



Check Point®
SOFTWARE TECHNOLOGIES LTD.

Тренды и технологии 2022 для защиты АСУ ТП от Check Point Software

Дмитрий Кудра | Консультант по безопасности

A large white arrow pointing to the right, with the text 'ONE STEP AHEAD' in white capital letters. The arrow is set against a dark background that includes a silhouette of a palm tree on the right side.

ONE STEP AHEAD



Март 2019

Атака шифровальщиком LockerGoga на Norsk Hydro

Май 2021

Атака шифровальщиком трубопровод Colonial Pipeline

Атака на завод Norsk Hydro

LockerGoga

Целевая
фишинговая
рассылка

Распространение
вредоносного
кода используя
групповые
политики AD

Шифрование как
документов так и
системных файлов

Частичная
остановка бизнес
процессов

Атака на трубопровод Colonial Pipeline



Получили пароль от
сервиса удаленного
управления RD

Распространение
вредоносного
кода по сети

Шифрование как
документов так и
системных файлов
Отправка на
внешний ресурс

Частичная
остановка бизнес
процессов



Отчет ICS-CERT

Самые распространенные риски 2021 года



Check Point
SOFTWARE TECHNOLOGIES LTD.

Область	Место	Описание рисков
Сегментация сетей	1	Неавторизованный доступ к критической инфраструктуре и OT-сетями
Идентификация и аутентификация	2	- Отсутствие учетных записей - Повышение рисков при увольнении сотрудников, особенно сотрудников с повышенным уровнем доступа
Человеческие ресурсы	3	- Отсутствие резервного персонала для замещения ролей основного - Снижение уровня знаний, необходимых для работы с системами управления
Физическая безопасность	4	- Несанкционированный физический доступ повышает риски: - добавления сторонних устройств для перехвата/перенаправления трафика - злонамеренной модификации, удаления или копирования информации - доступа к компонентам критической информационной инфраструктуры - кражи или уничтожения компонентов КИИ
Управление пользователями	5	- Компрометация паролей в силу незащищенности каналов связи - Несанкционированный доступ к компонентам критической инфраструктуры

**СЕДЬМОЙ ГОД
ПОДРЯД!**



Check Point®
SOFTWARE TECHNOLOGIES LTD.

КАКИМ ОБРАЗОМ МЫ
МОЖЕМ ОСТАВАТЬСЯ
НА ШАГ ВПЕРЕДИ УГРОЗ?

ONE STEP AHEAD

Лучшие практики защиты КИИ

Обеспечить
безопасность
IT- и OT-
окружений

Защитить корпоративную сеть
предприятия от угроз

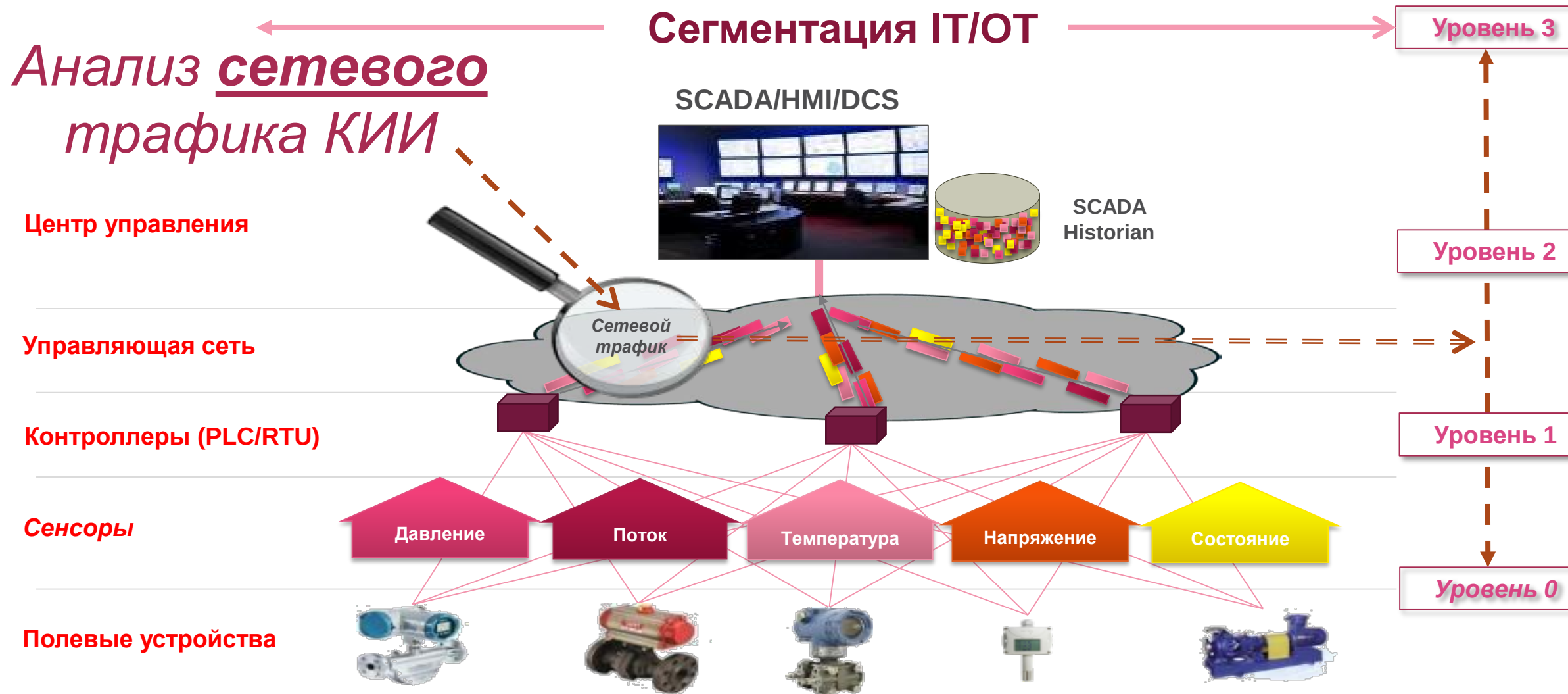
Обеспечить четкое разделение
между IT- и OT-инфраструктурами

Внедрить специализированные
системы защиты для КИИ

Мониторинг трафика КИИ в реальном времени



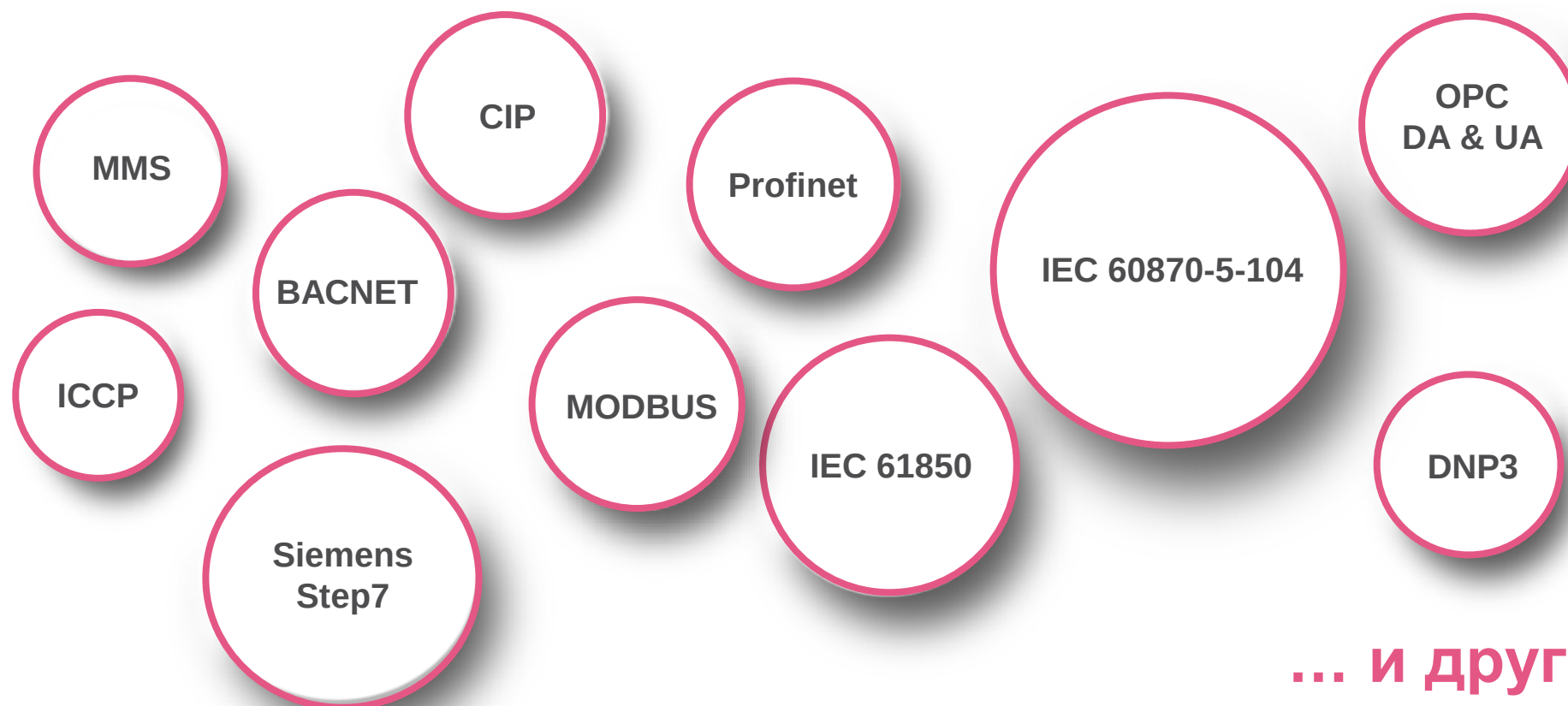
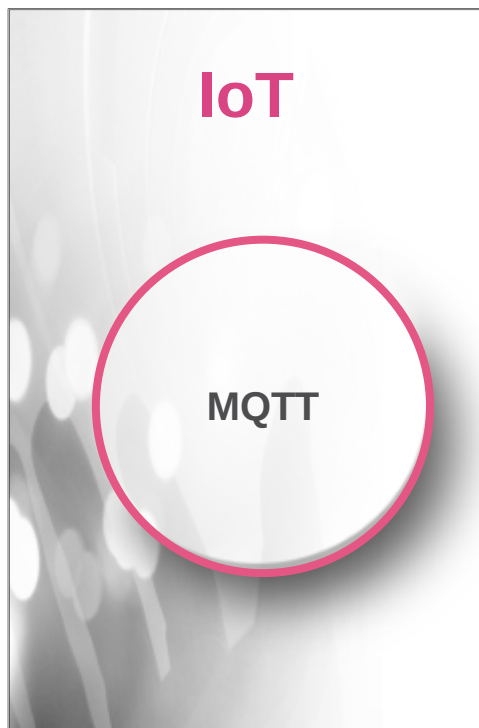
Check Point
SOFTWARE TECHNOLOGIES LTD.



Поддержка специализированных протоколов



Check Point
SOFTWARE TECHNOLOGIES LTD.



... и другие

Более **1000 SCADA и IoT** команд
в Check Point Application Control

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

Компоненты КИИ редко обновляются



Check Point



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
- 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 Vulnerability in OZW772

2015

- SSA-472334 (Last Update 2015-12-18): NTP Vulnerabilities in RUGGED Devices
- SSA-763427 (Last Update 2016-04-29): Vulnerability in Communication 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 F
- 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

Support

You are here: Home > Support > Cybersecurity > Vulnerabilities

Security

World presence

Customer Care Centre

- Contact

Cybersecurity

- News
- Report an incident

Substitution tool

Counterfeiting

- Counterfeiting
- Definitions
- Report a counterfeit

Idea Submission

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

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

©2019 Check Point Software Technologies Ltd.

10

Виртуальный патчинг

Более 300 специализированных IDS/IPS сигнатур



Check Point®
SOFTWARE TECHNOLOGIES LTD.

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 SCADARMS Report Template WriteFile Command Buffer Overflow	Critical
IGSS SCADA STDREP Request Buffer Overflow	High
Iconics Genesis SCADA Freeing of Uninitialized Memory Trigger	High
Rockwell RNA Message Negative Header Length	Critical
Intellicom NetBiter Config HICP Hostname Buffer Overflow	Medium
WonderWare SuiteLink DOS Attempt	High

Мониторинг промышленной сети

Информация о взаимодействии

- Протоколы и команды
- Внутрисистемные связи
- Открытые и проприетарные протоколы

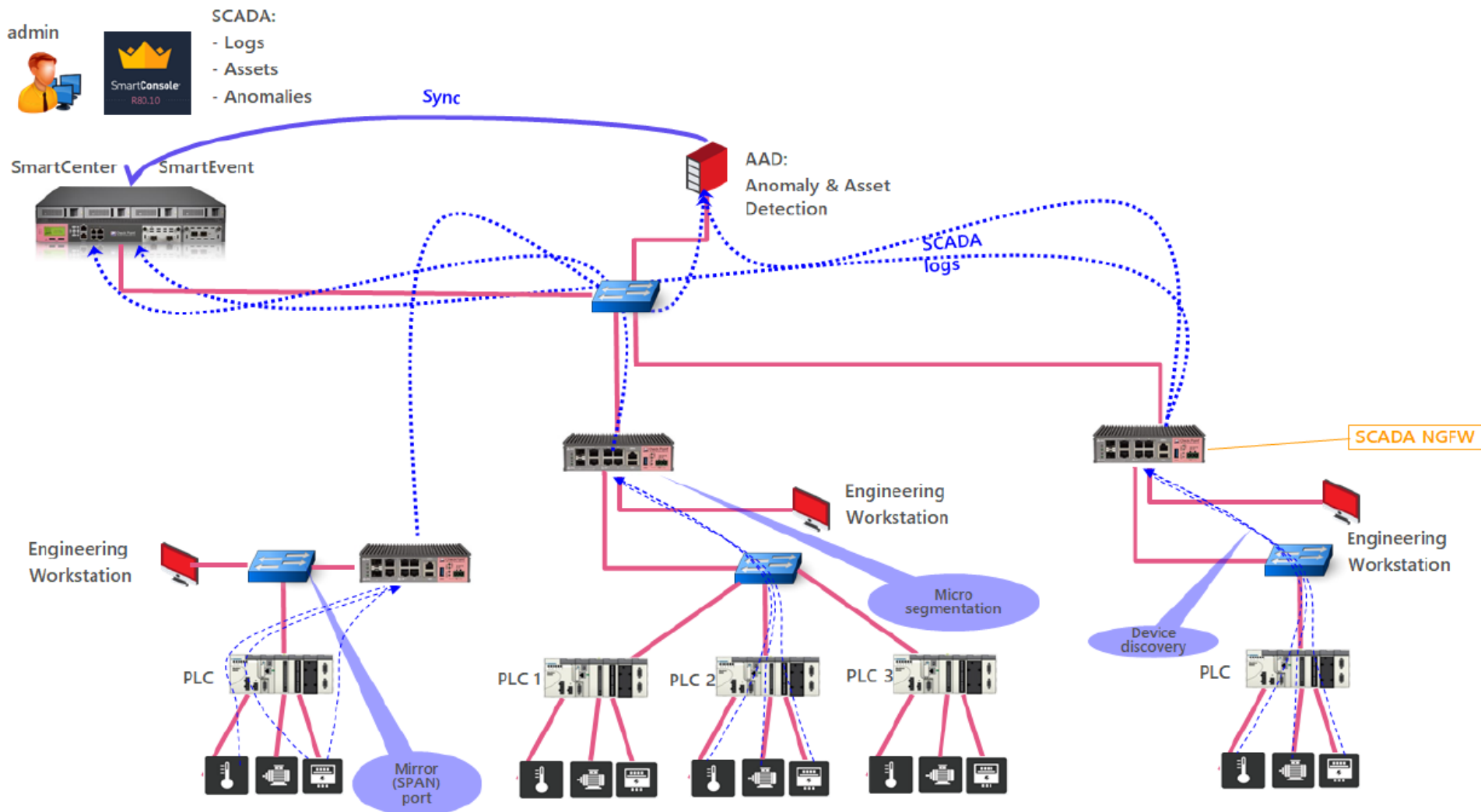
Информация об устройствах

- IP- и MAC-адреса
- Производитель устройства
- Тип устройства (PLC, HMI, рабочая станция, коммутатор, итд)
- Модель и серийный номер
- Версия прошивки

Информация о сети

- Какие устройства работают в вашей сети?
- Каким образом эти устройства взаимодействуют между собой и внешним миром?
- Существуют ли ошибки конфигурации и уязвимости?

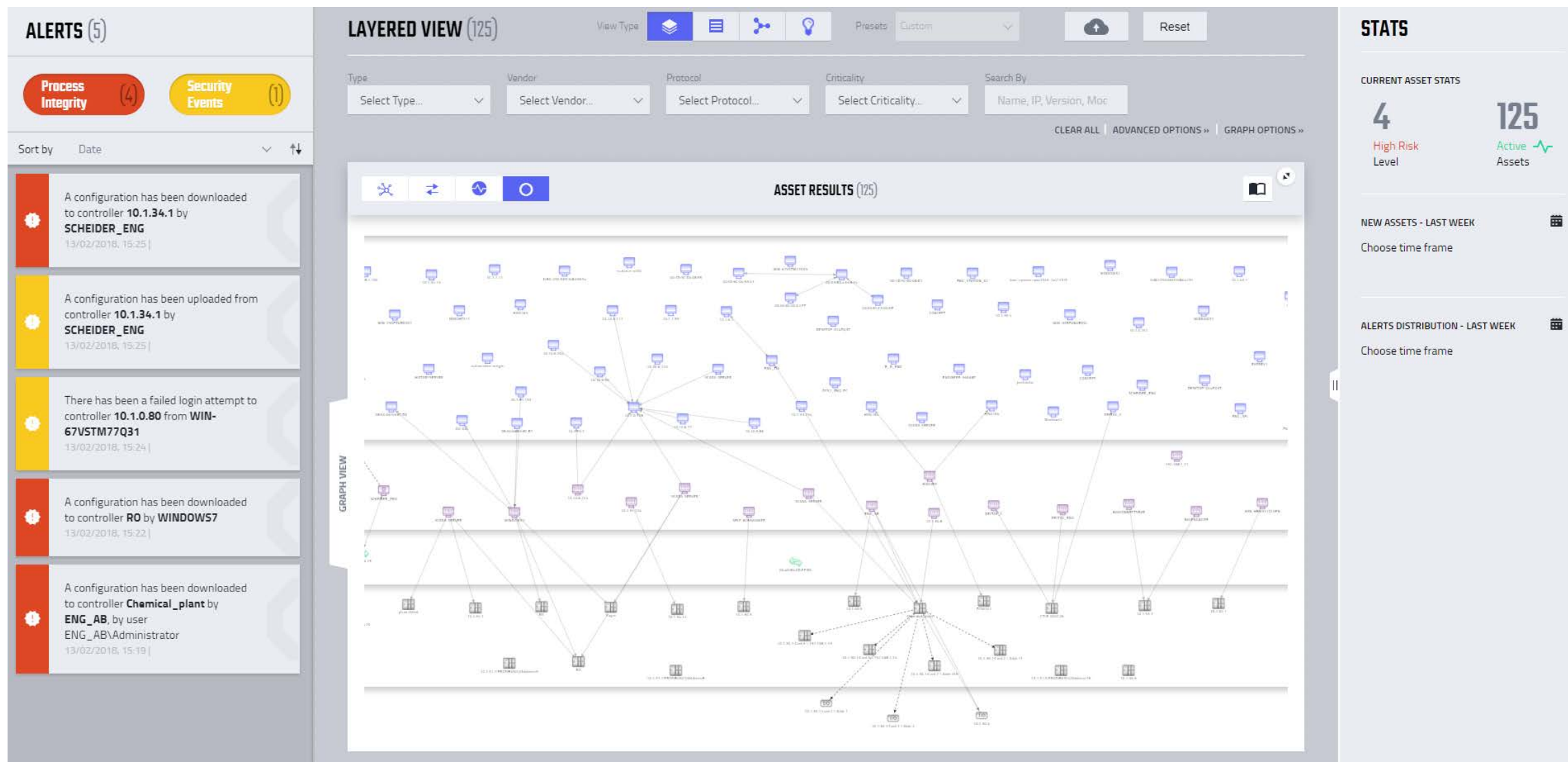
Архитектура Check Point и Claroty CTD



Информация об устройстве – иерархическая карта



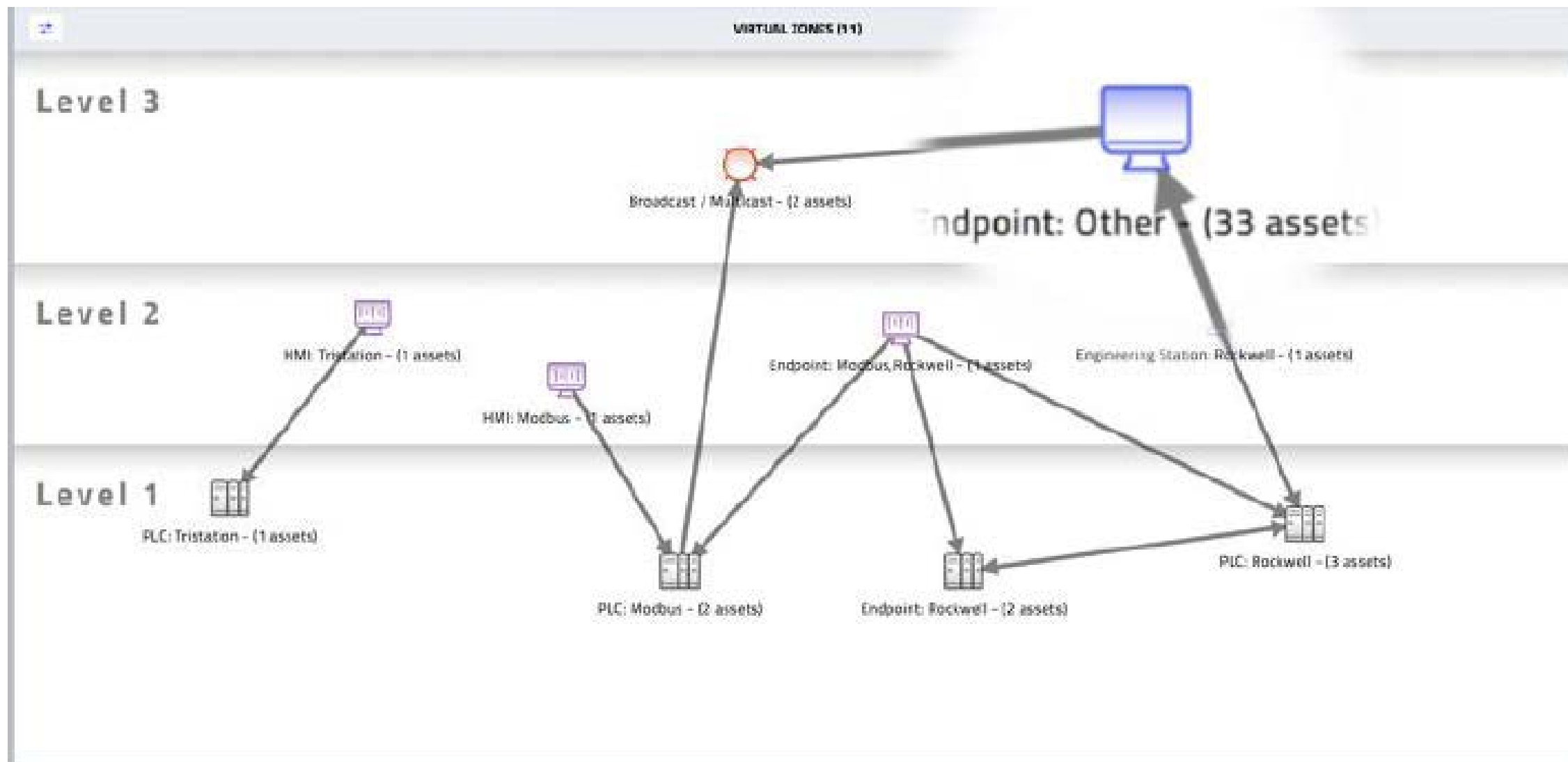
Check Point
SOFTWARE TECHNOLOGIES LTD.



Автоматическое распределение по уровням



Check Point
SOFTWARE TECHNOLOGIES LTD.



Примеры оповещений об операционных событиях



Check Point
SOFTWARE TECHNOLOGIES LTD.

- **Загрузка конфигурации** (Configuration Upload): код загружается с инженерной станции на контроллер (PLC).
- **Выгрузка конфигурации** (Configuration Upload): код скачивается с контроллера (PLC) на инженерную станцию
- **Изменение режима работы** (Mode Change): смена режима на контроллере (Program, Run, Monitor)
- **Обновление прошивки** (Firmware Upgrade): обновление прошивки контроллера.
- **Изменение информации об объекте** (Info Change): изменения уникальных идентификаторов объекта (IP адрес, имя и т.д.)
- **Редактирование конфигурации онлайн** (Online Edit): изменения программы во время работы контроллера

Информация об устройстве

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



NORMAL RISK LEVEL



Chemical_plant/ **Rockwell Automation**

PLC



DEVICE INFORMATION

IP
10.1.30.1

MAC
00:1D:9C:C0:04:9D

Network
Default

VLAN
0

Protocols
ARP / CIP / ENIP / ICMP / TCP

Site
Default

Vendor
Rockwell Automation

Model
1756-ENBT/A

Firmware version
V6.006

Serial
00987DBF

MORE DETAILS

Type 
PLC

Criticality 
HIGH

Risk Level
Normal

First seen
13/02/2018 15:18:21

Last seen
13/02/2018 15:23:35

Оповещения на базе поведенческого анализа



Check Point
SOFTWARE TECHNOLOGIES LTD.



INTEGRITY - CRITICAL

Firmware Download

Controller firmware download performed to controller Conveyor_Belt by ENGSTATION

[What does this mean?](#)

A firmware upgrade may introduce new vulnerabilities that have not previously existed. Therefore, this action should be examined and carefully considered before it is done. If an attacker is aware of this vulnerability, he/she may perform a firmware change in order to be able to perform more destructive actions. Since critical infrastructure is involved, such activity is severe and must trigger an alarm.

[Archive](#)[Approve](#)[Assign to](#)



MITIGATION STEPS

1. Verify if this maintenance work was scheduled.
2. If not, check it with the OT engineer that is the owner of this asset.

ALERT DETAILS - ID #309[Event Details](#)

**ENGSTATION**

IP	10.1.33.100 10.1.0.170 10.1.34.8	Criticality	High
MAC	00:50:56:B9:A1:F4	Virtual Zone	Engineering Station; Other
Network	Default	Vendor	VMware, Inc.
Risk Level	High	Host Name	ENGSTATION
Site	Demo_Site	Operating System	Windows 7/Server 2008 R2
Planned Asset	No		
Asset Type	Engineering Station		

**Conveyor_Belt**

IP	10.1.34.1
MAC	00:80:F4:12:8B:10
Network	Default
Risk Level	High
Asset Type	PLC
Site	Demo_Site
Criticality	High
Vendor	Schneider Electric
Model	M340 (BMX P34 2020)
Firmware Version	02.80

Примеры оповещений событиях безопасности

- **Новый объект** (New Asset): обнаружено новое устройство в сети
- **Ошибка входа** (Failed Login): ошибка при вводе логина/пароля
- **Сканирование сети** (Network Scan): устройство в сети сканирует множество других устройств на наличие открытых портов
- **Сканирование портов** (Port Scan): устройство сканирует открытые порты другого устройства
- **Атака Man-in-the-Middle**: скомпрометированное устройство инициирует назначение себе IP адресов других устройств для перехвата трафика
- **Обнаружение уязвимости** (CVE Matching): идентифицируются устройства с известными уязвимостями
- **Обнаружение угрозы** (Known Threat Alert): идентифицируются угрозы

Оповещения на базе поведенческого анализа



SECURITY - CRITICAL

Man In The Middle

A Man-In-The-Middle attack with MAC 005056b9c47b detected

Archive

Approve

Assign to

What does this mean?

A man-in-the-middle attack (MITM) indicates that an attacker inserted a new machine into the communication pathway between two assets within the network. This new machine will use this position to either monitor the communication between these assets, or to alter the communication between these assets. Whenever a MITM attack is generated, it will capture both the new machine that is inserted into the communication pathway, and both of the assets affected by the attack. The new asset added should be identified and removed or remediated to prevent it from being used in an attack again in the future. The pathway the attacker utilized to compromise the attacking machine should be evaluated as well. Additionally, all the actions taken during the man in the middle attack will be captured and should be used to reverse any changes made to the affected assets.



MITIGATION STEPS

1. Attack alarm! Report this activity to your Security Risk Officer as soon as possible.

ALERT DETAILS - ID #91

Event Details



10.1.0.41



10.1.0.41



Chemical_plant

IP

10.1.0.41

Criticality

Medium

MAC

00:00:BC:C7:BF:06

Virtual Zone

OT: Other

Network

Default

Vendor

Rockwell Automation

Risk Level

Normal

Site

Demo_Site

Personal Asset

No

IP

10.1.0.41

Criticality

Medium

10.1.0.31

Virtual Zone

OT: Other

10.1.0.40

Vendor

VMware, Inc.

fa80:250:56ff:feb9:c47b

MAC

00:50:56:B9:C4:7B

Network

Default

Risk Level

High

IP

10.1.30.1

Criticality

High

10.1.0.40

Virtual Zone

PLC: Other

00:1D:9C:C0:04:9D

MAC

Rockwell Automation

Network

Default

Vendor

Rockwell Automation

Risk Level

High

Serial Number

00987DBF

Site

Demo_Site

Model

1756-ENBT/A

Personal Asset

No

Virtual Zone

©2019 Check Point Software Technologies Ltd.

20

Удобство тестирования и анализа трафика удаленно



Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point
SOFTWARE TECHNOLOGIES LTD.

ConfigurationMaintenanceMonitoringSimulation

Play PCAPs

#	File name	Size	Upload Date	Detect Known Threats			
1	log_2017-11-13.0.1510578316.033351.pcap	96.00 MB	2019/03/25 08:13:17	☐	Play RT	Play	Delete
2	open_zdv_5.1.2(report 1).pcap	143.82 KB	2019/03/25 08:13:51	☐	Play RT	Play	Delete
3	plc_stop.pcap	1.21 KB	2019/03/25 08:14:00	☐	Play RT	Play	Delete
4	plcRun.pcap	1.22 KB	2019/03/25 08:14:09	☐	Play RT	Play	Delete
5	scanTSAP.pcap	193.09 KB	2019/03/25 08:14:24	☐	Play RT	Play	Delete
6	set_clock_11112011.pca	10.68 KB	2019/03/25	☐	Play RT	Play	Delete

Upload PCAP

Выберите файл Файл не выбран

UploadCancel

Автоматическая генерация и применение политики



Check Point
SOFTWARE TECHNOLOGIES LTD.

The screenshot displays the Check Point SmartConsole interface. On the left, the 'Access Control' menu is expanded, and the 'IoT' option is highlighted with a red box. A yellow callout box with the text 'Separate IoT Security Layer' points to this option. The main pane shows a table of 'IoT Security Rules'. A yellow callout box with the text 'IoT Security Rules' points to this table. The table has columns: No., Name, Source, Destination, Services & Applications, Action, Track, and Install On. It lists several rules for medical devices like MRI, PACS, and ECG. Below the table, the 'Summary' tab for 'Rule 4' is shown, displaying details like 'Created by: aa', 'Date created: Apr 22, 2019', and 'Hit Count: 0 (0%, Zero)'. On the right, the 'IoT Assets' pane is visible, showing a list of assets. A yellow callout box with the text 'IoT Assets' points to this list. The bottom status bar indicates 'Finished Creating IoT Layer Succeeded'.

No.	Name	Source	Destination	Services & Applications	Action	Track	Install On
1	Patient Monitoring	Philips IntelliBridge EC10 P...	Philips IntelliVue MX450 P...	* Any	Accept	Log	* Policy Targets
2	MRI	MRI	* Any	* Any	Accept	N/A	* Policy Targets
2.1	PACS	Manufacturer=Philips	Philips Ingenua PACS (ferS...	DICOM Protocol	Accept	Log	* Policy Targets
2.2	Update Service	Manufacturer=Philips	.philips.com	https	Accept	Log	* Policy Targets
Missing cleanup rule - Unmatched traffic will be accepted and not logged.							
3	UltraSound	UltraSound	* Any	* Any	Accept	N/A	* Policy Targets
4	E.C.G.	ECG	* Any	* Any	Accept	Log	* Policy Targets
4.1	PACS	Manufacturer=Belkin Inter...	Belkin International Inc. L...	DICOM Protocol	Accept	Log	* Policy Targets
Missing cleanup rule - Unmatched traffic will be accepted and not logged.							
5	Access to Medical Device	* Any	medical_device	* Any	Accept	Alert	* Policy Targets
6	Medical Device Access	medical_device	* Any	* Any	Accept	Alert	* Policy Targets
Missing cleanup rule - Unmatched traffic will be accepted and not logged.							

IoT Assets

- Belkin International Inc. Ingenua ECG (fer5863971282557)
- Belkin International Inc. Ingenua MRI (fer5863971282566)
- Belkin International Inc. Ingenua MRI (fer5863971282566)
- Belkin International Inc. Ingenua MRI (fer5863971282566)
- Belkin International Inc. Ingenua PACS (fer5863971282566)
- CT
- CYCLONE MICROSYSTEMS, INC. Ingenua MRI (fer586397128255d)
- ECG
- FIBERCOM, INC. Ingenua MRI (fer586397128255f)
- Galaxy Telecom Technologies Ltd Ingenua UltraSound (fer586397128255e)
- Google Ingenua CT (fer586397128255e)
- HUAWEI Ingenua US (fer5863971282555)
- IBM Corp Ingenua Tyto (fer5863971282559)
- INTEGRATED MEASUREMENT SYSTEMS Ingenua MRI (fer586397128255e)
- IQ TECHNOLOGIES, INC. Ingenua MRI (fer586397128255e)
- LECTRA SYSTEMS SA Ingenua MRI (fer5863971282562)
- medical_device
- medical_server
- METAPHOR COMPUTER SYSTEMS Ingenua MRI (fer5863971282563)
- MicroBrain, Inc. Ingenua MRI (fer5863971282560)
- MRI
- PACS
- PANASONIC TECHNOLOGIES, INC. Ingenua MRI (fer586397128255b)
- Philips Ingenua Blood Pressure Monitor (fer5863971282558)
- Philips Ingenua CT (fer5863971282554)

Rule 4 Summary:

- Created by: aa
- Date created: Apr 22, 2019
- Expiration time: Never
- Hit Count: 0 (0%, Zero)

IoT Asset Details:

- Belkin International Inc. Ingenua ECG (fer5863971282557)
- Data Center Name: MedicalDevice
- Data Center Type: M
- Type in Data Center: MedicalDevice
- Updated on Data Center: 22-Apr-19 09:45
- IPs: 34.233.39.94
- Function: ECG
- Manufacturer: Belkin International Inc.
- Location: Building A, Room 5030
- Model: Ingenua
- Last Modified: aa

Защита АСУ ТП с помощью Check Point



Check Point[®]
SOFTWARE TECHNOLOGIES LTD.

Линейка устройств в промышленном исполнении

- Работа в широком диапазоне температур, влажности
- Отсутствие движущихся частей
- Соответствие международным стандартам IEC 61850-3 и IEEE 1613



IAS U1



1570R



RuggedCom/Siemens



IAS T1

Монтаж на Din-рейку

*Средняя
производительность
Монтаж в стойку*

*Высокая
производительность
Монтаж в стойку*

1570 Rugged

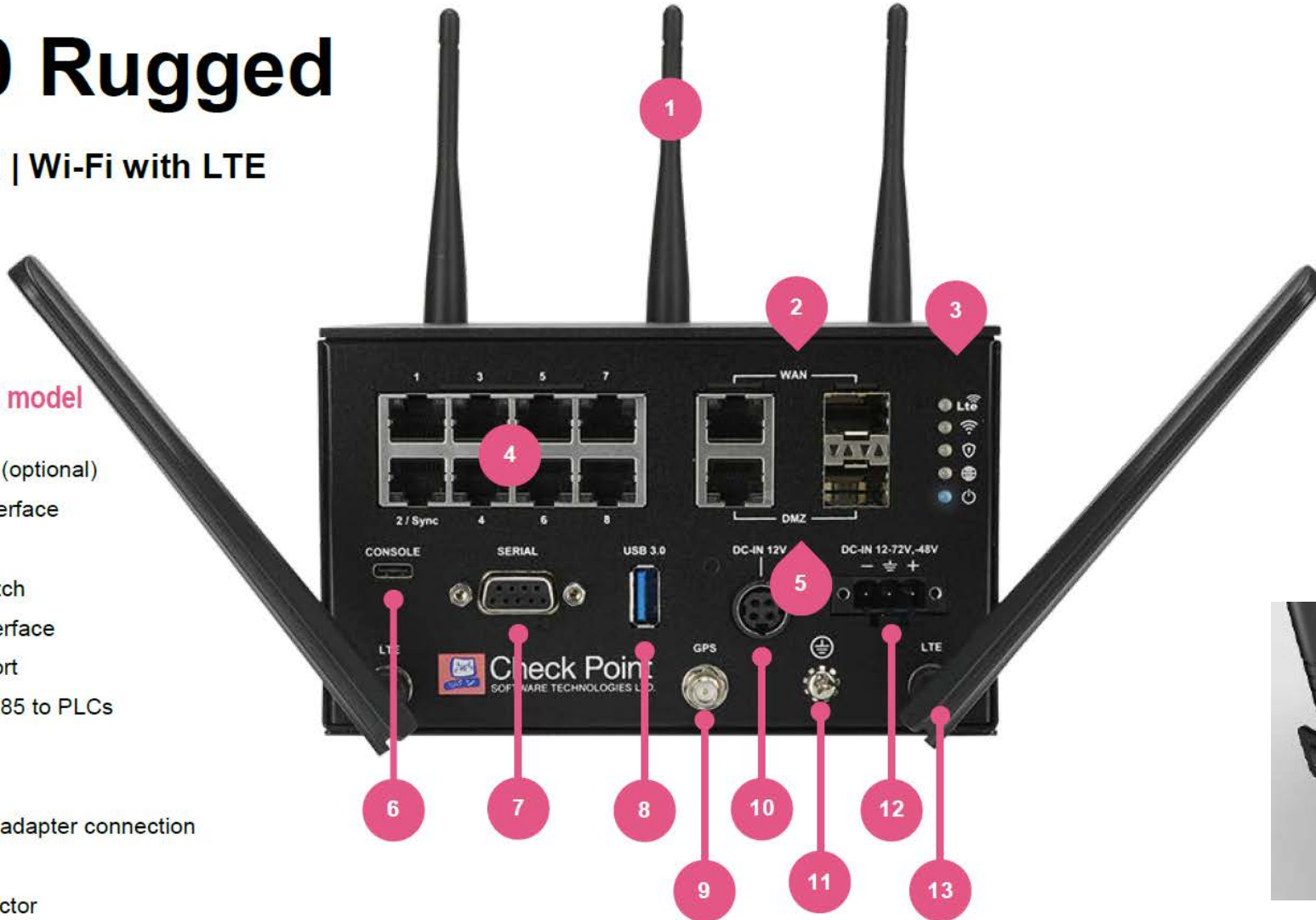
Wired | Wi-Fi with LTE



Check Point
SOFTWARE TECHNOLOGIES LTD.

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

Линейка устройств Check Point



Для защиты предприятий
любых масштабов

44000 и 64000
23000 линейка
(3 модели)



15000 Appliances
(2 модели)



Крупный офис

Защита ЦОД
Защита сервис
провайдеров

5000 Appliances
(4 модели)



Средний офис

3200 Appliance
1400 Appliances
(4 модели)



Малый офис



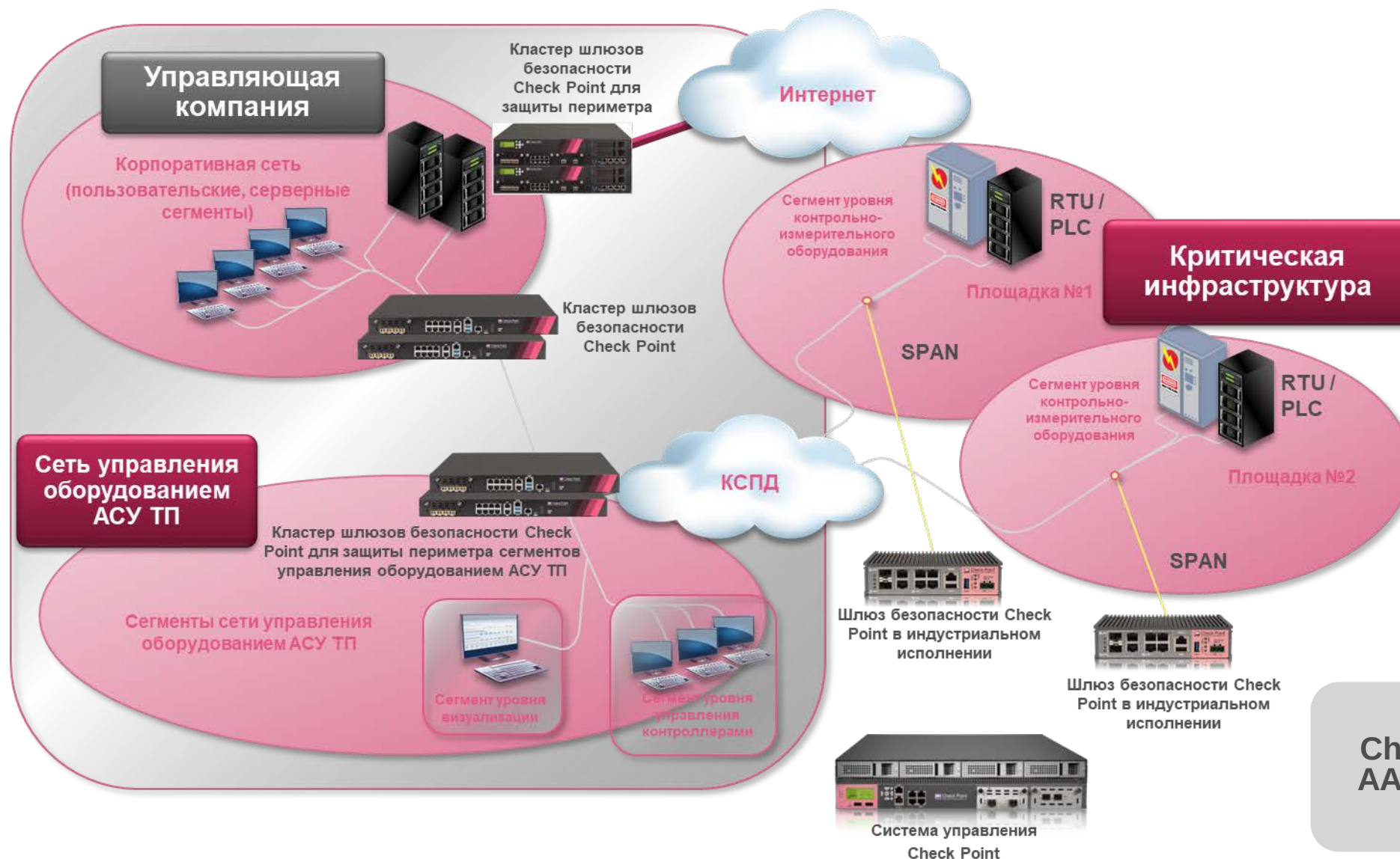
softwareblades™

[Restricted] ONLY for designated groups and individuals

Архитектура промышленной сети



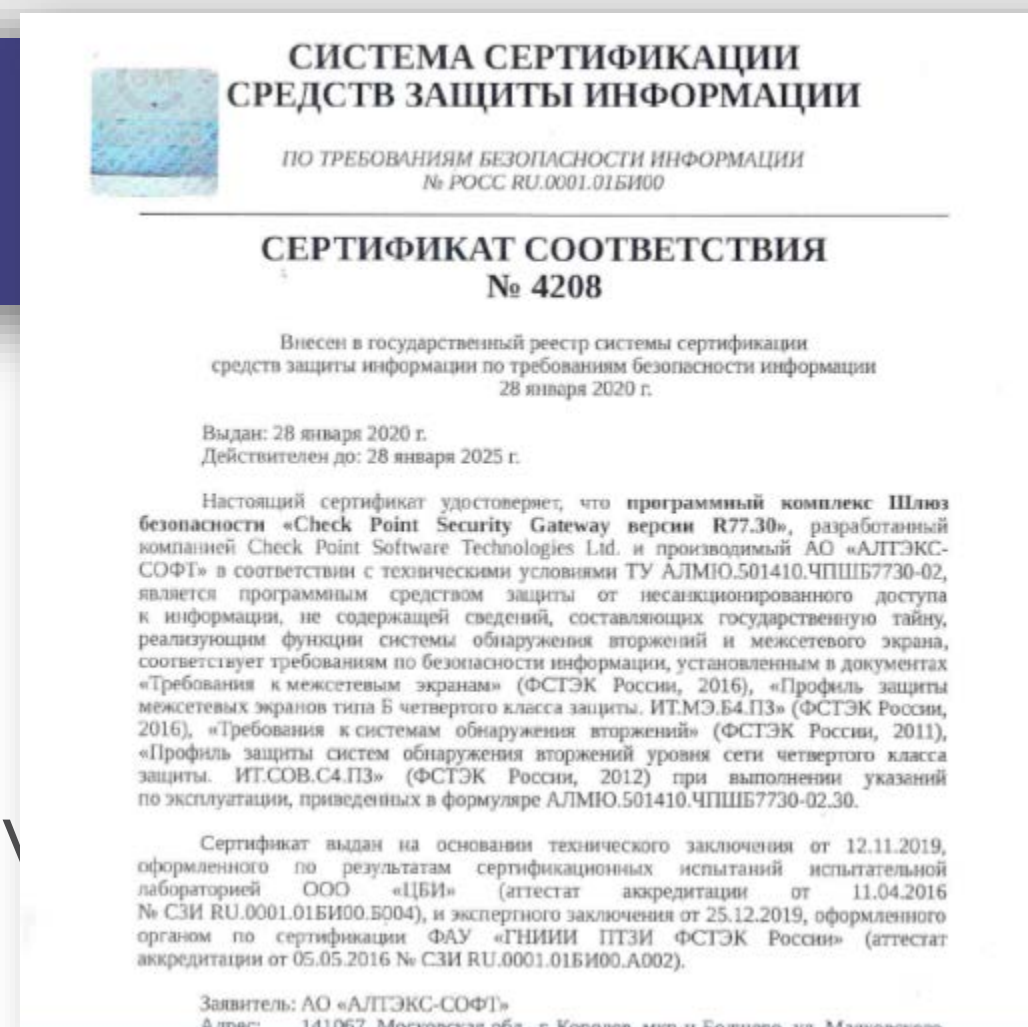
Check Point
SOFTWARE TECHNOLOGIES LTD.



Государственный реестр сертифицированных средств защиты информации



Check Point
SOFTWARE TECHNOLOGIES LTD.



Меры по обеспечению безопасности (I)



Приказ ФСТЭК N239. Приложение. Состав мер по обеспечению безопасности ЗНО КИИ

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	+	+	+
АУД.4	Регистрация событий безопасности	+	+	+
АУД.5	Контроль и анализ сетевого трафика			+
АУД.7	Мониторинг безопасности	+	+	+
СОВ.1	Обнаружение и предотвращение компьютерных атак		+	+

Меры по обеспечению безопасности (II)



Приказ ФСТЭК N239. Приложение XI. Защита информационной системы и ее компонентов

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)				
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+	+	+
ЗИС.2	Защита периметра информационной (автоматизированной) системы	+	+	+
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	+	+	+
ЗИС.4	Сегментирование информационной (автоматизированной) системы		+	+
ЗИС.5	Организация демилитаризованной зоны	+	+	+
ЗИС.6	Управление сетевыми потоками			
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения ("песочница")			

Меры по обеспечению безопасности (III)



Приказ ФСТЭК N239. Приложение XI. Защита информационной системы и ее компонентов

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)				
ЗИС.8	Соккрытие архитектуры и конфигурации информационной (автоматизированной) системы	+	+	+
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию			
ЗИС.19	Защита информации при ее передаче по каналам связи	+	+	+
ЗИС.20	Обеспечение доверенных канала, маршрута	+	+	+
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+	+	+

Меры по обеспечению безопасности (IV)



Приказ ФСТЭК N239. Приложение XI. Защита информационной системы и ее компонентов

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)				
ЗИС.23	Контроль использования мобильного кода		+	+
ЗИС.24	Контроль передачи речевой информации		+	+
ЗИС.25	Контроль передачи видеоинформации		+	+
ЗИС.27	Обеспечение подлинности сетевых соединений		+	+
ЗИС.32	Защита беспроводных соединений	+	+	+
ЗИС.33	Исключение доступа через общие ресурсы			+
ЗИС.34	Защита от угроз отказа в обслуживании (DoS, DDoS-атак)	+	+	+

Защита критических инфраструктур

Журналирование всей сетевой активности компонентов КИИ

Профилирование сетевой активности компонентов КИИ

Идентификация отклонений и атак на компоненты КИИ

Обнаружение / предотвращение атак на компоненты КИИ



Check Point®
SOFTWARE TECHNOLOGIES LTD.

СПАСИБО!

Дмитрий Кудра | Check Point Russia
dkudra@checkpoint.com

A large white arrow pointing right, with the text 'ONE STEP AHEAD' in white. The arrow is set against a dark background that includes a silhouette of a palm tree on the right side.

ONE STEP AHEAD