

От мониторинга безопасности OT инфраструктуры к непрерывности производства

10 сентября 2024 г., Красноярск

Positive Technologies

Начнём со знакомства



**Евгений
Орлов**

13 лет работы в
автоматизации
(энергетика)

Окончил ИжГТУ в
2005 г., инженер-
системотехник

Продавал АСУ в
энергетику, теперь
занимаюсь их защитой



5 вопросов на тему ИБ АСУ ТП
на сайте oproso.net

Кибербезопасность
производства

Кибербезопасность
ИТ инфраструктуры



Защиты периметра уже недостаточно

- Не на все устройства можно установить средства защиты
- Предприятия не всегда знают о своих активах
- Много легитимных пользователей, операций и процессов



За примерами ходить далеко не нужно:



Производство:

Компьютеры в сборочном цеху пострадали от шифровальщика, попавшего в технологическую сеть через подключенную к сети кофемашину

Как:

Кофемашина подключена к технологической сети, оставаясь подключенной к корпоративной сети (и интернету). Старое и необновлённое ПО производства быстро стало мишенью шифровальщиков



Непрерывность бизнеса — это способность организации планировать свою работу в случае инцидента и нарушения её деятельности, направленная на обеспечение **непрерывности основных операций** на установленном приемлемом уровне.

ГОСТ Р ИСО 22301-2014

Обеспечение непрерывности работы производственных систем



Область применения решений ОТ cybersecurity

Visibility

Наблюдаемость

ОТ инфраструктура обеспечена возможностью наблюдения за ней

Компо-
ненты и
инфра-
структура

Пользова-
тели

Режимы
работы

Resilience

Устойчивость

ОТ инфраструктура функционирует в условиях внешних и внутренних негативных воздействий

Устойчивое
функциони-
рование

Защищён-
ная
эксплуа-
тация

Безопас-
ное
обслужи-
вание

Continuity

Непрерывность

ОТ инфраструктура обеспечивает непрерывность производства и бизнес-процессов

Visibility / Наблюдаемость



Компоненты и инфраструктура

Знание о

- инфраструктуре (оборудование, ПО)
- взаимодействиях (трафик на периметре и внутри технологического сегмента)
- уязвимостях и недостатках конфигураций

Пользователи

Знание о

- всех легитимных пользователей, их ролях
- правилах доступа к инфраструктуре функциям
- правах на выполнение операций
- способах управления пользователями

Режимы

Знание о

- нормальных, аварийных, сервисных режимах работы систем
- правилах эксплуатации систем во всех режимах

Обеспечение видимости

AM/VM (управление активами и уязвимостями)

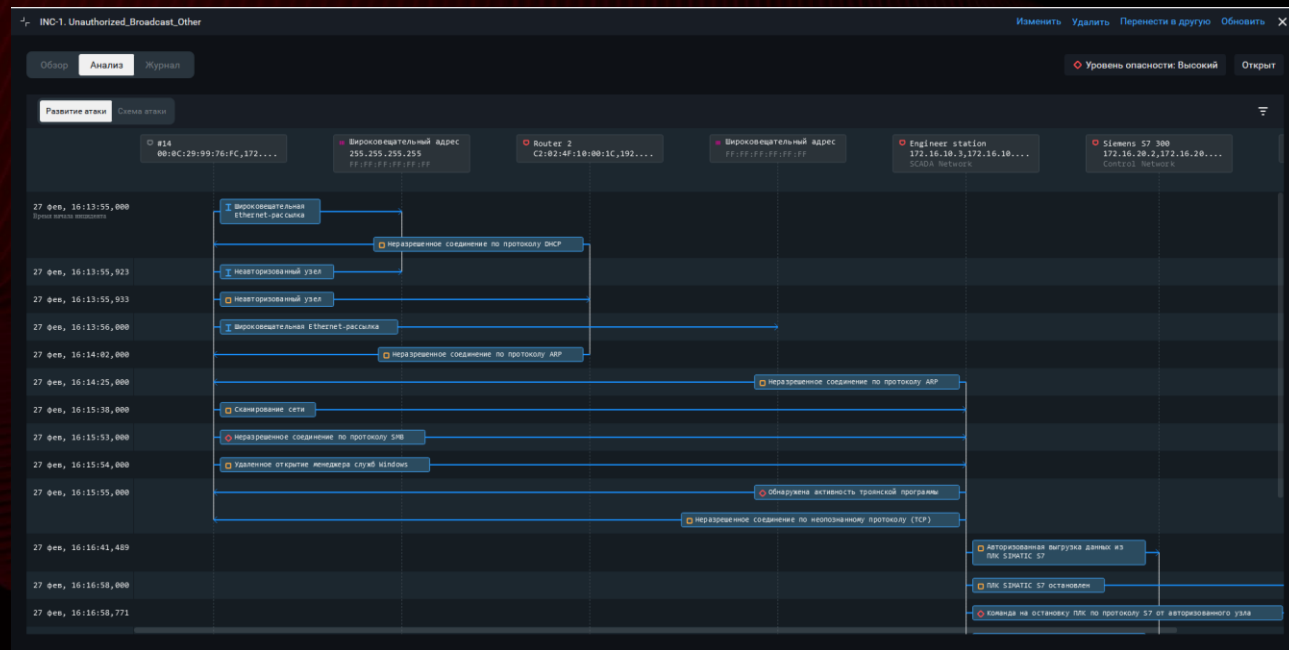
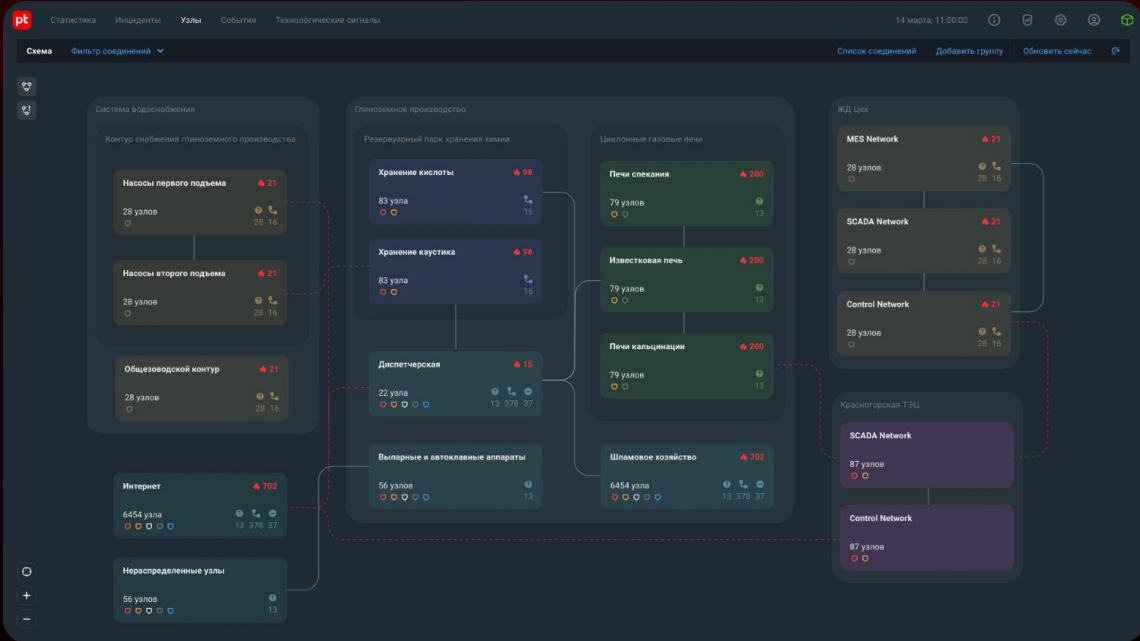
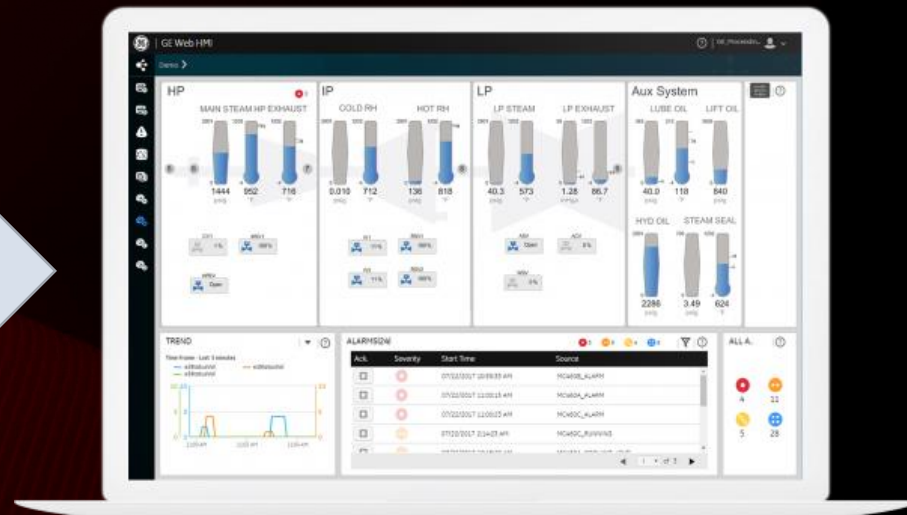
МОНИТОРИНГ

Контроль состава, конфигураций, уязвимостей и изменений Системы

Контроль изменений в профилях пользователей.

Контроль изменений системы во всех режимах эксплуатации

Visibility / Наблюдаемость



Устойчивое
функционирование

Защищённая
эксплуатация

Безопасное
обслуживание

Обеспечение устойчивости

МОНИТОРИНГ

ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ

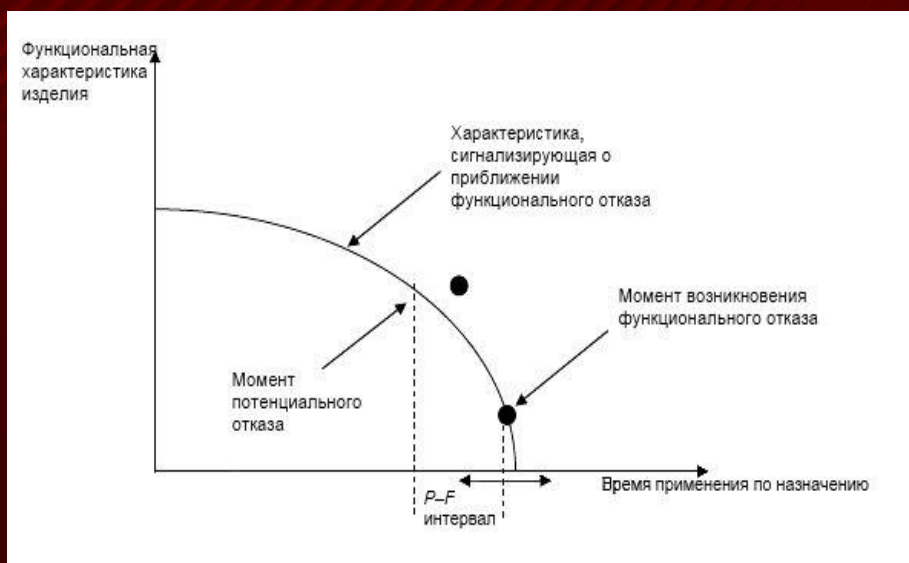
УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- Контроль функционирования ОТ-инфраструктуры
- Своевременное восстановление после сбоев

- Контроль действий пользователей
- Контроль операций управления
- Обнаружение аномалий

- Контроль доступа и операций сервисного обслуживания
- Контроль изменений ОТ-инфраструктуры

Мониторинг – ключевой процесс



Предиктивное обслуживание:

Кривая P-F иллюстрирует выявление оптимальной точки потенциального отказа (P), когда обнаружен потенциальный отказ и ещё можно предпринять меры по обслуживанию и ремонту оборудования, до его функционального отказа (F). Чем раньше выявили – тем дешевле обслуживание и больше времени на реагирование → требуется мониторинг и сбор, хранение и обработка данных с различных источников

Результативная кибербезопасность:

Средства ИБ на предприятии должны усложнить и замедлить атаку, а мониторинг ИБ должен обеспечивать выявление атаки на самых ранних стадиях.

$$TTA \curvearrowright > TTR \curvearrowleft$$



Комплексный ИБ мониторинг в АСУ ТП

	ПЛК	Сетевое оборудование	АРМы	Серверы
Прикладной уровень				
Пользовательский (операционный) уровень	Управление процессами и производством			
	Конфигурирование систем управления			
	Сервисное обслуживание ОТ-инфраструктуры			
	Администрирование ОТ-инфраструктуры			
Уровень прикладного ПО	Firmware		Ком-ное ПО	
	Проект ПЛК		Инженерное ПО	
			ПО SCADA	
			Проект ПЛК и SCADA	
Системный уровень			ОС	ОС
			СУБД	СУБД
				Среды вирт-ции
				Орк-торы контейнеров
Сетевой уровень		Конфиг-е файлы		
		Firmware		
			Трафик	
			NetFlow	

Опасные команды и операции
 Подозрительные сервисные команды и операции
 Смена конфигураций ПЛК, SCADA
 Модификация/удаление исторических данных
 Манипуляции с настройками ПО
 Подлог и нелегитимные действия

Обнаружение вредоносного ПО
 Обнаружение вторжений
 Обнаружение повышения привилегий
 Обнаружение сетевых аномалий
 Обнаружение смены конфигураций Системного ПО

Комплексный ИБ мониторинг в АСУ ТП

	ПЛК	Сетевое оборудование	АРМы	Серверы
Прикладной уровень				
Пользовательский (операционный) уровень	Управление процессами и производством			
	Конфигурирование систем управления			
	Сервисное обслуживание ОТ-инфраструктуры			
	Администрирование ОТ-инфраструктуры			
Уровень прикладного ПО	Firmware		Ком-ное ПО	
	Проект ПЛК		Инженерное ПО	
			ПО SCADA	
			Проект ПЛК и SCADA	
Системный уровень			ОС	ОС
			СУБД	СУБД
				Среды вирт-ции
				Орк-торы контейнеров
Сетевой уровень		Конфиг-е файлы		
		Firmware		
			Трафик	
			NetFlow	

Покрытие решениями Positive Technologies

Достаточно для формального и практического соответствия требованиям по защите критической инфраструктуры
Необходимо для гарантированного обнаружения реальных и атак в АСУ ТП

Покрытие стандартными СЗИ

Недостаточно для практического (не формального) соответствия требованиям по защите ОКИИ
Недостаточно для гарантированного обнаружения реальных угроз и атак в АСУ ТП

«Джентельменский набор» СЗИ для АСУ ТП?

- ✓ Антивирус (ФСТЭК же!)
- ✓ МСЭ (наконец-то мы отделим ТСПД от КСПД!)
- ✓ Бэкапы
- ✓ СЗИ от НСД
- ✓ СКЗИ (шифровать каналы)



Обработка событий АСУ ТП средствами защиты информации (СЗИ)



	События с конечных точек			События в сетевом трафике на периметре	События в сетевом трафике внутри АСУ ТП
	ПЛК, РЗА и т.д.	КОММУТАТОР	АРМ и СЕРВЕР		
Межсетевой экран (МСЭ, NGFW)	✗	✗	✗	✓	✗
Антивирусы и EDR	✗	✗	✓	✗	✗
SIEM Центр мониторинга	✓	✓	✓	✗	✗
Средство анализа сетевого трафика в АСУ ТП	✓	✗	✗	✗	✓

Непрерывный мониторинг сети

PT ISIM — основной инструмент обеспечения киберустойчивости промышленных предприятий

- Разбирает трафик общесетевых и промышленных протоколов на периметре и внутри сети
- Выявляет атаки и потенциально опасные действия
- Предоставляет информацию для расследования инцидентов

Непрерывный мониторинг, контроль и распознавание угроз

The screenshot displays the PT ISIM interface, which is used for managing attack detection rules and monitoring network activity. The interface is divided into several sections:

- Управление правилами обнаружения атак (Attack Detection Rule Management):** This section shows a list of rules, including "3S Codesys Gateway Server: переполнение буфера (CVE-2015-6460)" and "3S Codesys Gateway Server: переполнение буфера в CmpWebServer (CVE-2011-5007)". Both rules are currently "Включено" (Enabled).
- Инциденты (Incidents):** A table lists detected incidents with columns for "Уровень опас..." (Risk Level), "Статус" (Status), "Источник" (Source), "Цель" (Target), and "Название" (Name). For example, an incident with a "Высокий" (High) risk level, "Открыт" (Open) status, and source "Win XP SP2" is listed.
- Сканирование сети (Network Scanning):** This section shows the status of network scanning, which is currently "Включено" (Enabled). It includes a "Журнал" (Log) section with a table of scan results, such as "15 мар, 12:21:52 Administrator" and "Изменено исключение" (Exception changed).
- Анализ (Analysis):** A detailed view of network traffic analysis is shown, including a timeline of events and a flow diagram. The timeline shows events like "Попытка доступа в интернет по TCP" (Attempt to access internet via TCP) and "Обнаружена активность троянской программы" (Trojan program activity detected).

Промышленная экспертиза в продуктах PT ICS

Атомик Софт

ALPHA Platform



Прософт-Системы

Astra Regul



МПС Софт

Master SCADA



Yokogawa

Centum

Aveva

Wonderware System Platform

SIEMENS

WinCC, PCS7

AdAstra

Trace Mode

Прософт-Системы

Redkit

Еще +2 системы

до конца 2024

Корреляция и обнаружение инцидентов в ОТ инфраструктуре



Корреляция – сопоставление нескольких событий из одного или нескольких источников для обнаружения последовательностей/взаимосвязей

Обнаружение инцидентов – применение предварительно разработанных правил для определения подозрительных/опасных единичных событий или их последовательностей/взаимосвязей

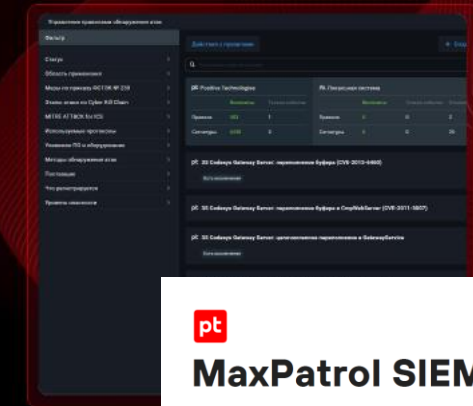


Технологическая экспертиза PT ISTI

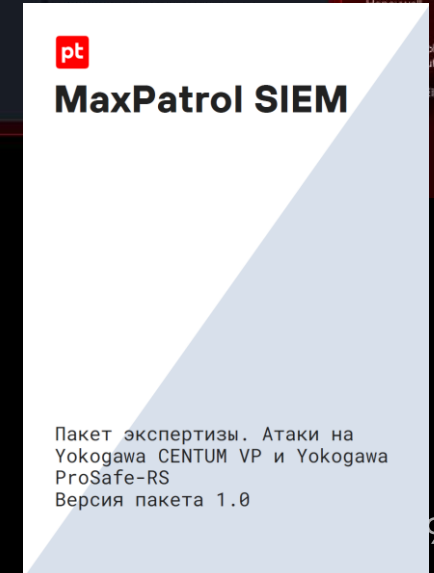
8000+

правил и индикаторов промышленных угроз «из коробки»

Охватывают промышленное ПО и оборудование в инфраструктурах на Windows и Linux



АвАстра
АМТ-груп
Атомик Софт
Монитор Электрик
МПС софт
НПФ «КРУГ»
Прософт-системы
СПИК СЗМА
ЦИФРА ЦИП
ЧЭАЗ
ЭНРА
Энвера
ABB
AVEVA
B&B
Emerson
GE
Hirschmann

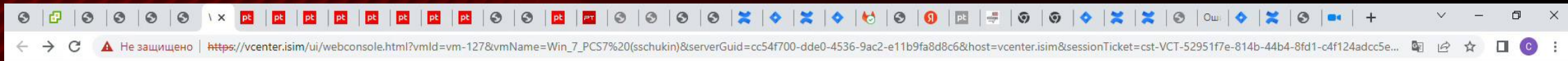


SIEM/ NTA/IDS – чем больше правил разработчиком предоставляется «из коробки» тем быстрее и проще вводить решение в эксплуатацию и тем проще требования к количеству и уровню квалификации эксплуатирующих специалистов

Демо мониторинга ИБ на прикладном уровне АСУ ТП с помощью анализатора сетевого трафика РТ ISIM и системы MaxPatrol SIEM



Среда разработки Siemens PCS7. Обнаружение остановки ПЛК серии S7-400 и перезаписи логических блоков в проекте с помощью PT ISIM и MaxPatrol SIEM



Win_7_PCS7 (sschukin) Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete



File Explorer window showing contents of 'Data' folder on Local Disk (C:).

Name	Date modified	Type	Size
TOOLS	11/12/2021 5:14 PM	Folder	
User_rules	11/12/2021 5:14 PM	File folder	
client_connect_disconnect_to_wincnc_multuser	1/20/2022 1:51 PM	Wireshark capture file	717 KB
HexEditor_0.9.5.19_x64	10/28/2021 3:26 PM	Compressed (zippe...	304 KB
MicrosoftEdgeSetup	11/12/2021 7:19 PM	Application	1,738 KB
New Text Document	10/23/2021 12:17 AM	Text Document	0 KB
npp.7.8.8.Installer.x64	10/23/2021 1:12 AM	Application	3,956 KB
Open_wincnc_alarm_logging	12/23/2021 5:07 PM	XML Document	117 KB
Open_wincnc_tag_logging	12/23/2021 5:08 PM	XML Document	360 KB
Open_wincnc_tag_management	12/23/2021 5:01 PM	Text Document	127 KB
Open_wincnc_tag_management	12/23/2021 5:03 PM	XML Document	116 KB
ProcessMonitor	1/14/2022 3:29 PM	Compressed (zippe...	3,332 KB
Rules	11/12/2021 5:05 PM	Compressed (zippe...	865,901 KB
s7_monitor_modify_m8_3	11/16/2021 1:57 AM	Wireshark capture file	3,265 KB
simatic_software.csv	2/14/2022 3:28 PM	CSV File	3 KB
tcmd1000x64	2/3/2022 6:36 PM	Application	5,720 KB
test - Copy21	12/21/2021 5:45 PM	WinCC.Graphics.Do...	1 KB
test_sysmon_event	2/3/2022 11:27 AM	XML Document	2 KB
versionSW.csv	8/3/2022 2:51 PM	CSV File	3 KB
Wireshark-win64-3.4.9	10/22/2021 12:36 PM	Application	69,702 KB



pt@ptsecurity.com



ptsecurity.com