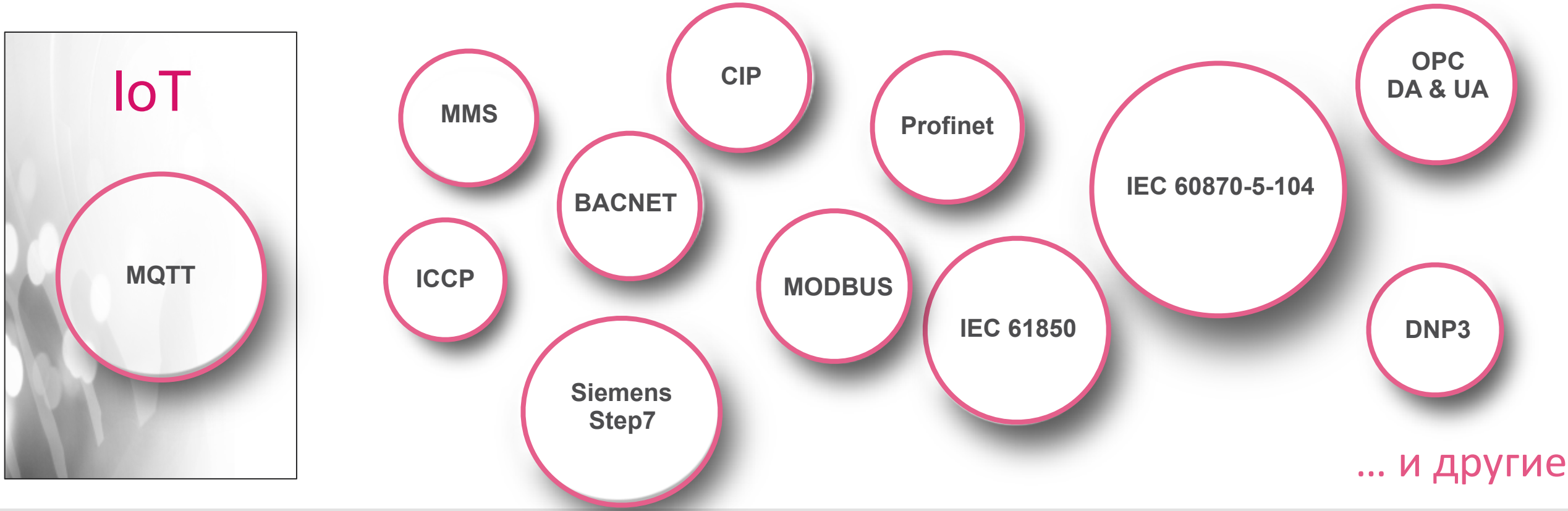
Анализ событий безопасности

Специализированная защита от угроз

Надежные устройства для агрессивной среды

Контроль SCADA-трафика

Поддержка специализированных протоколов



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

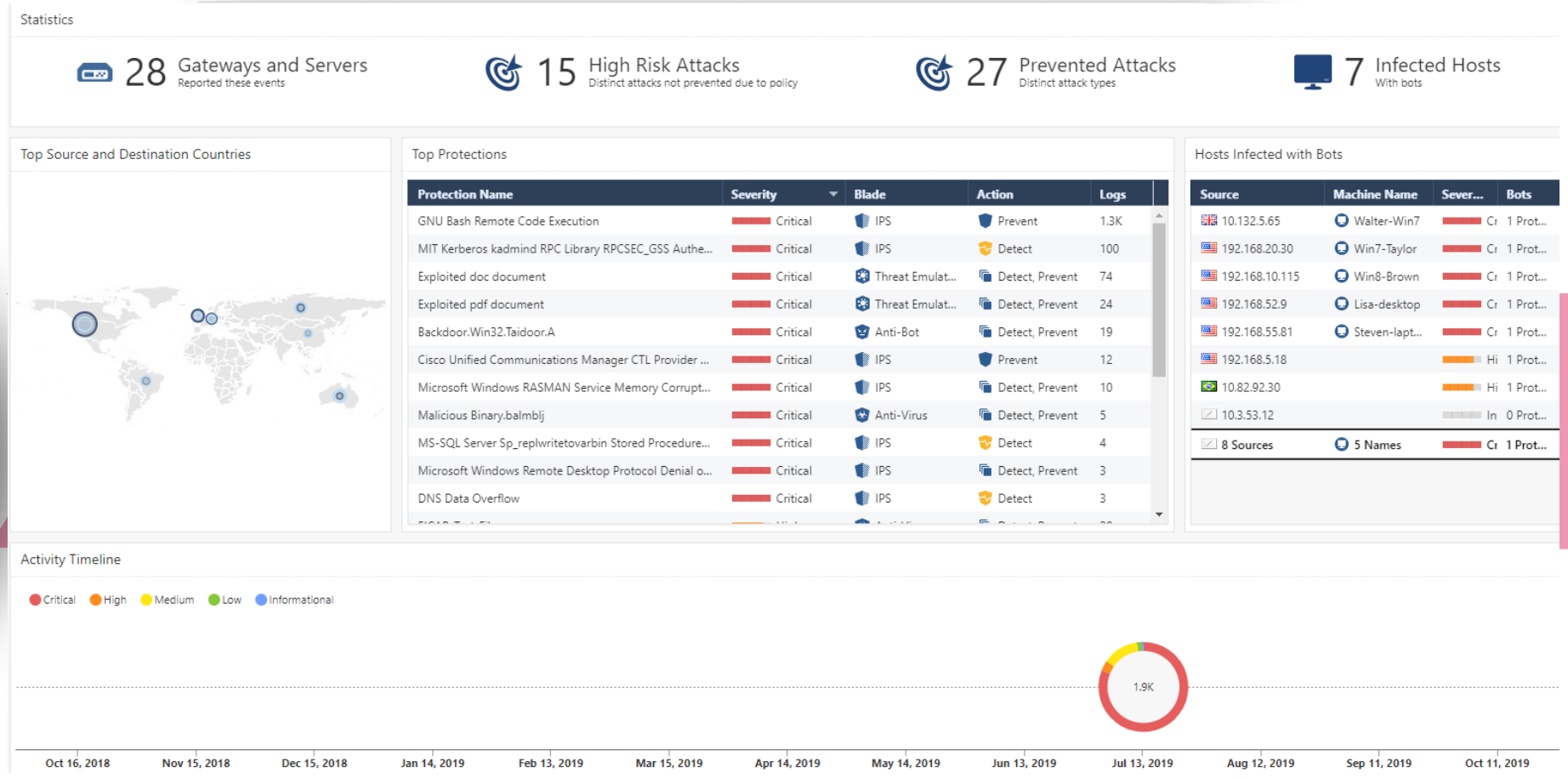
Надежные устройства для агрессивной среды

Детальное журналирование трафика

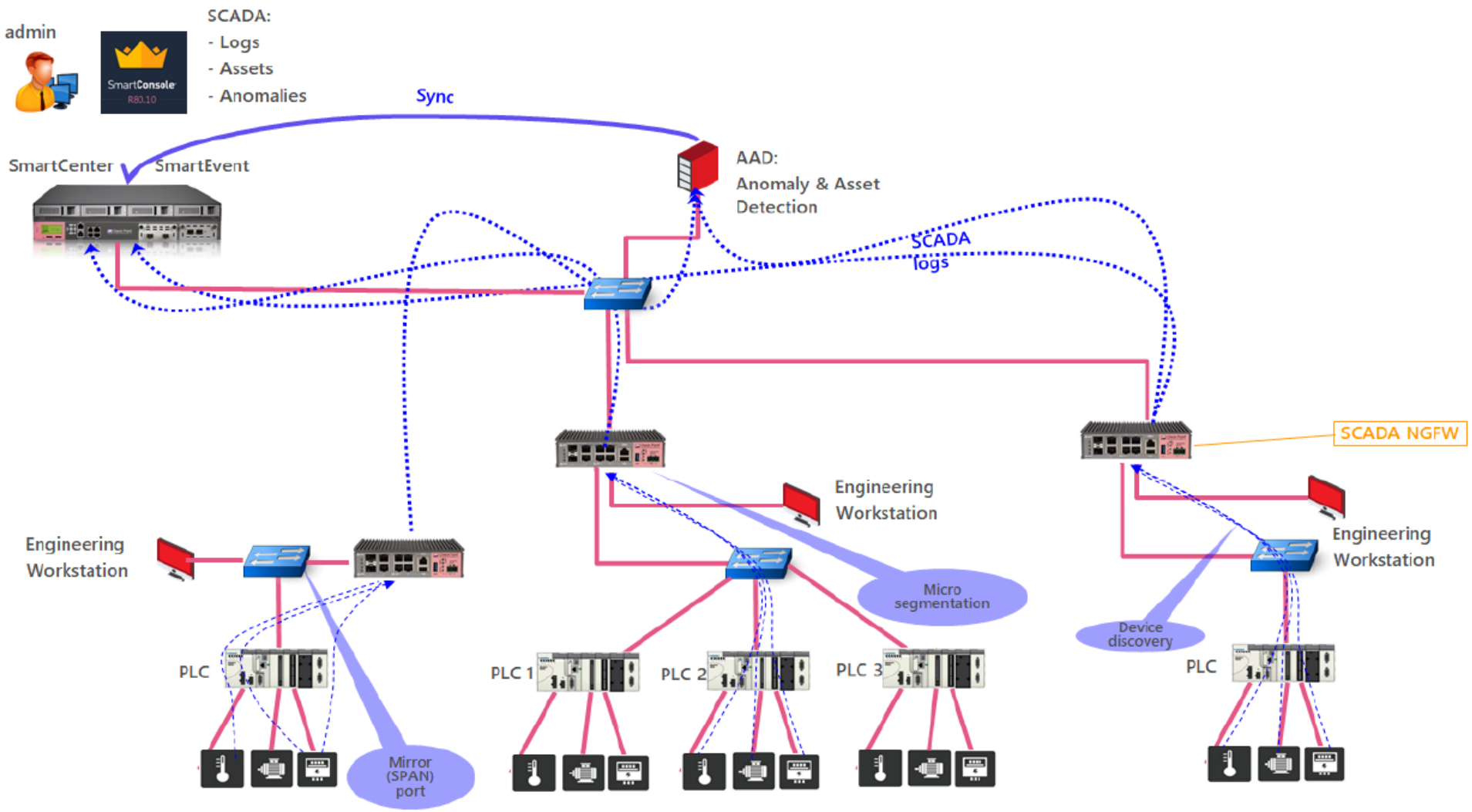
Детальная информация для расследования инцидентов

СГРУППИРОВАНО

CHECK POINT
SMARTLOG & SMARTEVENT

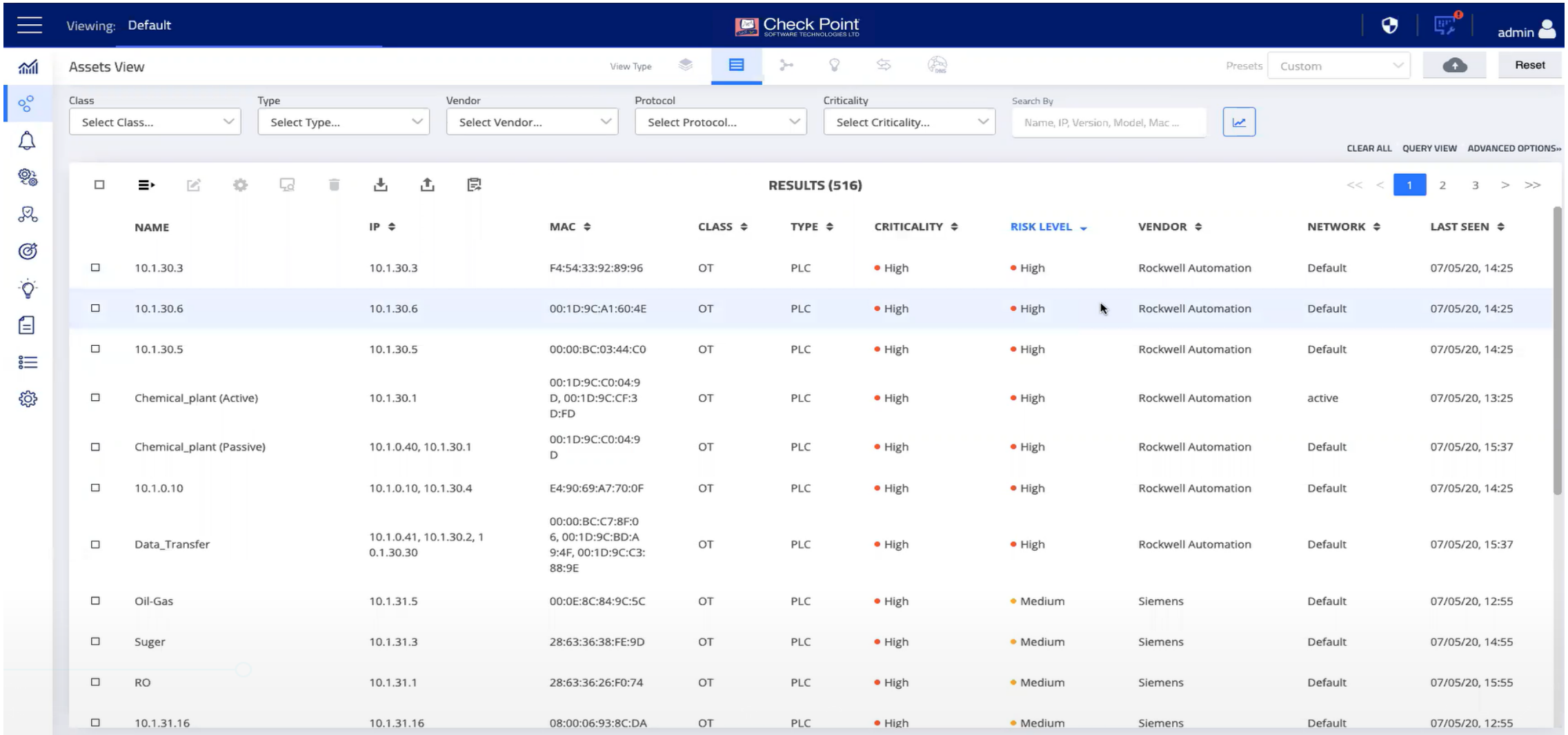


Архитектура Check Point AAD



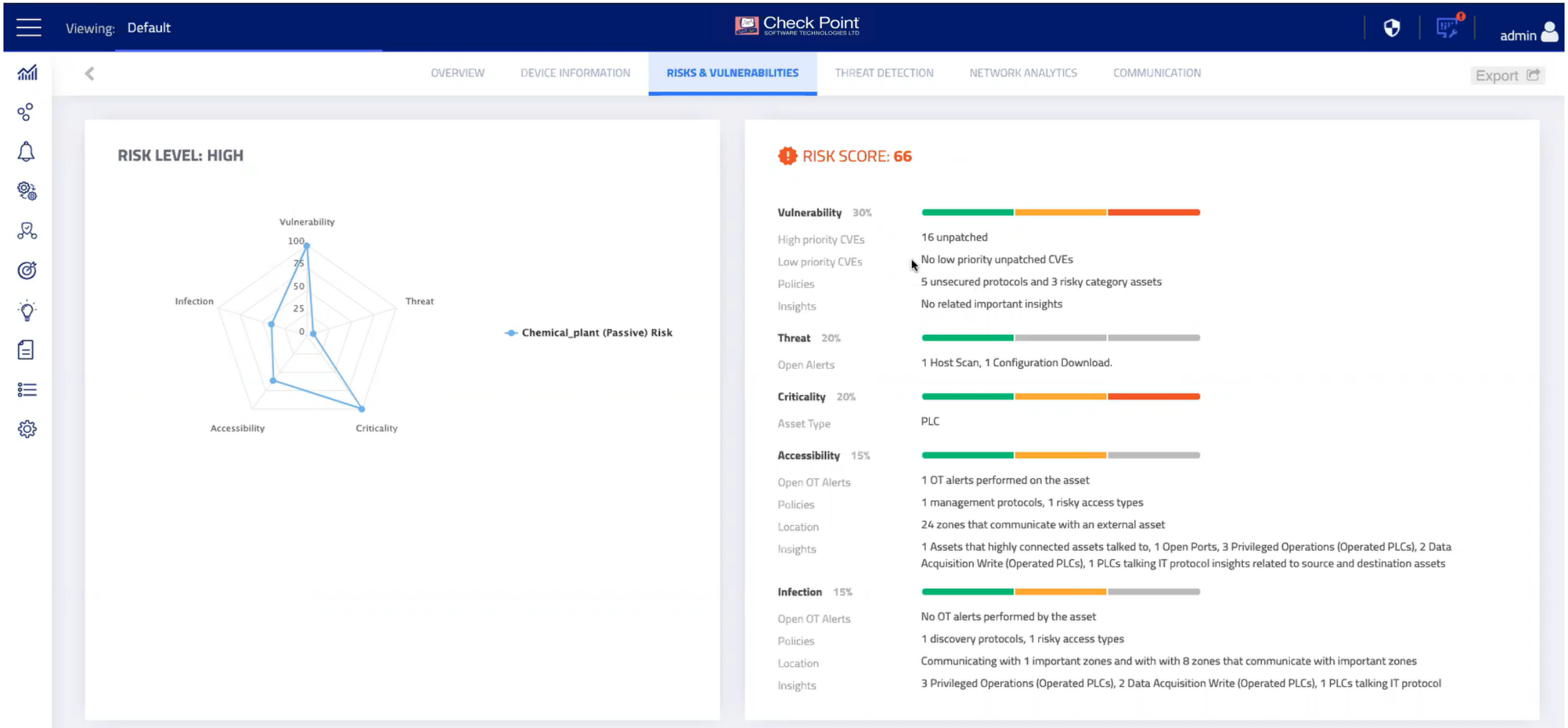
Информация об устройстве

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

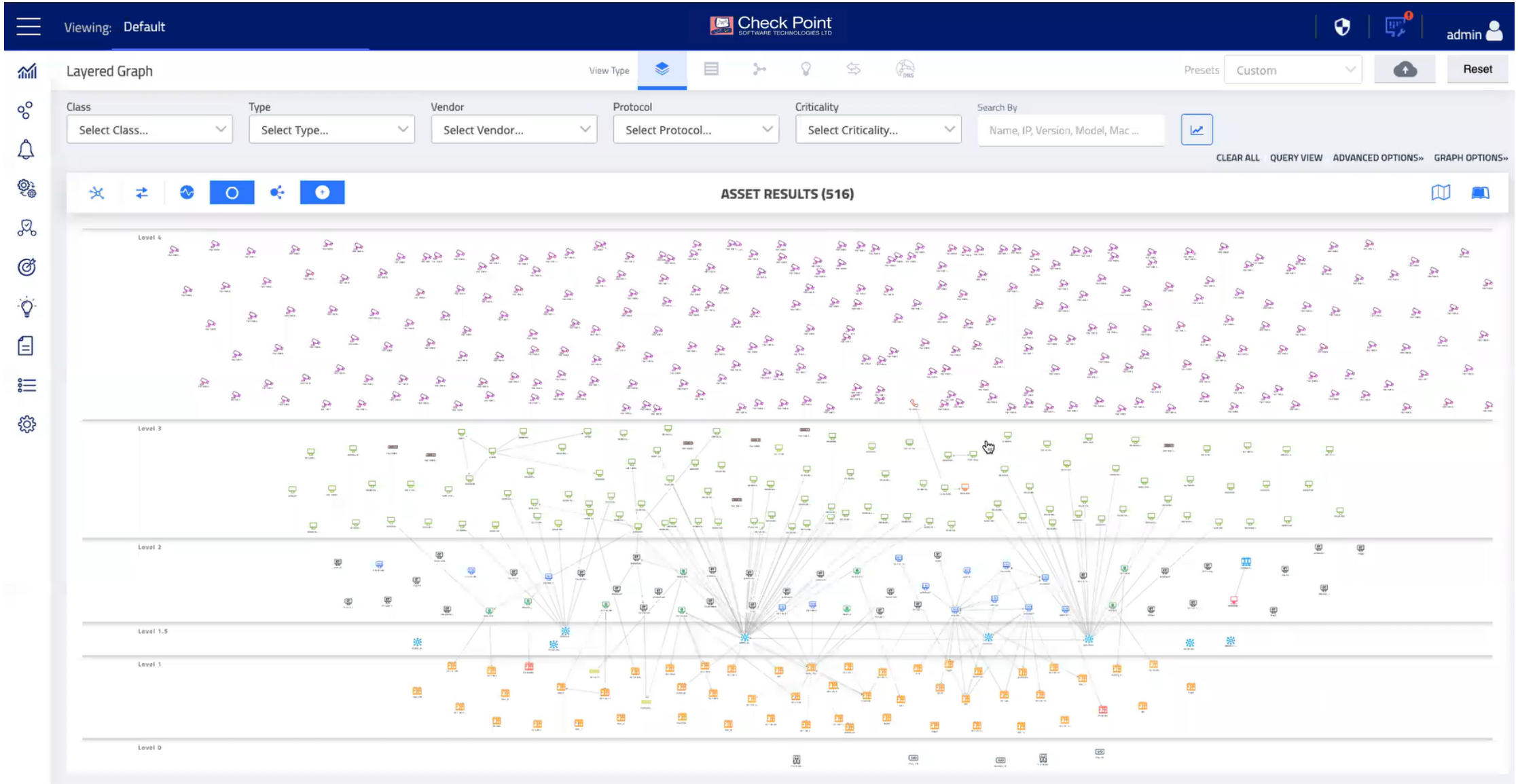


Информация об устройстве

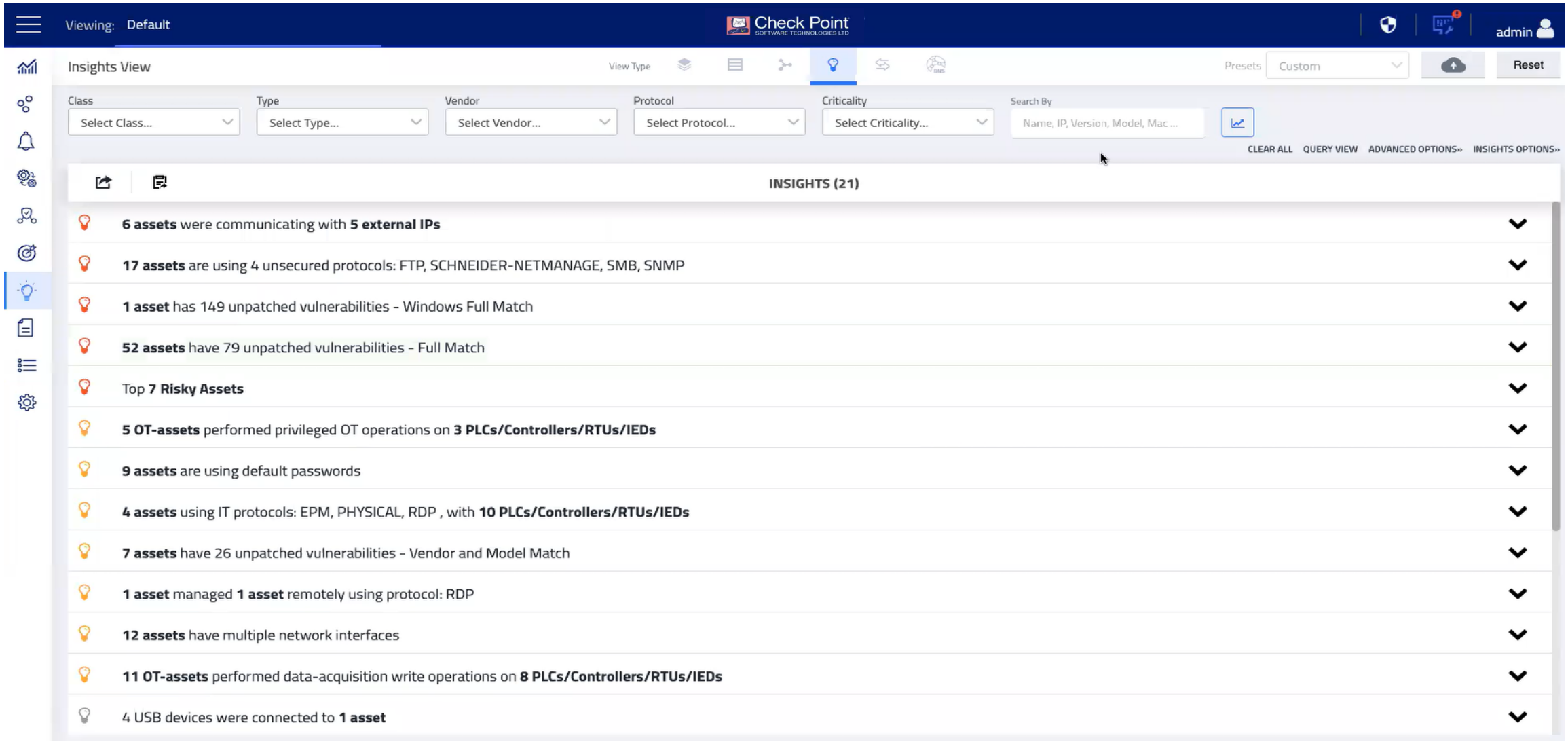
Детальная информация об устройстве – тип, производитель, версия прошивки и прочее



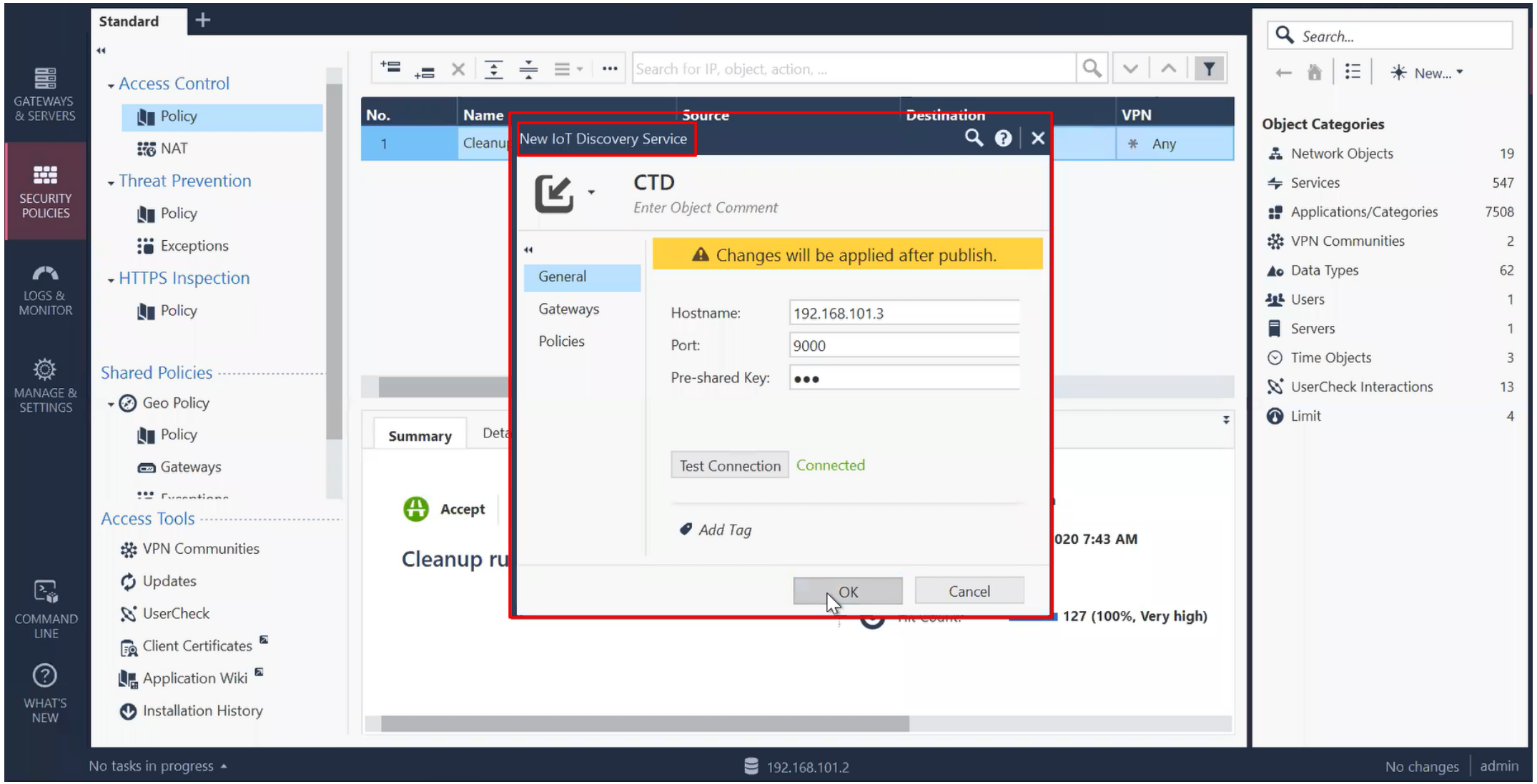
Информация об устройстве – иерархическая карта



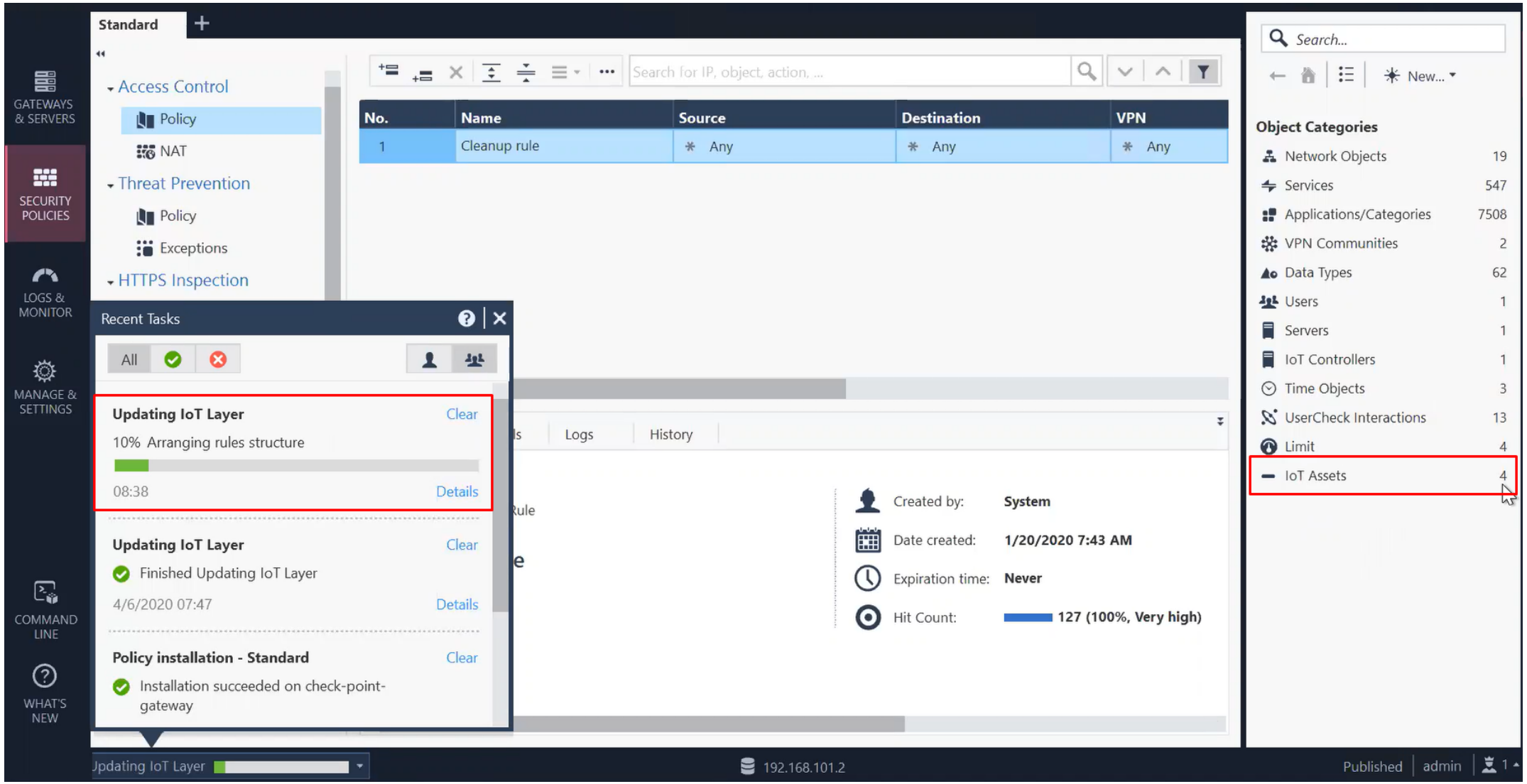
Оповещения на базе поведенческого анализа



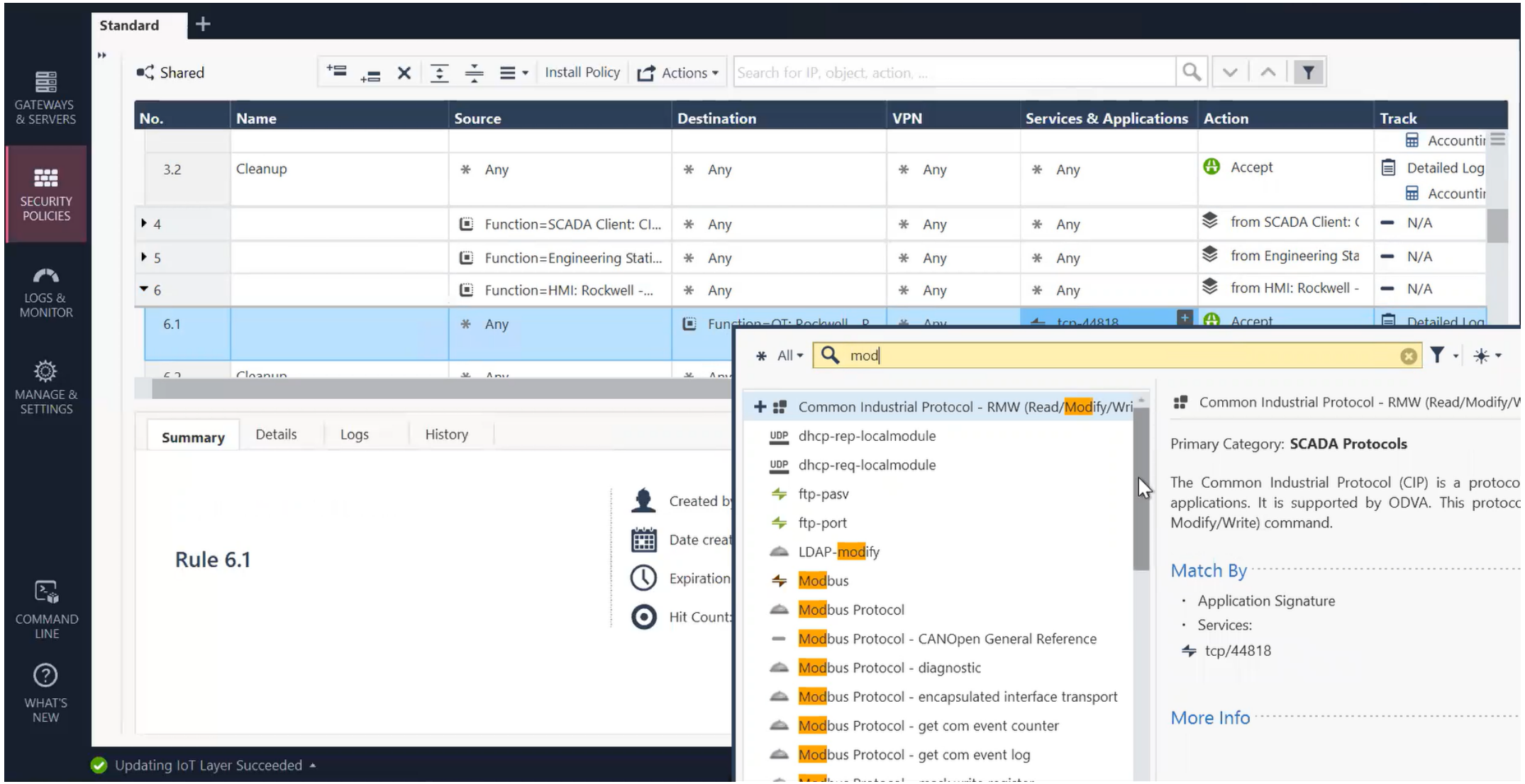
Автоматическое добавление устройств и создание политики



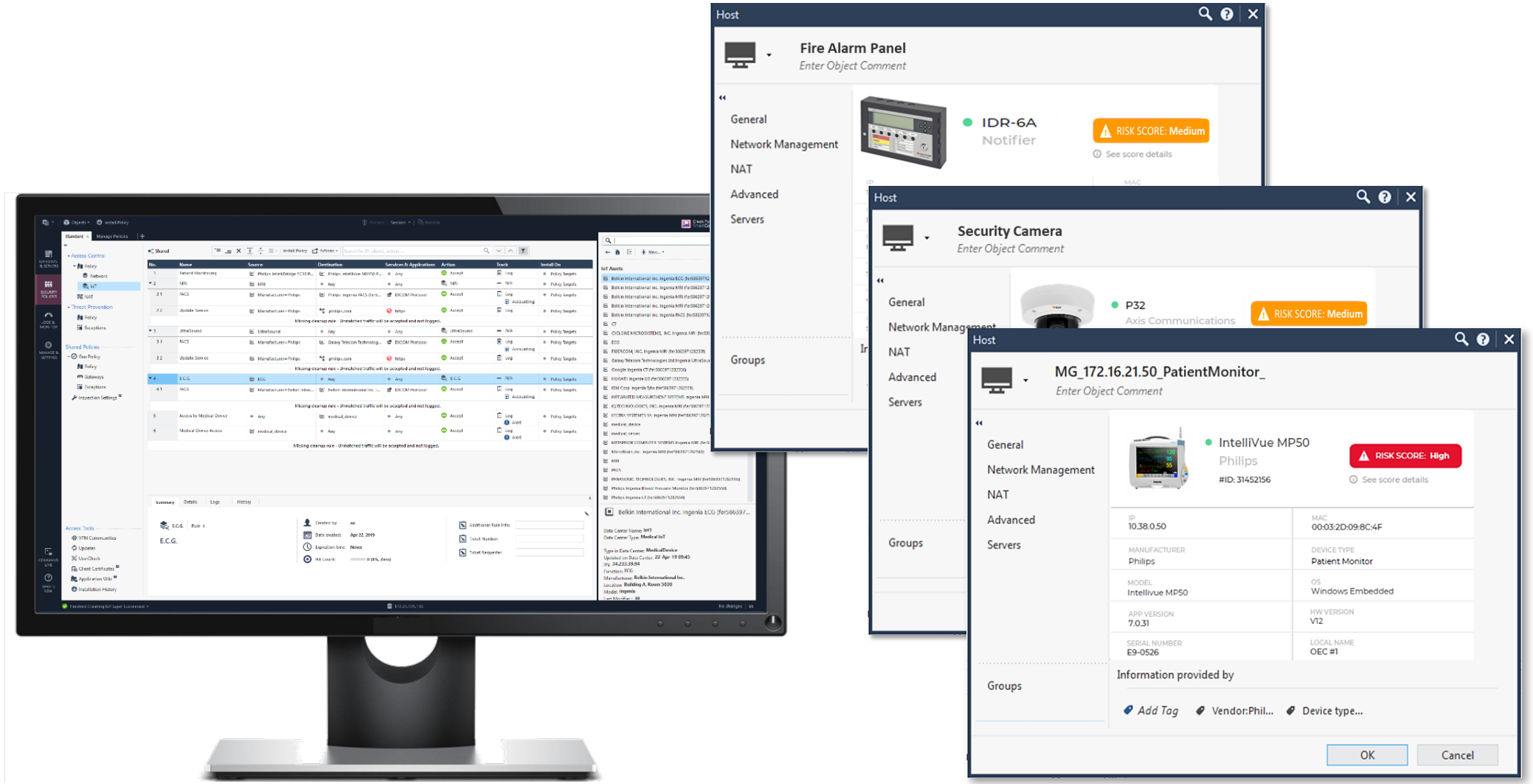
Автоматическое добавление устройств и создание политики



Автоматическое добавление устройств и создание политики



Автоматическое добавление устройств и создание политики



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

Компоненты КИИ редко обновляются

Siemens Global Website

ProductCERT Security Advisories

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

2016

- SSA-751155 (Last Update 2016-04-08): Denial-of-Service Vulnerabilit
- 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 Vulnerat
  OZW772

2015

- SSA-472334 (Last Update 2015-12-18): NTP Vulnerabilities in RUGG
  Devices
- SSA-763427 (Last Update 2016-04-29): Vulnerability in Communicatio
  modules SIMATIC CP 343-1, TIM 3V-IE, TIM 4R-IE, and CP 443-1
- SSA-921524 (Last Update 2016-04-29): Incorrect Frame Padding in P
- SSA-720081 (Last Update 2015-09-01): IP Forwarding in RUGGEDC
  Devices
- 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

Securi

- World presence
- Customer Care Centre
  - Contact
- Cybersecurity
  - News
  - Report an incident
- Substitution tool
- Counterfeiting
  - Counterfeiting
  - Definitions
  - Report a counterfeit
- Idea Submission

Date (dd/mm/yyyy)				
14/03/2016				
12/03/2016				
29/02/2016				
17/02/2016				
04/02/2016				
25/01/2016				
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

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

GLOBAL SITE - ENGLISH

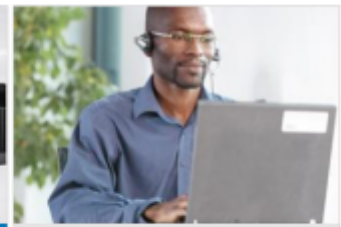
Power and productivity for a better world™ ABB

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

Виртуальный патчинг
Более 350 специализированных IDS/IPS сигнатур

Защита от уязвимостей
и обнаружение
аномального трафика

CHECK POINT
IPS

NSS Labs
Highest Rating

Protection	Sever...
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
Siemens Tecnomatix FactoryLink Stack Overflow Vulnerability	Critical
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 SCADA RMS Report Template WriteFile Command Buffer Overflow	Critical
IGSS SCADA STDREP Request Buffer Overflow	High
Iconics Genesis SCADA Freeing of Unitialized Memory Trigger	High
Rockwell RNA Message Negative Header Length	Critical
Intellicom NetBiter Config HICP Hostname Buffer Overflow	Medium
WonderWare SuiteLink DOS Attempt	High

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

Check Point 1570R

1570R Wi-Fi, LTE model

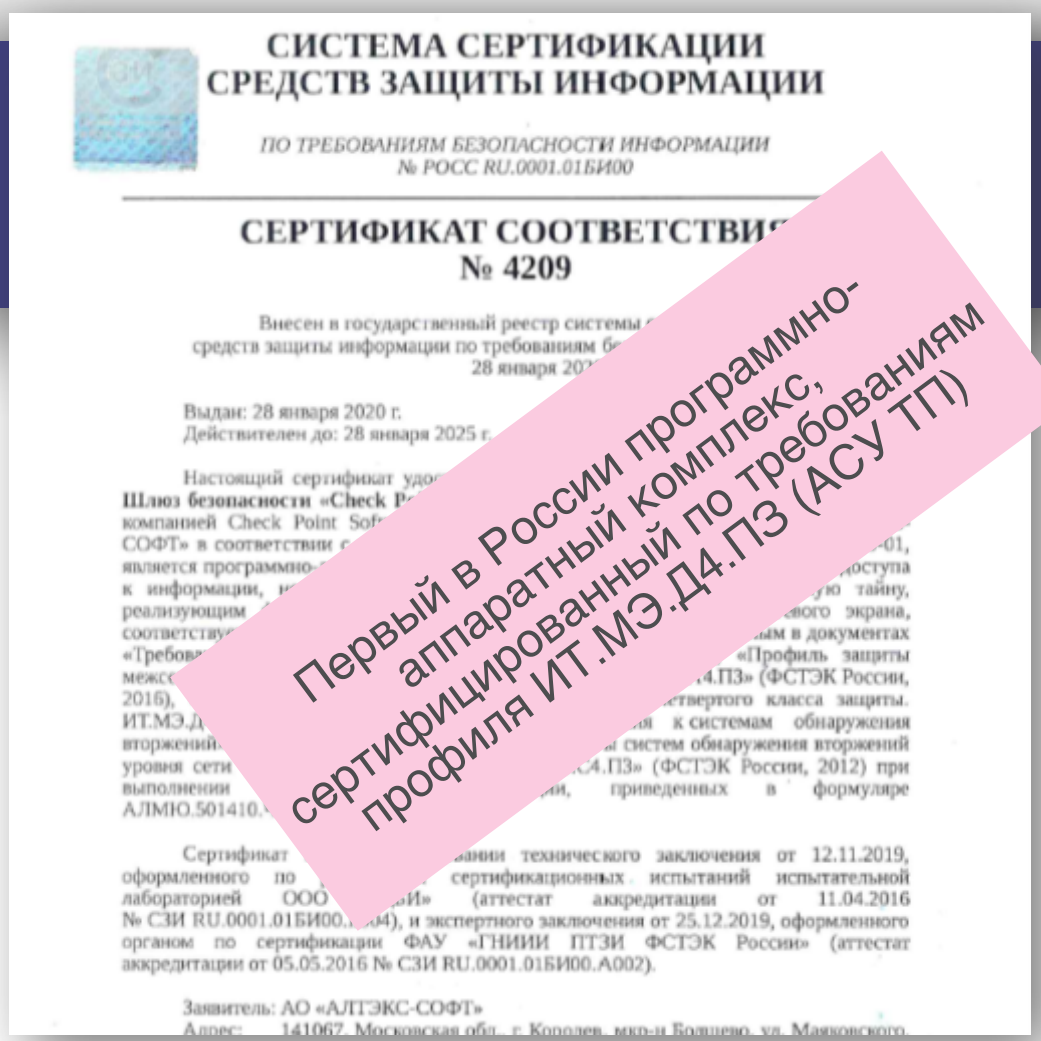
1. 802.11 n/ac Wi-Fi (optional)
2. 1x 1GbE WAN interface
3. LED tower
4. 8x 1GbE LAN switch
5. 1x 1GbE DMZ interface
6. USB-C console port
7. DB9 RS232/422/485 to PLCs
8. USB 3.0 port
9. GPS connector
10. AC to DC power adapter connection
11. Ground screw
12. DC power connector
13. Embedded LTE modem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

8x1GbE ports

400 Mbps Threat Prevention

Dual band 802.11ac 3X3 MIMO

Государственный реестр сертифицированных средств защиты информации



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4209

Внесен в государственный реестр системы
средств защиты информации по требованиям бе
28 января 202

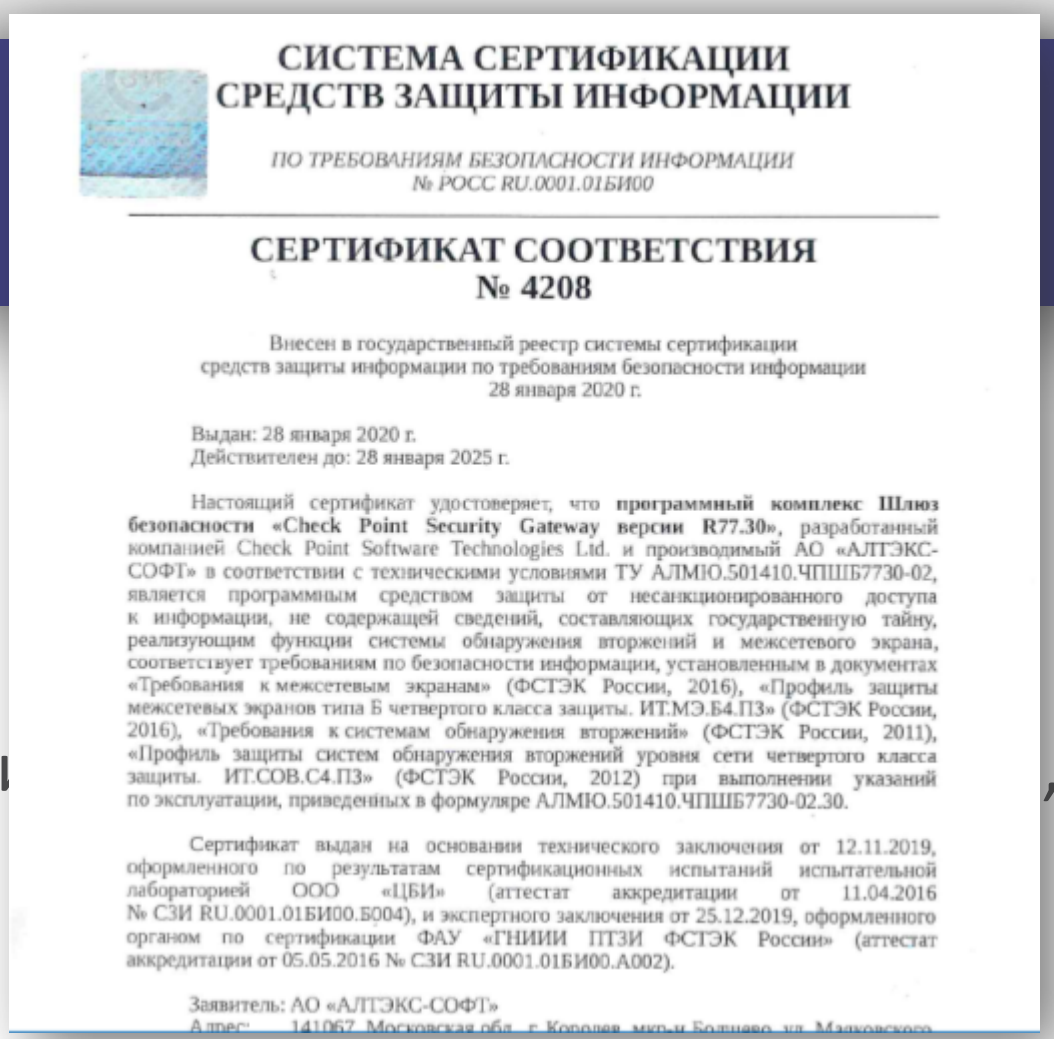
Выдан: 28 января 2020 г.
Действителен до: 28 января 2025 г.

Настоящий сертифик
Шлюз безопасности «Check P
компанией Check Point Soft
СОФТ» в соответствии с
является программно-
к информации,
реализующим
соответству
«Требова
межсе
2016),
ИТ.МЭ.Д
вторжений
уровня сети
выполнении
АЛМЮ.501410.

Сертификат
оформленного по
лабораторией ООО
№ СЗИ RU.0001.01БИ00.
органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «АЛТЭКС-СОФТ»
Адрес: 141067, Московская обл., г. Королев, мкр-н Болшево, ул. Маяковского,

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



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4208

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
28 января 2020 г.

Выдан: 28 января 2020 г.
Действителен до: 28 января 2025 г.

Настоящий сертификат удостоверяет, что **программный комплекс Шлюз безопасности «Check Point Security Gateway версии R77.30»**, разработанный компанией Check Point Software Technologies Ltd. и производимый АО «АЛТЭКС-СОФТ» в соответствии с техническими условиями ТУ АЛМЮ.501410.ЧПШБ7730-02, является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции системы обнаружения вторжений и межсетевого экрана, соответствует требованиям по безопасности информации, установленным в документах «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 вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012) при выполнении указаний по эксплуатации, приведенных в формуляре АЛМЮ.501410.ЧПШБ7730-02.30.

Сертификат выдан на основании технического заключения от 12.11.2019, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004), и экспертного заключения от 25.12.2019, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «АЛТЭКС-СОФТ»
Адрес: 141067, Московская обл., г. Королев, мкр-н Болшево, ул. Маяковского,

Государственный реестр сертифицированных средств защиты информации

4208	28.01.2020	28.01.2025	программный комплекс Шлюз безопасности «Check Point Security Gateway версии R77.30»	Соответствует требованиям документов: 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 «ГНИИИ ПТЗИ ФСТЭК России»	АО «АЛТЭКС-СОФТ»	141067, Московская г. Королев Болшево, ул. Маяко д. 10А, пом (495) 543-310	31.12.2023
4209	28.01.2020	28.01.2025	программно-аппаратный комплекс Шлюз безопасности «Check Point Security Gateway версии R77.30»	Соответствует требованиям документов: 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 «ГНИИИ ПТЗИ ФСТЭК России»	АО «АЛТЭКС-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

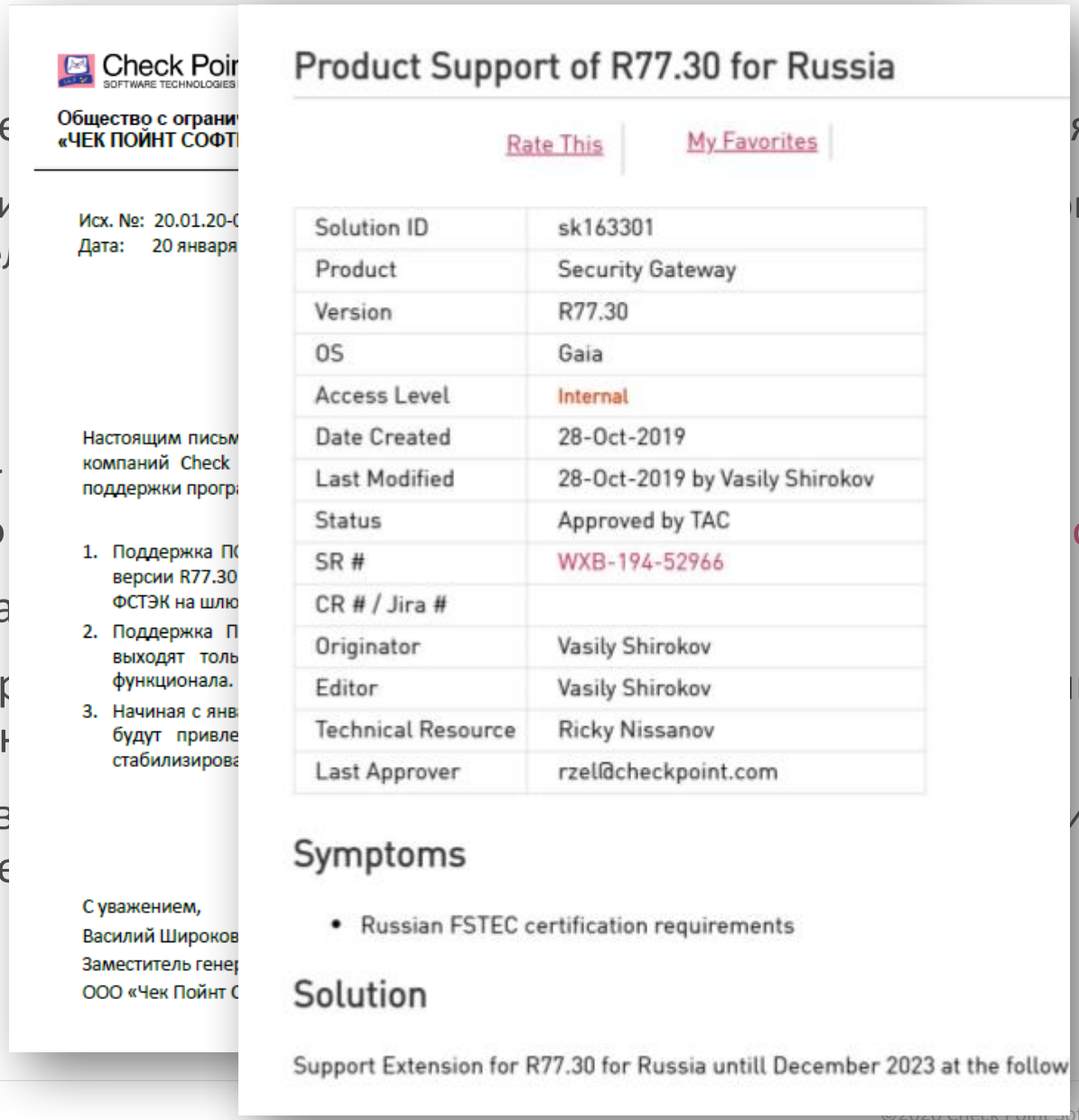
Потребитель, не являющийся заявителем

Срок де явителя).

Сертифи к по обращению
заявител

Может срока действия
сертиф овий:

- за
- пр иям по защите
ин
- се ию находятся в
Ре



Check Poi
SOFTWARE TECHNOLOGIES

Общество с ограни
«ЧЕК ПОЙНТ СОФТ

Исх. №: 20.01.20-
Дата: 20 января

Настоящим письм
компаний Check
поддержки програ

1. Поддержка П
версии R77.30
ФСТЭК на шлю
2. Поддержка П
выходят толь
функционала.
3. Начиная с янв
будут привле
стабилизирова

С уважением,
Василий Широков
Заместитель генер
ООО «Чек Пойнт С

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	rzell@checkpoint.com

Symptoms

- Russian FSTEC certification requirements

Solution

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

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 «АЛТЭКС-СОФТ» (АО «АЛТЭКС-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, 2012)

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 «АЛТЭКС-СОФТ» (АО «АЛТЭКС-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®
SOFTWARE TECHNOLOGIES LTD

СПАСИБО!