Check Point
SOFTWARE TECHNOLOGIES LTD

РЕШЕНИЯ ПО БЕЗОПАСНОСТИ CHECK POINT

Дмитрий Кудра
Консультант по безопасности
dkudra@checkpoint.com

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION

CHECK POINT INFINITY

CLOUD

Infrastructure
CloudGuard IaaS

- Advanced Threat Prevention
- Adaptive Security
- Automation and Orchestration
- Cross Environment Dynamic Policies

Applications
CloudGuard SaaS

- Zero-Day Threat Protection
- Sensitive Data Protection
- End-to-end SaaS Security
- Identity Protection

Multi & Hybrid Cloud

NETWORK

SandBlast NETWORK

Headquarters

- Access Control
- Data Protection
- Multi Layered Security
- Advanced Threat Prevention

Branch

- Access Control
- Multi Layered Security
- Advanced Threat Prevention
- Wi-Fi, DSL, PPoE Ready

Shared Threat Intelligence

THREATCLOUD

R80

Consolidated Security Management

MOBILE

SandBlast MOBILE

- App Protection
- Network Protection
- Device Protection

Capsule WorkSpace/Docs

- Remote Access
- Secure Business Data
- Protect Docs Everywhere

ENDPOINT

SandBlast AGENT

- Threat Prevention
- Anti-Ransomware
- Forensics

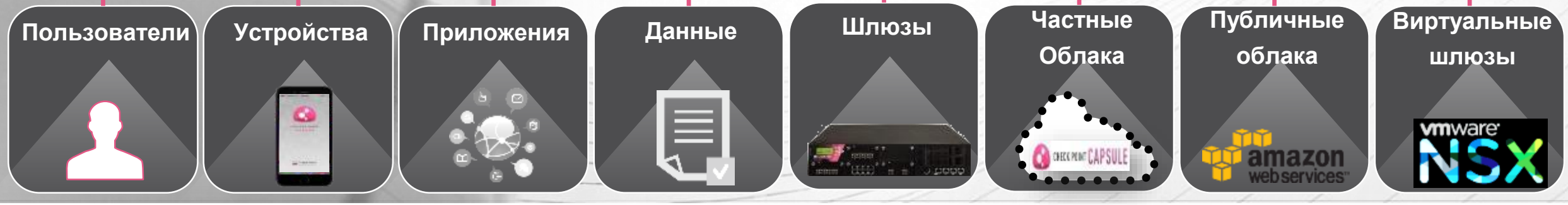
Access/Data Security

- Access Control
- Secure Media
- Secure Documents

Единая Политика Управления

Check Point
SOFTWARE TECHNOLOGIES LTD.

Name	Source	Destination	Services & Applications	Data	Action	Install On
Outbound access	production_net	Internet	Any	Any	AccessSubLayer	Policy Targets
Social media for marketing	marketing_role John	Internet	Twitter LinkedIn Instagram	Any	Accept	SG13800
Developers upload	developer_role	Internet	Dropbox Box	Any Direction Source Code - JAVA	Accept	SG13800 CapsuleCloud
Access Sensitive Servers	Any	Any	Any	Any	SensitiveServers	Policy Targets
Mobile Access	Mobile Devices	MailUS	MailServer	Any	Accept	Mobile
Access to Web Server	Any	WebServer	https	Any	Accept	AWS VMWare



Контроль приложений и URL-фильтрация

Check Point
SOFTWARE TECHNOLOGIES LTD.

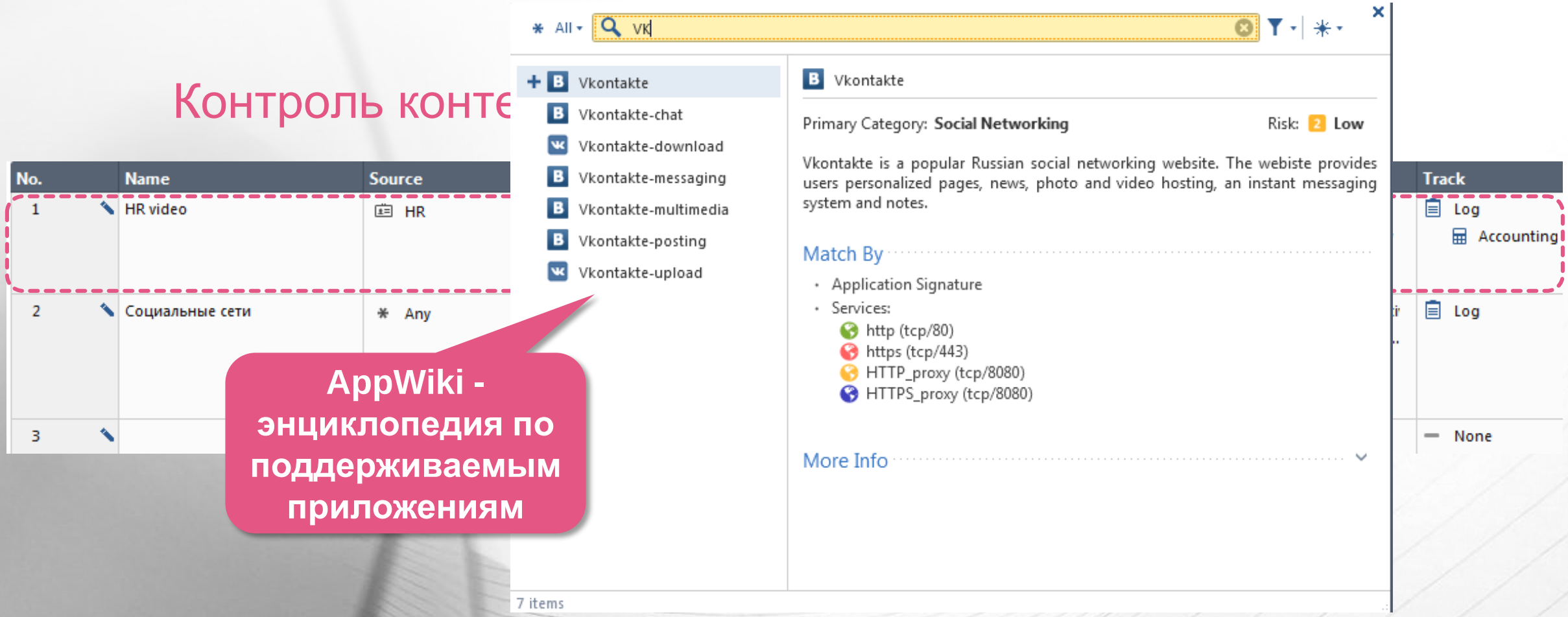
Контролируйте весь трафик из производственной сети в Интернет

No.	Name	Source	Destination	Services & Applications	Data	Action	Install On
1	Outbound access	production_net	Internet	Any	Any	AccessSubLayer	Policy Targets
1.1	Social media for marketing	marketing_role John	Internet	Twitter LinkedIn Instagram	Any	Accept	SG13800
1.2	Developers upload	developer_role	Internet	Dropbox Box	Any Direction Source Code - JAVA	Accept	SG13800
1.3	Cleanup rule	Any	Any	Any	Any	Drop	SG13800

Гранулированность и контроль политики

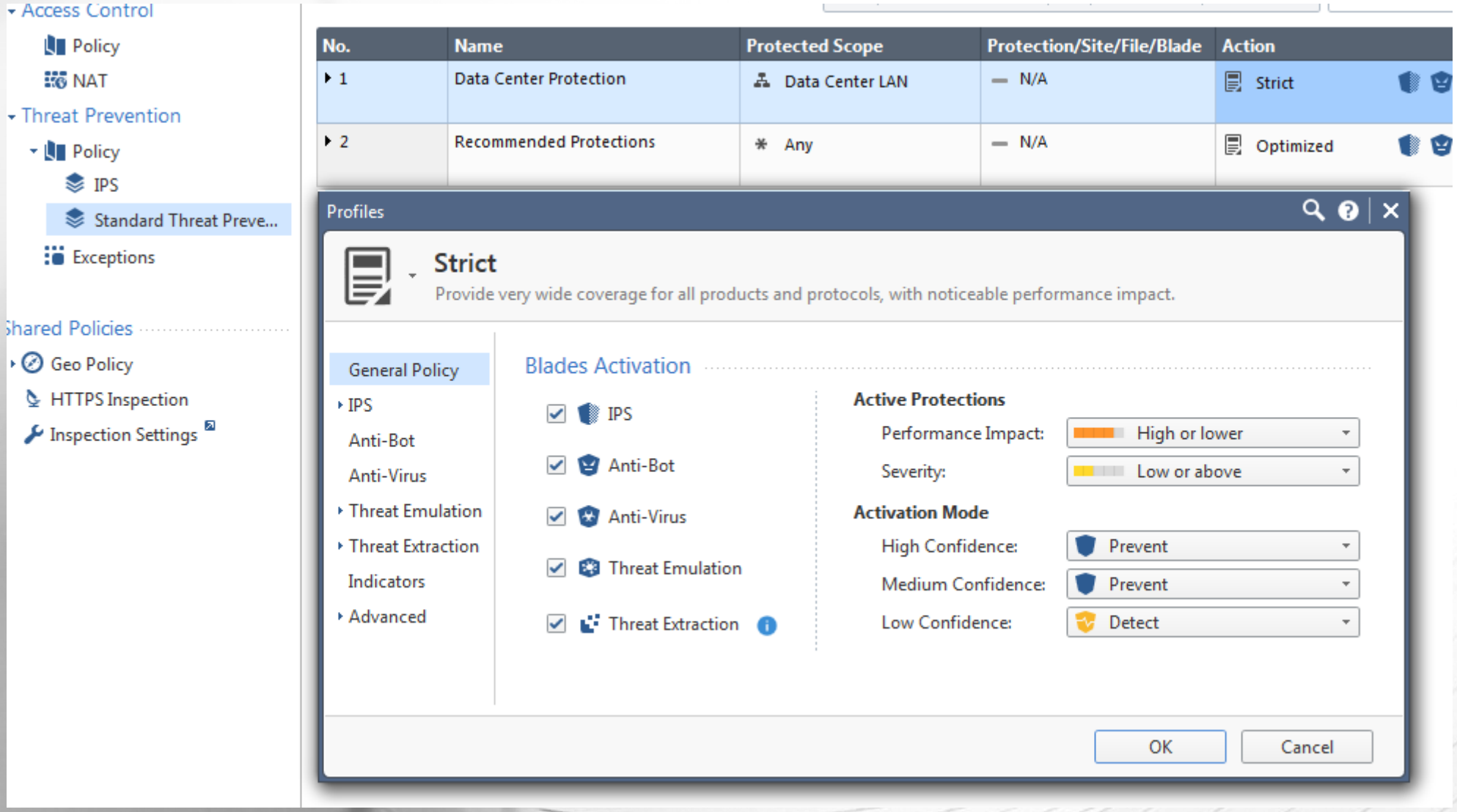
Check Point
SOFTWARE TECHNOLOGIES LTD.

Контроль конте



AppWiki - энциклопедия по поддерживаемым приложениям

Threat Prevention



IPS

Protection	Industry Refere...	Releas...	Update...	Performance Im...	Severity	Confidence Le...	Optimized	Strict
3Com Network Supervisor Directory Tra...	CVE-2005-2020	24/11/2009	24/11/2009					
3Com TFTP Server Transporting Mode R...	CVE-2006-6183	15/01/2007	15/11/2011					
3CX Phone System VAD_Deploy.aspx Ar...	None	25/12/2016	29/12/2016					
3ivx MPEG-4 MP4 File Handling Stack O...	CVE-2007-6401	01/10/2009	20/10/2013					
3ivx MPEG-4 MP4 File Handling Stack O...	CVE-2007-6401	01/10/2009	11/02/2013					
3S Smart Software Solutions CoDeSys G...	CVE-2012-4707	19/05/2013	22/05/2013					
3S Smart Software Solutions CoDeSys G...	CVE-2012-4705	05/05/2013	06/10/2015					
3S Smart Software Solutions CoDeSys G...	CVE-2012-4706	05/05/2013	07/05/2013					
3S Smart Software Solutions CoDeSys G...	CVE-2012-4704	05/05/2013	07/05/2013					
3S Smart Software Solutions CoDeSys G...	CVE-2012-4708	05/05/2013	06/10/2015					
7-Zip ARJ Archive Handling Buffer Overf...	CVE-2005-3051	12/10/2009	12/10/2009					
7T Interactive Graphical SCADA RMS Re...	None	23/04/2013	02/05/2013					
7T Interactive Graphical SCADA System (I...	CVE-2011-1565	23/08/2011	23/08/2011					
7T Interactive Graphical SCADA System...	CVE-2011-1566	23/08/2011	23/08/2011					
7T Interactive Graphical SCADA System F...	CVE-2011-1567 CVE-201	15/05/2011	22/10/2014					
ABB MicroSCADA Wserver Command Ex...	None	19/12/2013	31/12/2013					
ABB MicroSCADA Wserver Multiple Buff...	None	31/12/2013	31/12/2013					
ABB Multiple Products RobNetScanHos...	CVE-2012-0245	02/07/2012	02/12/2013					
ABB Test Signal Viewer CWGraph3D Act...	CVE-2013-5022	03/12/2013	23/02/2016					

Details | Logs

3Com Network Supervisor Directory Traversal

Performance Impact: Low | Severity: High | Confidence Level: Medium

Attack ID: CPAI-2005-288

Last Update: **24-November-2009**

Threat Description:

The 3Com Network Supervisor is a network management application that discovers, maps, and displays network links and IP devices. It monitors devices and connections for stress levels, set thresholds and various network events. The product is also capable of generating reports in various formats. A directory traversal vulnerability exists in the 3Com Network Supervisor product. The flaw is caused by insufficient sanitization of HTTP requests. This vulnerability allows an unauthorized user to read arbitrary files on the target host. The target will not exhibit any unusual behaviour as a result of this

Check Point SOFTWARE TECHNOLOGIES LTD.

NSS Labs RECOMMEND

NGIPS Recommended – Ноябрь 2017

99.52% Exploit Block Rate Score! 5th IPS Recommended, 16th since 2011.

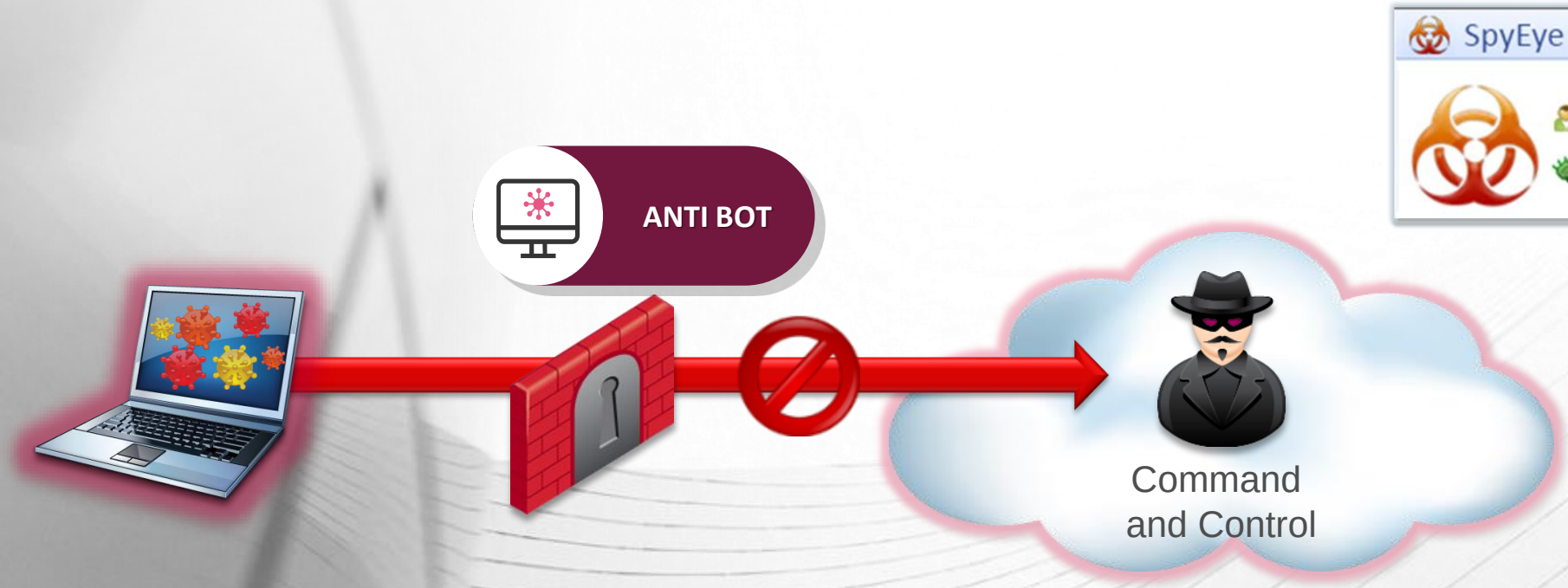
Anti-Bot

Check Point
SOFTWARE TECHNOLOGIES LTD.

Находит зараженные машины

Обезвреживает зараженные машины

Интегрированная система



SANDBLAST
THREAT EMULATION

- **Устойчивая** к попыткам обхода песочница
- **Блокирует** неизвестное вредоносное ПО и атаки нулевого дня

ОБНАРУЖЕНИЕ УГРОЗ

Бескомпромиссное обнаружение угроз

УСТОЙЧИВАЯ К ОБХОДАМ

Устойчивая к обходам песочница*

БЫСТРАЯ И ЭФФЕКТИВНАЯ

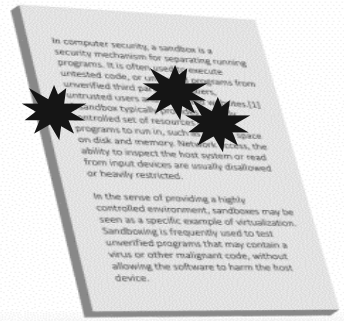
Вердикт выносится менее чем за три минуты

*Источник: 2016 NSS Labs Breach Detection Systems Test Report

ТРАДИЦИОННАЯ ПЕСОЧНИЦА

Check Point
SOFTWARE TECHNOLOGIES LTD.

Эмуляция файлов в виртуальной среде

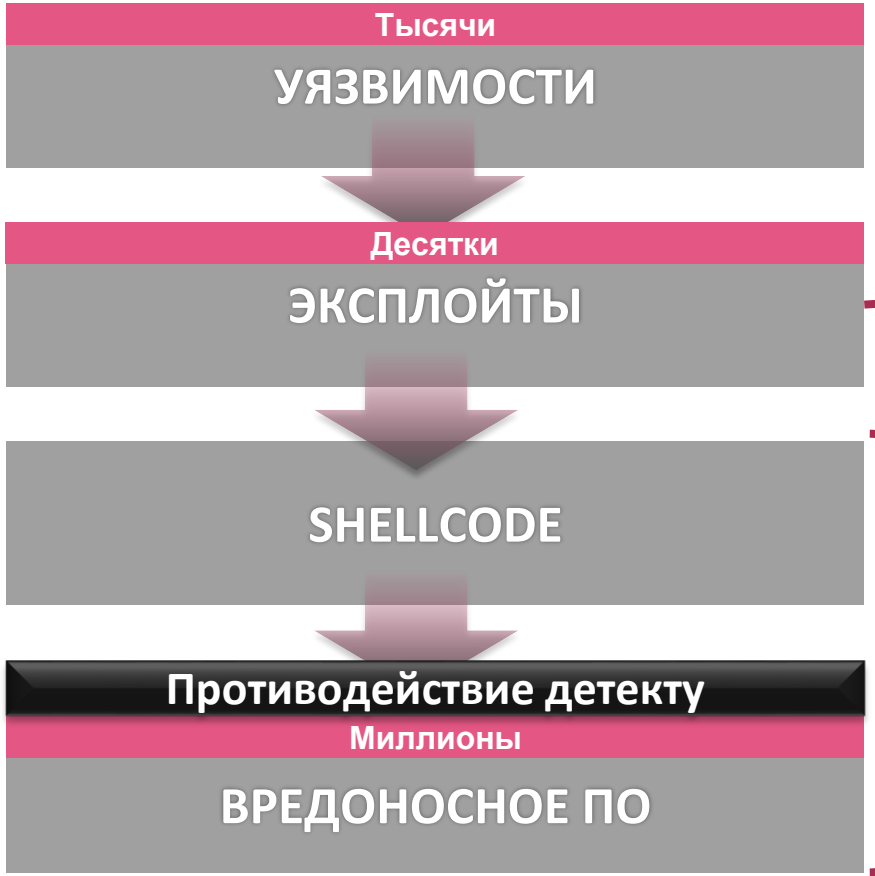


Мониторинг:

- Системный реестр
- Сетевые соединения
- Файловая активность
- Системные процессы

Поиск признаков заражения на уровне операционной системы

ЕДИНСТВЕННАЯ песочница с обнаружением на уровне процессора **(CPU-LEVEL DETECTION)**



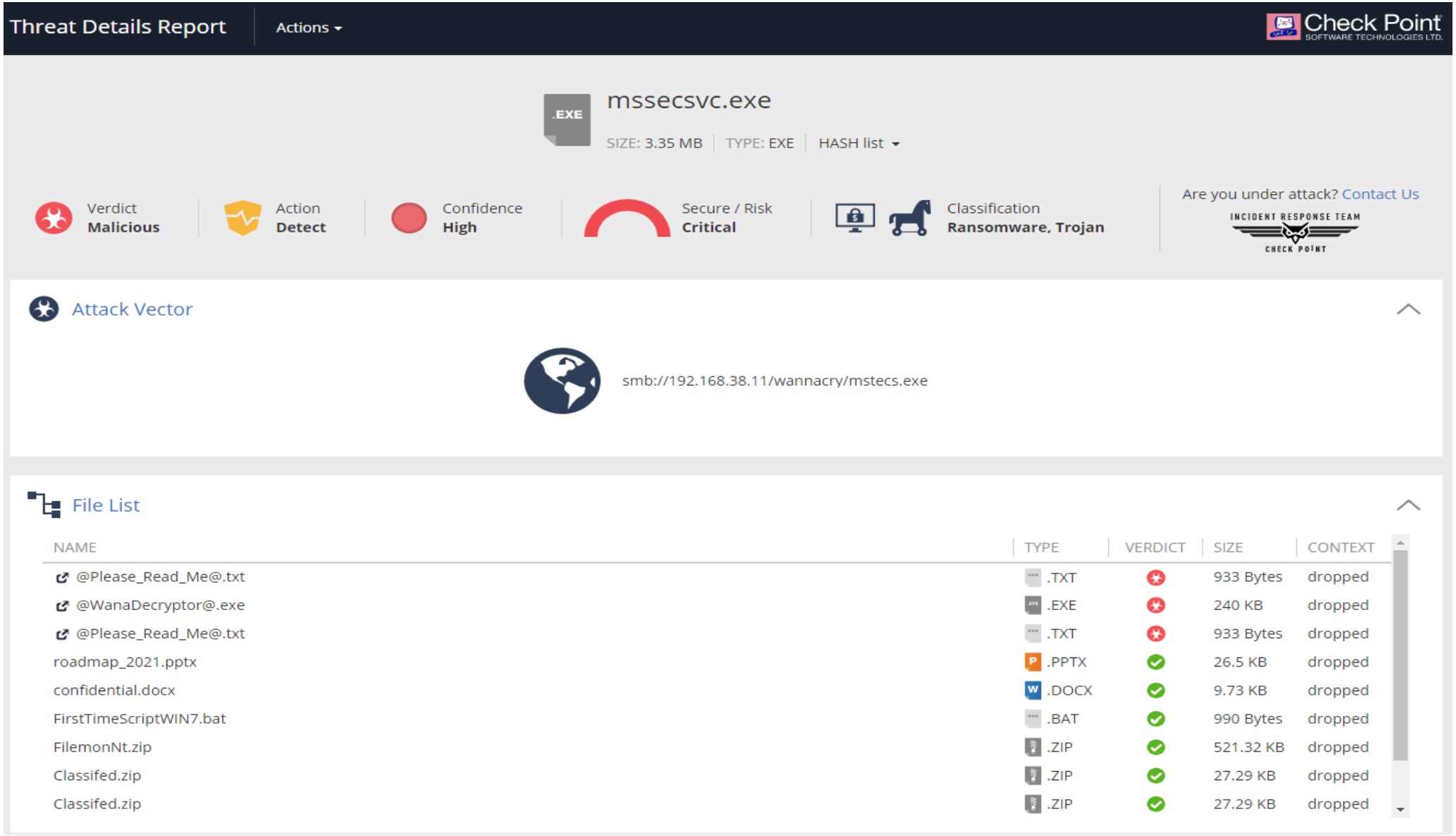
Check Point SandBlast

- Обнаружение на уровне CPU
- **УСТОЙЧИВ К ОБХОДУ**

Традиционные песочницы

- Поведенческое обнаружение
- **Можно обойти защиту**

Отчет работы Threat Emulation



Отчет работы Threat Emulation

Check Point
SOFTWARE TECHNOLOGIES LTD.

Suspicious Activities

Win7, Office 2013, Adobe 11 | WinXP, Office 2003/7, Adobe 9

CATEGORY	COUNT	DESCRIPTION
Data Loss	2	This technique is used by steal browsing information.
Evasion	1	This technique is used by malware to check if its being analyzed or to evade Anti-Virus software.
Evasion	1	This technique is used by malware to check if its being analyzed.
Evasion	2	This technique is used by malware to decrypt some of it's internal parts during runtime and avoid detection.
File system event	74	Suspicious file was accessed during emulation
Generic	1	This technique is indicative of malware, as legitimate applications rarely create new executable files.
Generic	1	This technique is indicative of malware. Legitimate applications rarely use this technique.
Persistance	1	This technique keeps the malware running after the PC reboots.
Process event	5	Suspicious process was launched during emulation
Registry event	6	Suspicious registry path was accessed during emulation
Reputation	4	Well-known malware
Spyware	2	This technique is used by malware to monitor all network connection on a system, and steal information from the traffic.
Stealth	1	This technique is used by malware to hide traces of infection.

Отчет работы Threat Emulation

Check Point
SOFTWARE TECHNOLOGIES LTD.

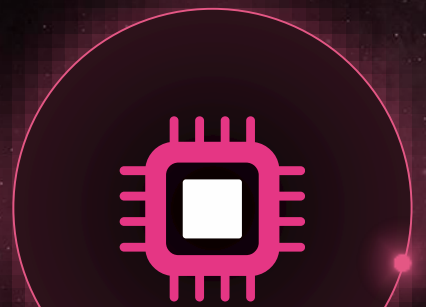
Emulation Videos

Win7, Office 2013, Adobe 11

WinXP, Office 2003/7, Adobe 9

THREAT EMULATION

Устойчивая к обходу песочница



И ЕЩЕ ДЕСЯТКИ ТЕХНОЛОГИЙ …

CPU-LEVEL

Human Interaction Simulator

Network Activity Monitor

UAC Monitor

DeepScan

SMEP Detector

FP Guard

Virtual Network Service

PUSH-FORWARD

Icon Similarity

Image Sanitation

Dropped File Emulation

Decoys

DGA Generator

Static Analyzer

Evasion Detection

Macro Analysis

Link Scanner

Shellcode Detector

Менее двух минут

среднее время анализа

SANDBLAST
THREAT EXTRACTION

- Доставка очищенных файлов в режиме реального времени
- Оригинальные файлы в это время проходят эмуляцию

ПРОАКТИВНАЯ ЗАЩИТА

Доставка очищенных файлов

ОТЛИЧНАЯ БЕЗОПАСНОСТЬ

Удаление опасного содержимого

БЫСТРАЯ ДОСТАВКА

Доставка данных за секунды

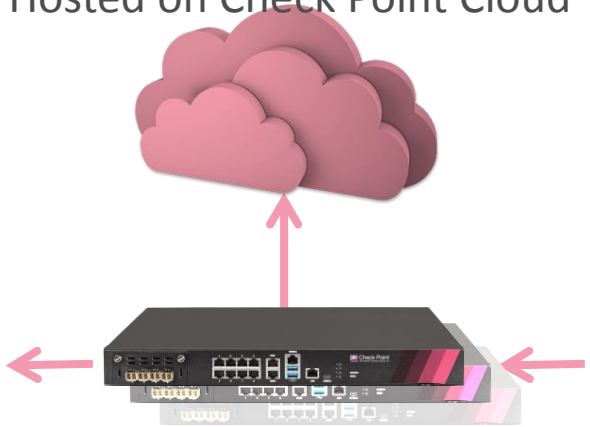
Различные варианты внедрения

Для средств защиты периметра сети

Check Point
SOFTWARE TECHNOLOGIES LTD.

CLOUD SERVICE
Gateways + SandBlast Service

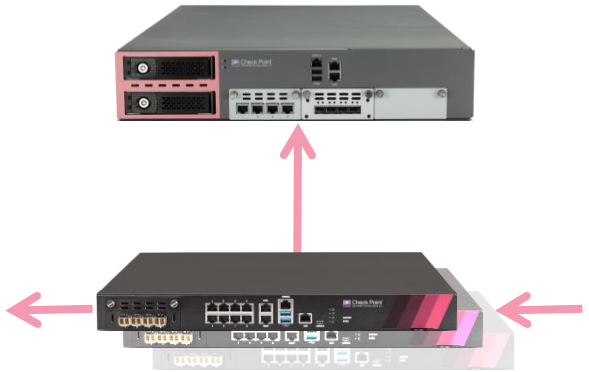
SandBlast Service
Hosted on Check Point Cloud



NGTX Security Gateways

ON-PREM SERVICE
Gateways + SandBlast TE Appliance

SandBlast TE Appliance



NGTX Security Gateways

DEDICATED APPLIANCE
Inline SandBlast TE Appliance

SandBlast TE Appliance

- **LEVERAGE SECURITY GATEWAYS** – Масштабируемое решение

Варианты установки шлюзов и песочниц:

- Inline / SPAN / TAP
- MTA – защита почтового трафика
- ICAP server – интеграция со сторонними решениями

Программно-аппаратные комплексы

18

Линейка устройств Check Point

Для защиты предприятий любых масштабов

3200 Appliance
1400 Appliances
(4 модели)

Малый офис

5000 Appliances
(4 модели)

Средний офис

15000 Appliances
(2 модели)

Крупный офис

44000 и **64000**
23000 линейка
(3 модели)

Защита ЦОД

Защита сервис провайдеров

Лучшая производительность

Point
NOLOGIES LTD.

Высокая эффективность

Масштабируемость

Отказоустойчивость

Check Point 44000 и 64000

Представляем новую линейку Check Point Smart-1 Appliance

Security Management

Пять новых устройств

Централизованный менеджмент до 5000 шлюзов*

Smart-1 5150

Для 150 шлюзов и больше

Smart-1 5050

Для 50 шлюзов

Smart-1 525

Для 25 шлюзов

Smart-1 410

Для 10 шлюзов

Smart-1 405

Для 5 шлюзов

* 5000 Check Point 1400 gateways

Защита АСУ ТП с помощью Check Point

Check Point
SOFTWARE TECHNOLOGIES LTD.

Линейка устройств в индустриальном исполнении

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

IAS U1

RuggedCom/Siemens

IAS T1

1200R

Монтаж на Din-рейку

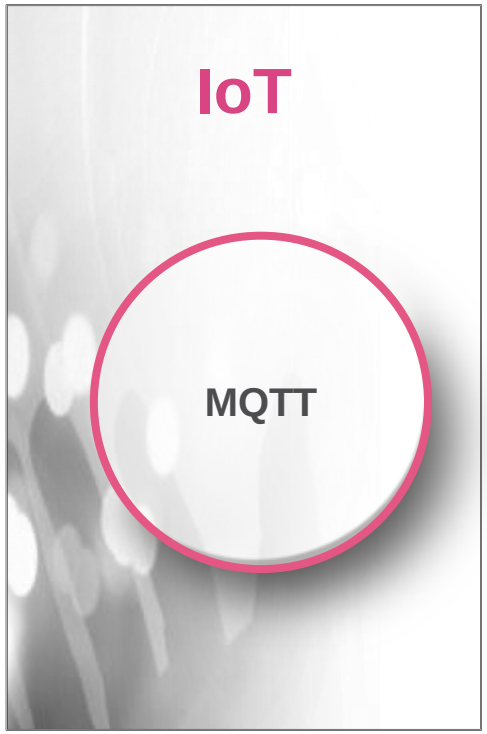
Средняя производительность

Монтаж в стойку

Высокая производитель ность

Монтаж в стойку

Поддержка специализированных протоколов



MMS
CIP
BACNET
Profinet
IEC 60870-5-104
OPC
DA & UA
ICCP
MODBUS
IEC 61850
DNP3
Siemens
Step7

… и другие

Более 1000 SCADA и IoT команд в Check Point Application Control

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

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
2013-11-06: 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 300 специализированных IDS/IPS сигнатур

Check Point
SOFTWARE TECHNOLOGIES LTD.

Защита от уязвимостей
и обнаружение
аномального трафика

CHECK POINT
IPS

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

NSS Labs
RECOMMEND

NSS Labs
Highest Rating

Детальное журналирование трафика

Check Point
SOFTWARE TECHNOLOGIES LTD.

Детальная информация для расследования инцидентов

CHECK POINT
SMARTLOG & SMARTEVENT

ПОДРОБНО

Time		B...	A...	T...	Origin	Application...	Transa...	Fu...	Function Description	Source	Desti...	...	Matc...
Today	10:45:35				gw-71ec22	ModbusAll	33394	3	Read Holding Registers	HMI-1	PLC-1		SCADA Pr...
Today	10:45:53				gw-71ec22	ModbusAll	33490	4	Read Input Registers - Response	HMI-1	PLC-1		SCADA Pro...
Today	10:45:53				gw-71ec22	ModbusAll	33490	4	Read Input Registers	HMI-1	PLC-1		SCADA Prot...
Today	10:45:53				gw-71ec22	ModbusAll	33489	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot...
Today	10:45:53				gw-71ec22	ModbusAll	33489	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot...
Today	10:45:53				gw-71ec22	ModbusAll	33488	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot...
Today	10:45:53				gw-71ec22	ModbusAll	33488	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot...
Today	10:45:53				gw-71ec22	ModbusAll	33487	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot...
Today	10:45:53				gw-71ec22	ModbusAll	33487	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot...
Today	10:45:53				gw-71ec22	ModbusAll	33486	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot...
Today	10:45:53				gw-71ec22	ModbusAll	33486	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot...
Today	10:45:53				gw-71ec22	ModbusAll	33485	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot...
Today	10:45:53				gw-71ec22	ModbusAll	33485	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot...
Today	10:45:51				gw-71ec22	ModbusAll	33484	4	Read Input Registers - Response	HMI-1	PLC-1		SCADA Prot...
Today	10:45:51				gw-71ec22	ModbusAll	33484	4	Read Input Registers	HMI-1	PLC-1		SCADA Prot...
Today	10:45:51				gw-71ec22	ModbusAll	33483	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot...
Today	10:45:51				gw-71ec22	ModbusAll	33483	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot...
Today	10:45:51				gw-71ec22	ModbusAll	33482	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot...
Today	10:45:51				gw-71ec22	ModbusAll	33482	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot...
Today	10:45:51				gw-71ec22	ModbusAll	33481	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot...
Today	10:45:51				gw-71ec22	ModbusAll	33481	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot...
Today	10:45:51				gw-71ec22	ModbusAll	33480	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot...

СГРУППИРОВАНО

Count	Source	Destination	Unit ID	Function Description
500	**HMI (10.1.1.5)**	**PLC (20.1.1.5)**	**1**	**Read Holding Registers**
100	**HMI (10.1.1.5)**	**PLC (20.1.1.5)**	**1**	**Read Input Registers**
1	HMI (10.1.1.5)	PLC (20.1.1.5)	1	Write Single Register

Мониторинг промышленной сети

Check Point
SOFTWARE TECHNOLOGIES LTD.

Информация о взаимодействии

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

Информация об устройствах

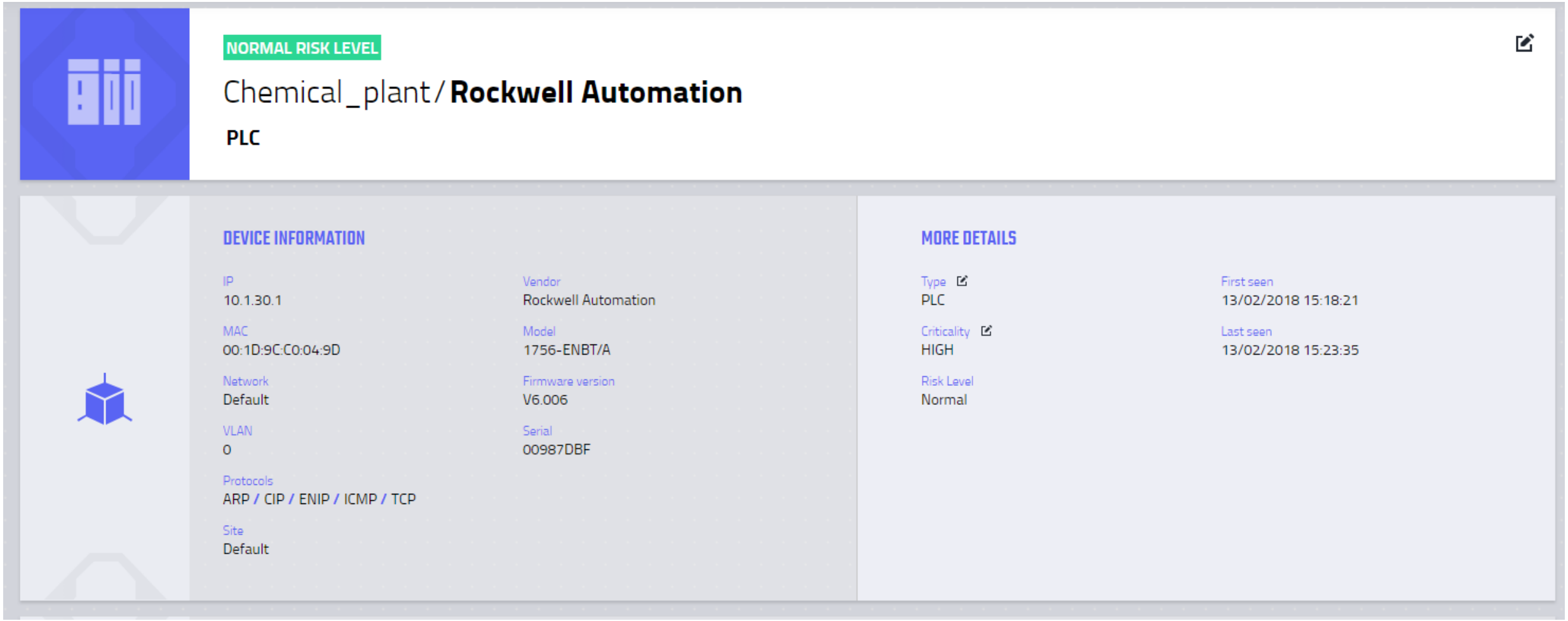
- IP- и MAC-адреса
- Производитель устройства
- Тип устройства (PLC, HMI, рабочая станция, коммутатор, итд)
- Модель и серийный номер
- Версия прошивки

Информация о сети

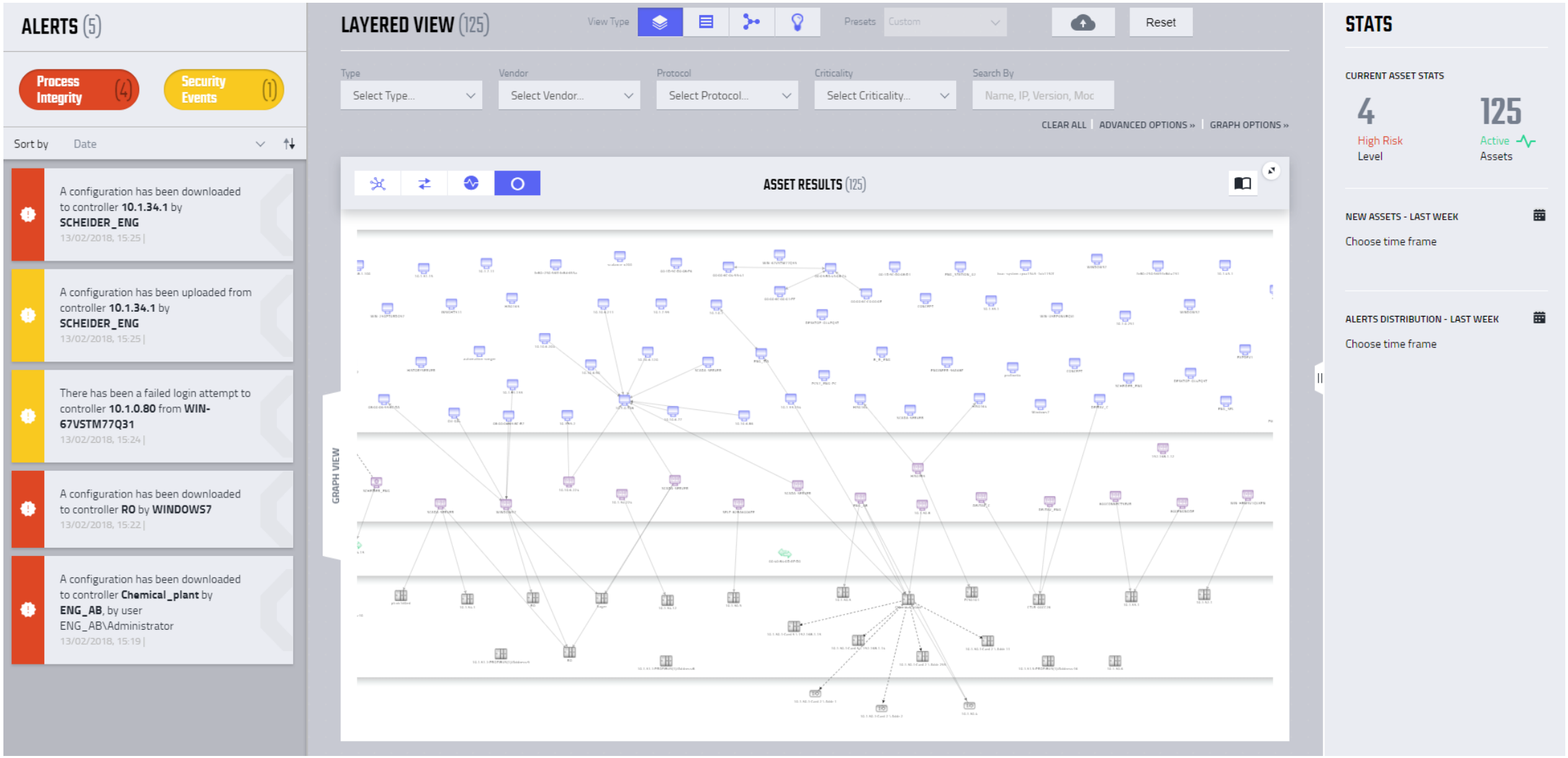
- Какие устройства работают в вашей сети?
- Каким образом эти устройства взаимодействуют между собой и внешним миром?
- Существуют ли ошибки конфигурации и уязвимости?

Информация об устройстве

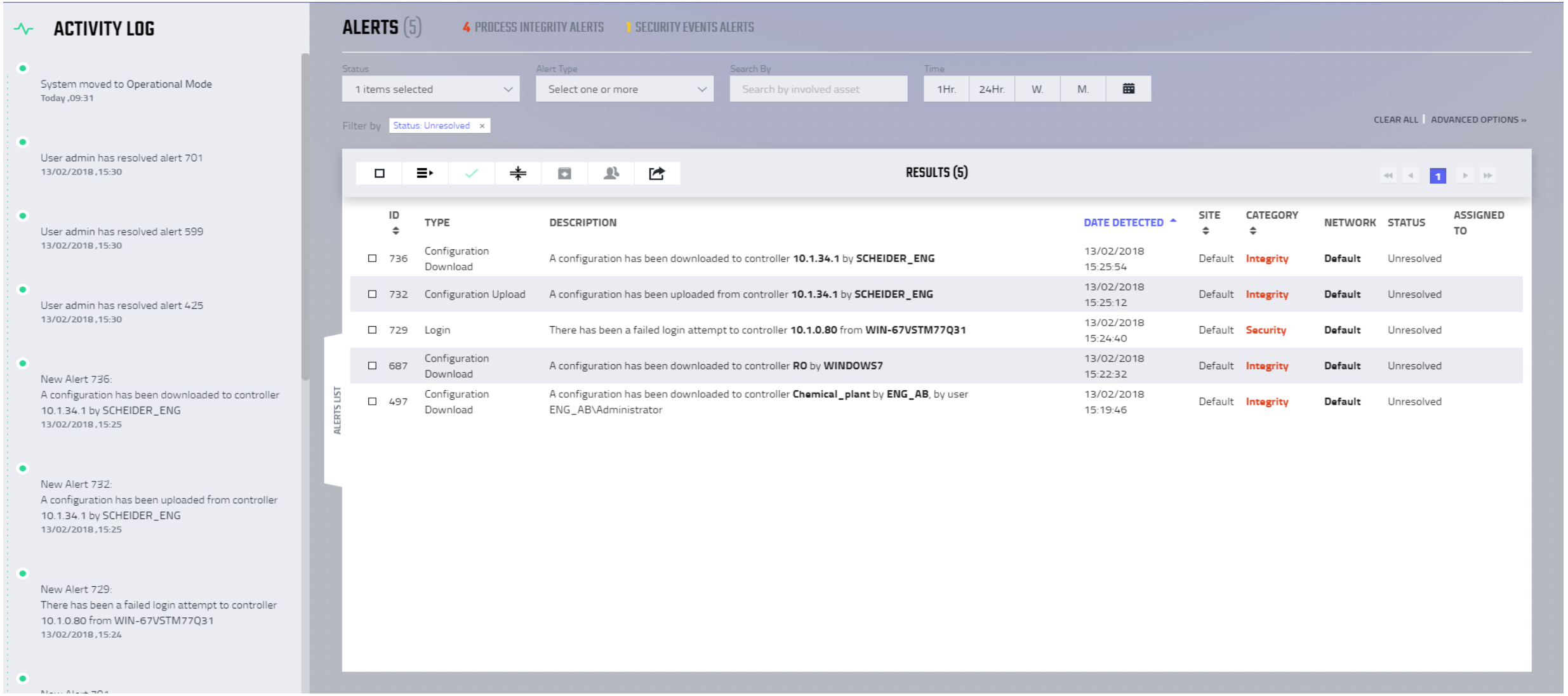
Детальная информация об устройстве – тип, производитель, версия прошивки и прочее



Информация об устройстве – иерархическая карта



Оповещения на базе поведенческого анализа



Комбинированная защита

Check Point
SOFTWARE TECHNOLOGIES LTD.

Настраиваемые политики

- **Фаза обучения** – анализ сетевого трафика и логов
- Ручная конфигурация нормального режима работы
- Специализированные политики для команд и значений
- Политики на основе временны*х* шаблонов трафика

Обнаружение аномалий

- **Фаза обучения** – автоматическое обнаружение устройств
- Поведенческий анализ на основе обнаружения аномалий
- Создание базисного профиля производственного процесса

Комбинированная защита на основе настраиваемых политик и обнаружения аномалий

Защита критических инфраструктур

Check Point
SOFTWARE TECHNOLOGIES LTD.

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!