R80.10

ЗАЩИТА ПРОМЫШЛЕННЫХ СЕТЕЙ

ONE STEP AHEAD

Степан Ульянов
CCSE CheckPoint MONT

Факты и реальность

Check Point
SOFTWARE TECHNOLOGIES LTD.

Декабрь 2014	Металлургический завод в Германии был взломан с помощью фишинговой атаки – Массивные повреждения на заводе
Декабрь 2015	Взлом энергетическая компании Украины «Прикарпатьеоблэнерго» благодаря вредоносной атаке BlackEnergy Spear Phishing (19 Января – повтор на подстанции Пивничнath)
Март 2016	Хакеры взломали систему управления очистки водных ресурсови поменяли уровень химических элементов, которые использовались для обработки водопроводной воды (Kemuri Water Company)
Май 2017	Массовое распространение WannaCry пострадало 500 тысяч компьютеров, принадлежащих частным лицам, коммерческим и правительственным организациям, в более чем 200 странах мира

ICS-CERT Итоги: постоянное увеличение Атак на Критическую Инфраструктуру США

Взломы ИБ

20%

увеличение

Наиболее Атакованные Секторы

Производство, затем Энергетика

Наиболее распространенный метод атаки

Фишинг

ICS-CERT: Эти атаки были возможны благодаря архитектурным просчетом построения сетей ICS

Почему эти атаки возможны?

Устаревшие и необновленные системы

Ошибки в сегментации, подключение технологических сетей к Интернету

Задержки в обслуживании критических систем препятствуют адекватной защите

Векторы Атак на корпоративные сети

Внешние накопители

Почтовый Фишинг и Вложения

Удаленная поддержка

Уязвимости в ПО

Гостевые Сети
Незащищенные Розетки

Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT'S

Решения безопасности для АСУ ТП (Industrial control Systems)

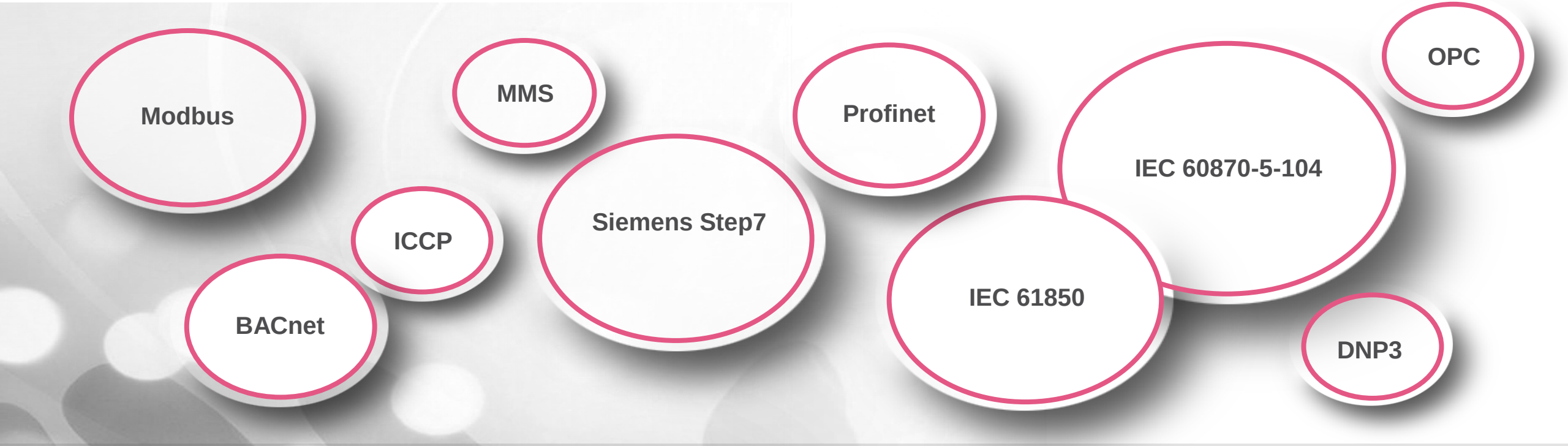
КИБЕР ЗАЩИТА

Обзор и детальный контроль SCADA трафика

Специализированная защита от SCADA угроз

Надежные устройства для агрессивной среды

Обширная поддержка SCADA/ICS-специализированных протоколов



Свыше 720 АСУ ТП команд в Check Point Application Control

Детальное протоколирование SCADA трафика

Детальная форензика для расследования инцидентов

АНАЛИЗ
с помощью
Check Point
SMARTLOG & SMARTEVENT

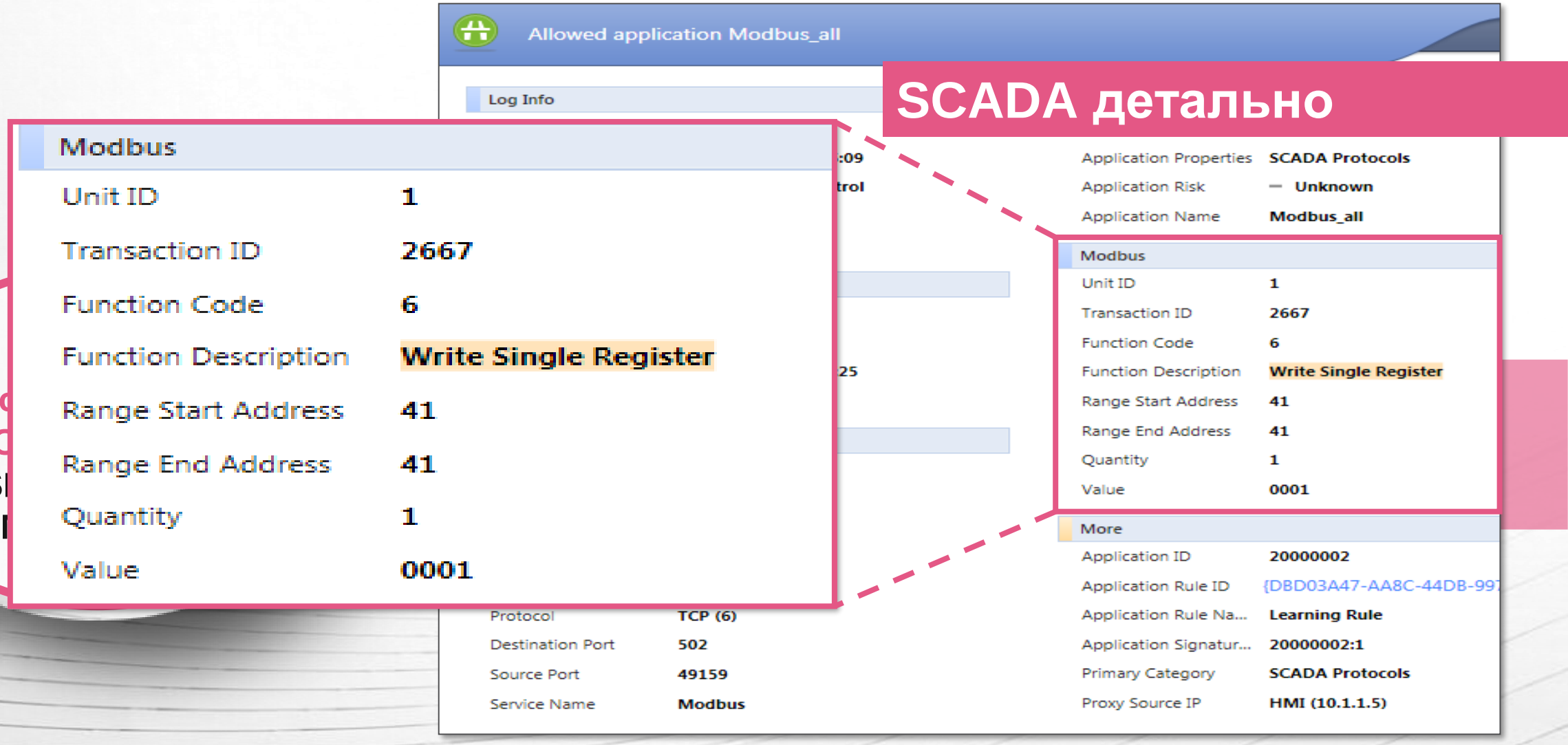
ДЕТАЛЬНО

Time		B...	A...	T...	Origin	Application...	Transa...	Fu...	Function Description	Source	Desti...	...	Matched Ca
Today	10:45:35				gw-71ec22	ModbusAll	33394	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33490	4	Read Input Registers - Response	HMI-1	PLC-1		SCADA Prot
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

ПО ГРУППАМ

Count	Source	Destination	Unit ID	Function Description	Transaction ID	Start Address
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**		**10**
1	HMI (10.1.1.5)	PLC (20.1.1.5)	1	Write Single Register	19	50

Полная отчетность по SCADA трафику

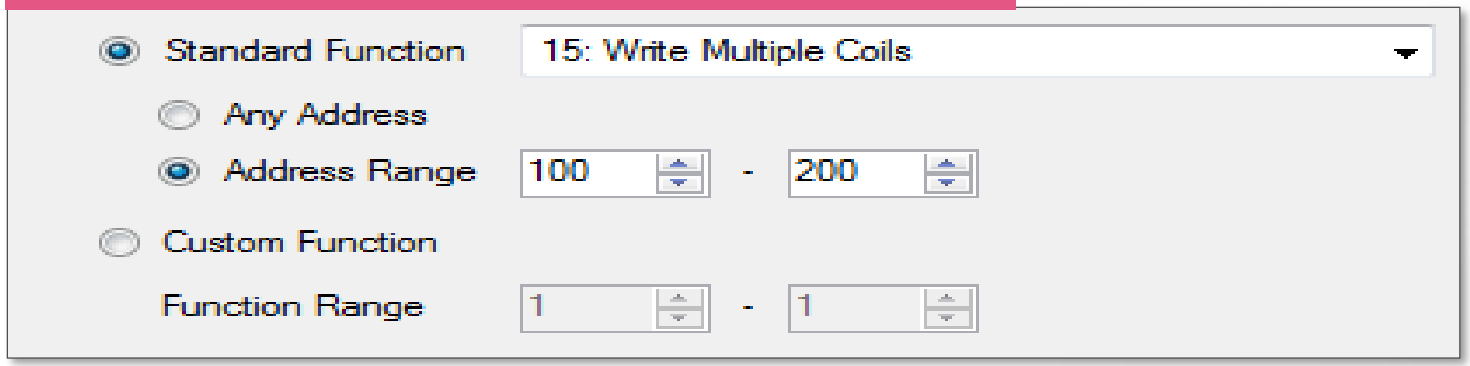


Полный контроль и видимость SCADA трафика

ПРОТОКОЛЫ и КОМАНДЫ

Source	Destination	Applications/Sites	Action
Any	Any	High Risk	Block Blocked
Control_servers	PLCs	Modbus Protocol-write single register Modbus Protocol-write multiple coils Modbus Protocol-write file record Modbus Protocol-write single coil	Allow
Monitor_servers	PLCs	Modbus Protocol-read input register Modbus Protocol-read coils Modbus Protocol-read file record	Allow

ПАРАМЕТРЫ КОМАНД



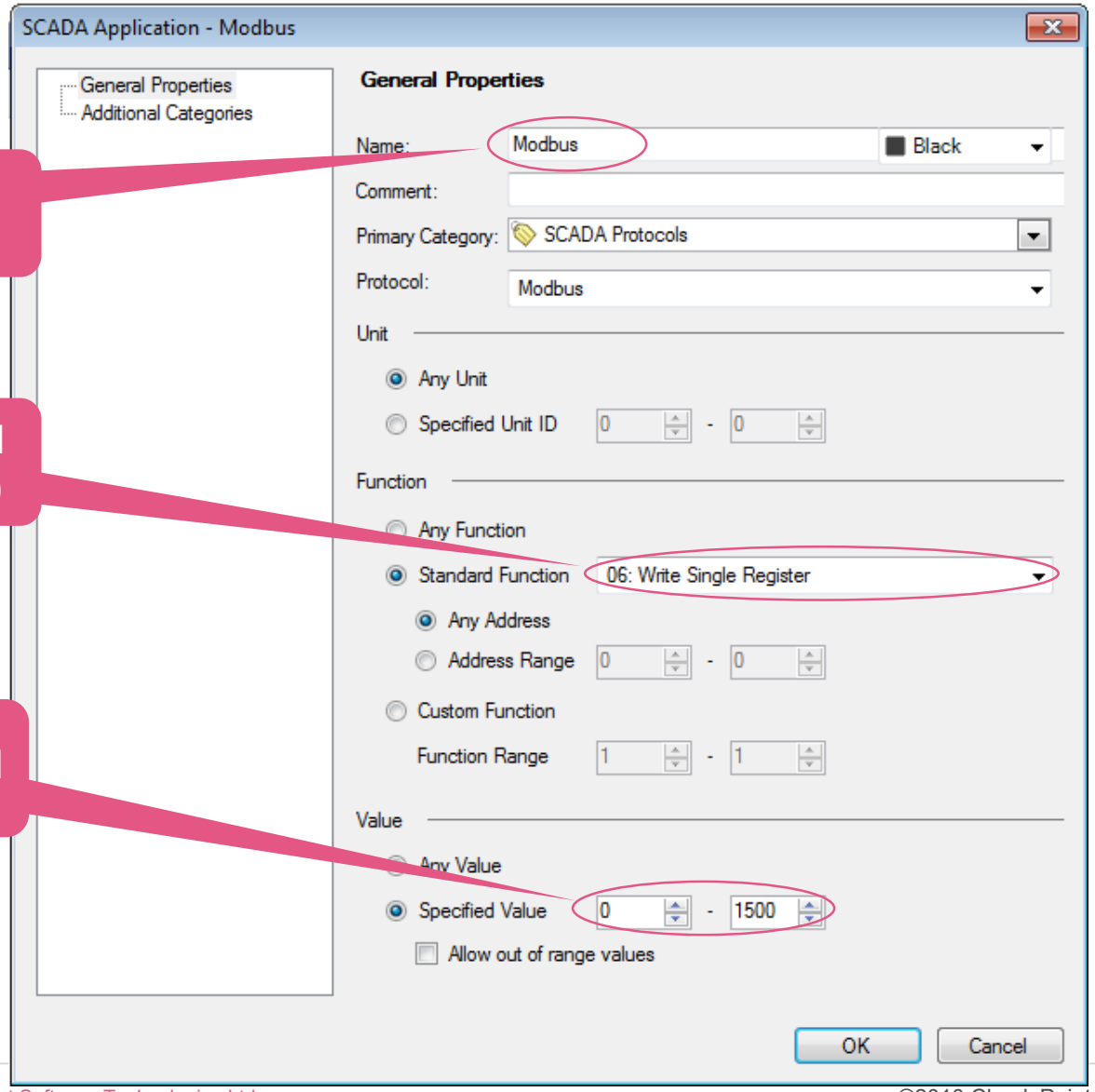
Настройка Политик и Правил устанавливая Функции и Значения (Functions and Values)

Check Point
SOFTWARE TECHNOLOGIES LTD.

Protocol

Command (Function)

Allowed values and ranges



Active or Passive Policy

Name	Source	Destination	Applications/Sites	Action
Block High Risk apps	Any	Any	High Risk	Block Blocked
Control servers	Control_servers	PLCs	Modbus Protocol-write single register Modbus Protocol-write multiple coils Modbus Protocol-write file record Modbus Protocol-write single coil	Allow
Monitor servers	Monitor_servers	PLCs	Modbus Protocol-read input register Modbus Protocol-read coils Modbus Protocol-read file record	Allow
Block SCADA traffic	Any	Internal PLCs	SCADA Protocols	Block

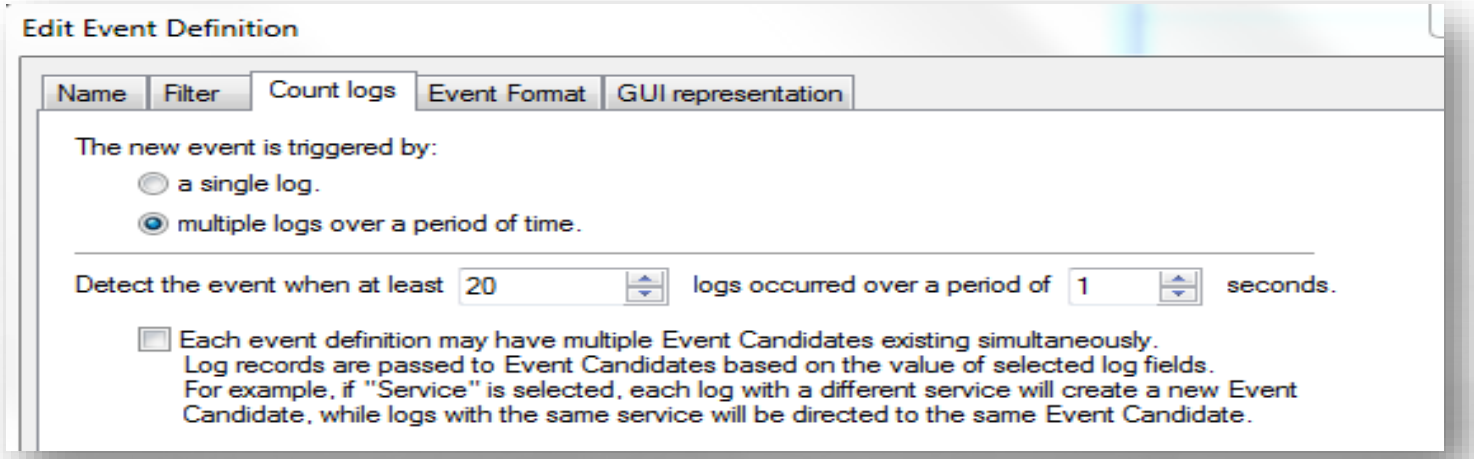
Виртуальный пачтинг с помощью свыше 200 специализированных IDS/IPS сигнатур

Check Point
SOFTWARE TECHNOLOGIES LTD.

ЗАЩИТА
с помощью
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

Быстрый анализ подозрительного трафика между контроллерами



АНАЛИЗ
с помощью
Check Point
SMARTEVENT

- Анализ риска с помощью специализированных отчетов угроз
- Просмотр попыток отправить избыточные команды
- Просмотр попыток сетевой разведки

Check Point 1200R

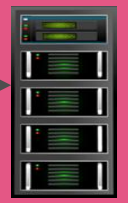
Специально разработанный защищенный шлюз безопасности

- **Полнофункциональный** шлюз безопасности Check Point
- **6x1GbE портов** и firewall throughput до 2Gbps
- **Соответствует** самым жестким регуляторным требованиям: IEC 61850-3 и IEEE 1613
- **Компактный безвентиляторный** дизайн; температурный диапазон от -40°C до 75°C

OT Security Blueprint

Management Facility

Main Control Center



SCADA Historian

SmartEvent

SCADA VPN

Control & monitor

Control

Monitor

PLC1 PLC2 PLC3

PLC4

Shop Floor

Shop Floor