От мониторинга безопасности ОТ 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

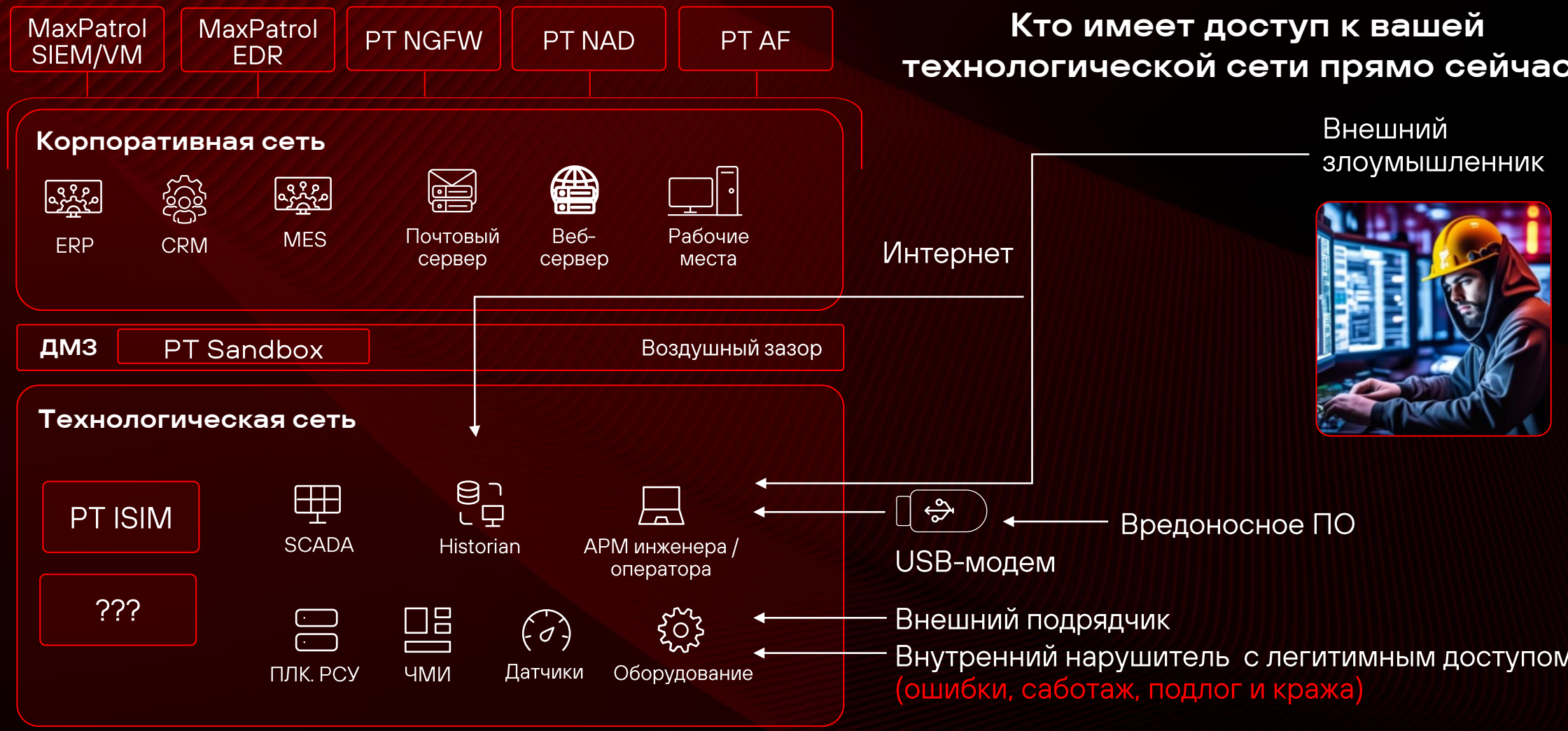
5 вопросов на тему ИБ АСУ ТП

на сайте oprosso.net

Кибербезопасность производства

Кибербезопасность ИТ инфраструктуры

А от кого защищать производство?



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 OT cybersecurity

Visibility

Наблюдаемость

OT инфраструктура обеспечена возможностью наблюдения за ней

- **Компоненты и инфраструктура**
- **Пользователи**
- **Режимы работы**

Resilience

Устойчивость

OT инфраструктура функционирует в условиях внешних и внутренних негативных воздействий

- **Устойчивое функционирование**
- **Защищённая эксплуатация**
- **Безопасное обслуживание**

Continuity

Непрерывность

OT инфраструктура обеспечивает непрерывность производства и бизнес-процессов

Visibility / Наблюдаемость

Компоненты и инфраструктура

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

Пользователи

Знание о
- всех легитимных пользователях, 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)

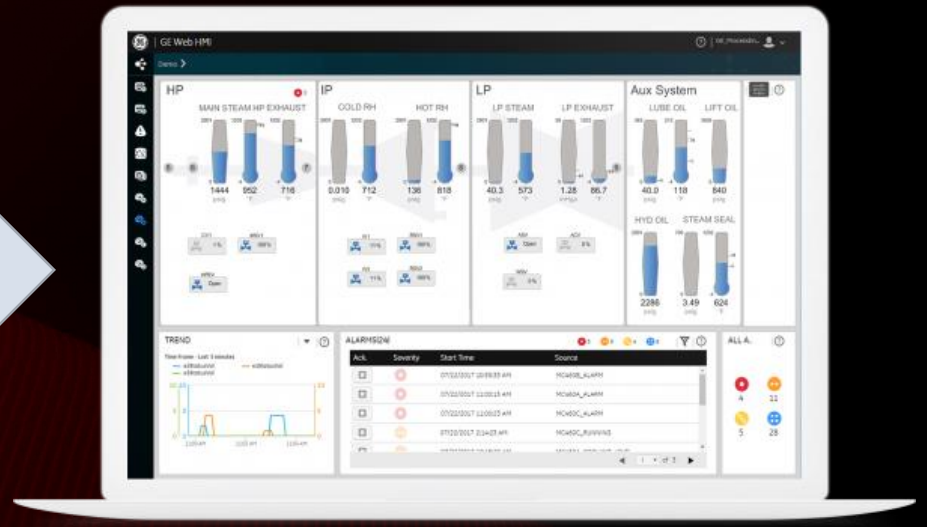
МОНИТОРИНГ

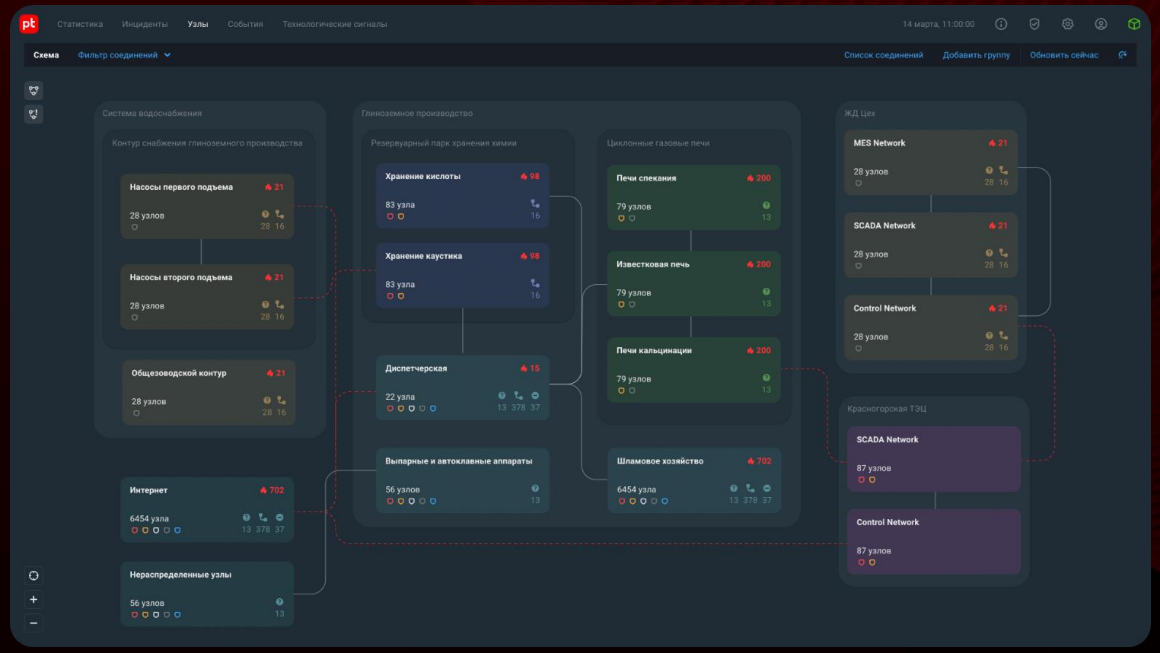
Контроль состава, конфигураций, уязвимостей и изменений Системы

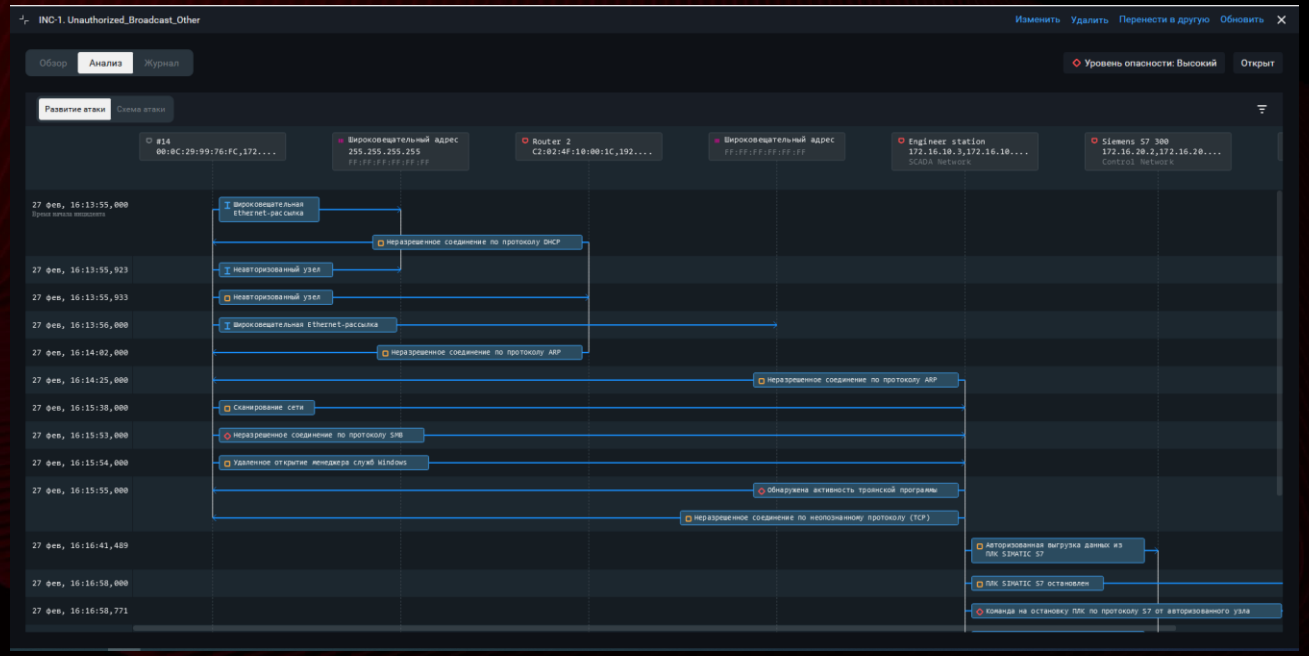
Контроль изменений в профилях пользователей.

Контроль изменений системы во всех режимах эксплуатации

Visibility / Наблюдаемость







Resilience / Устойчивость

Устойчивое функционирование	Защищённая эксплуатация	Безопасное обслуживание

Обеспечение устойчивости

МОНИТОРИНГ

ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ

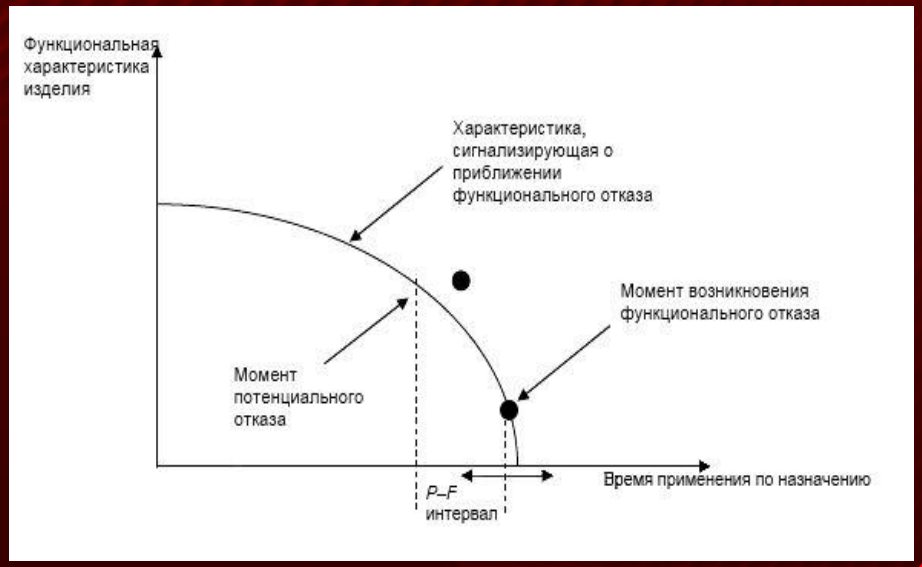
УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- Контроль функционирования OT-инфраструктуры
- Своевременное восстановление после сбоев

- Контроль действий пользователей
- Контроль операций управления
- Обнаружение аномалий

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

Мониторинг – ключевой процесс

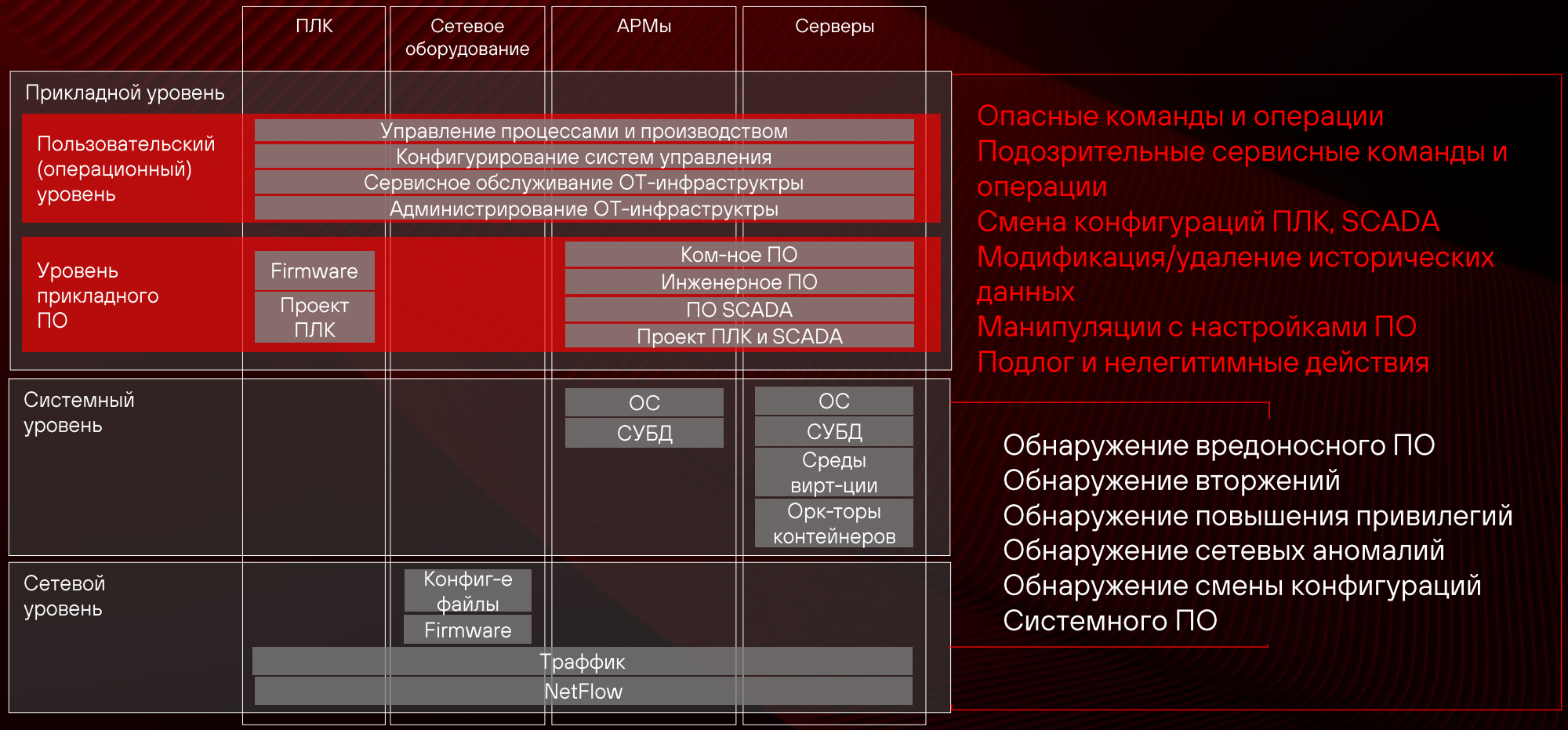


Предиктивное обслуживание:
Кривая P-F иллюстрирует выявление оптимальной точки потенциального отказа (P), когда обнаружен потенциальный отказ и ещё можно предпринять меры по обслуживанию и ремонту оборудования, до его функционального отказа (F). Чем раньше выявили – тем дешевле обслуживание и больше 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 ↗ > TTR ↘

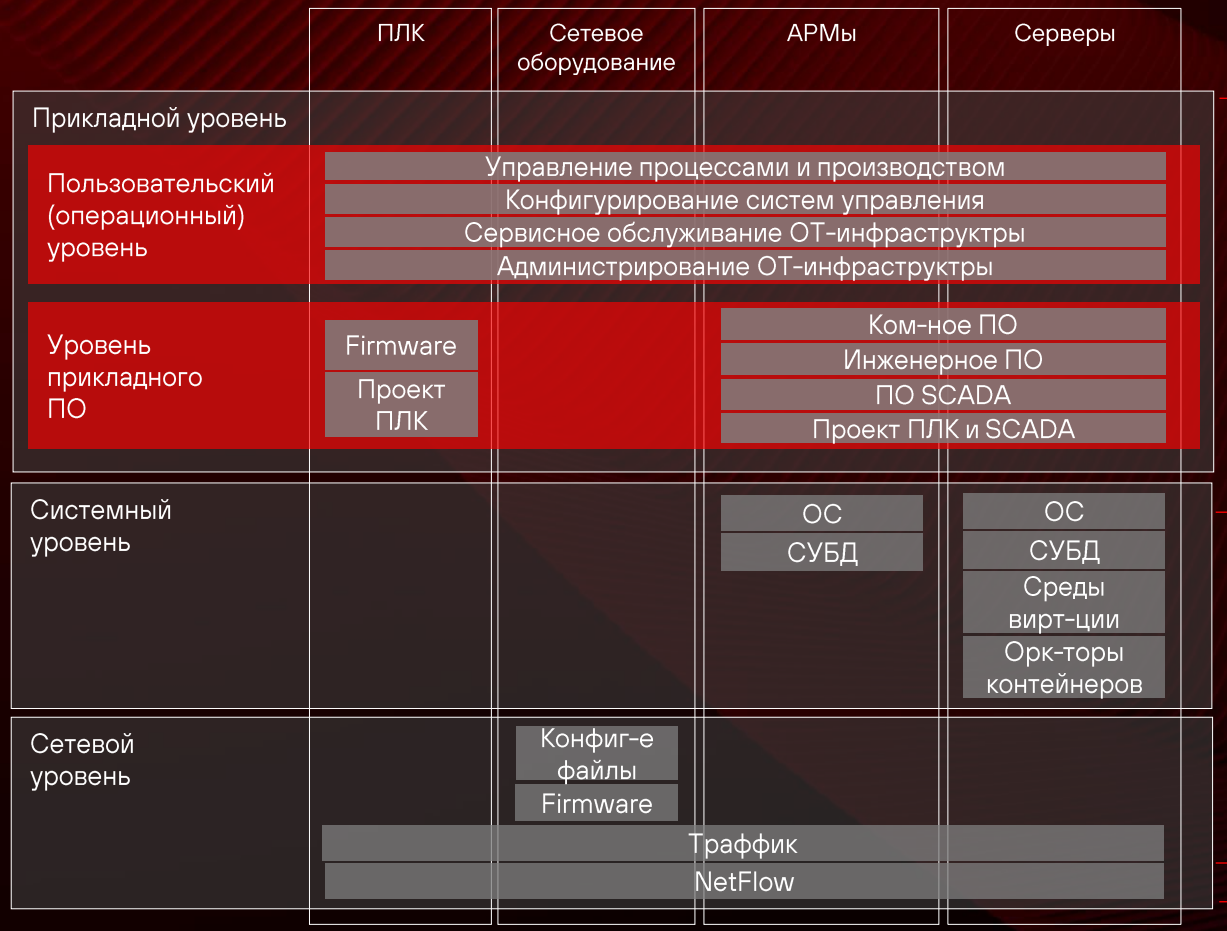
Комплексный ИБ мониторинг в АСУ ТП



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



Покрытие решениями Positive Technologies

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

Покрытие стандартными СЗИ

Недостаточно для практического (не формального) соответствия требования 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)

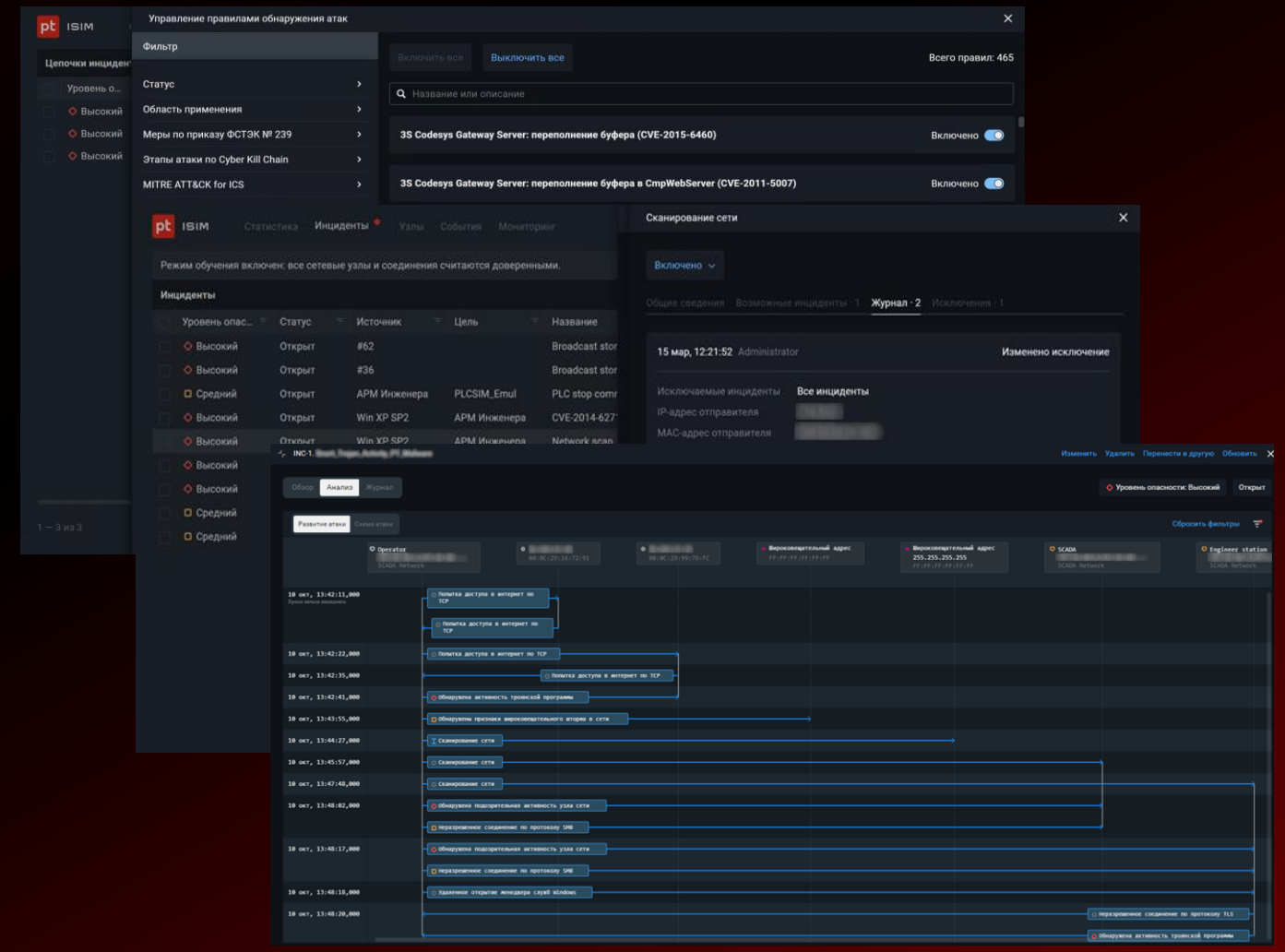
Обработка событий АСУ ТП средствами защиты информации (СЗИ)

	События с конечных точек			События в сетевом траффике на периметре	События в сетевом траффике внутри АСУТП
	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

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

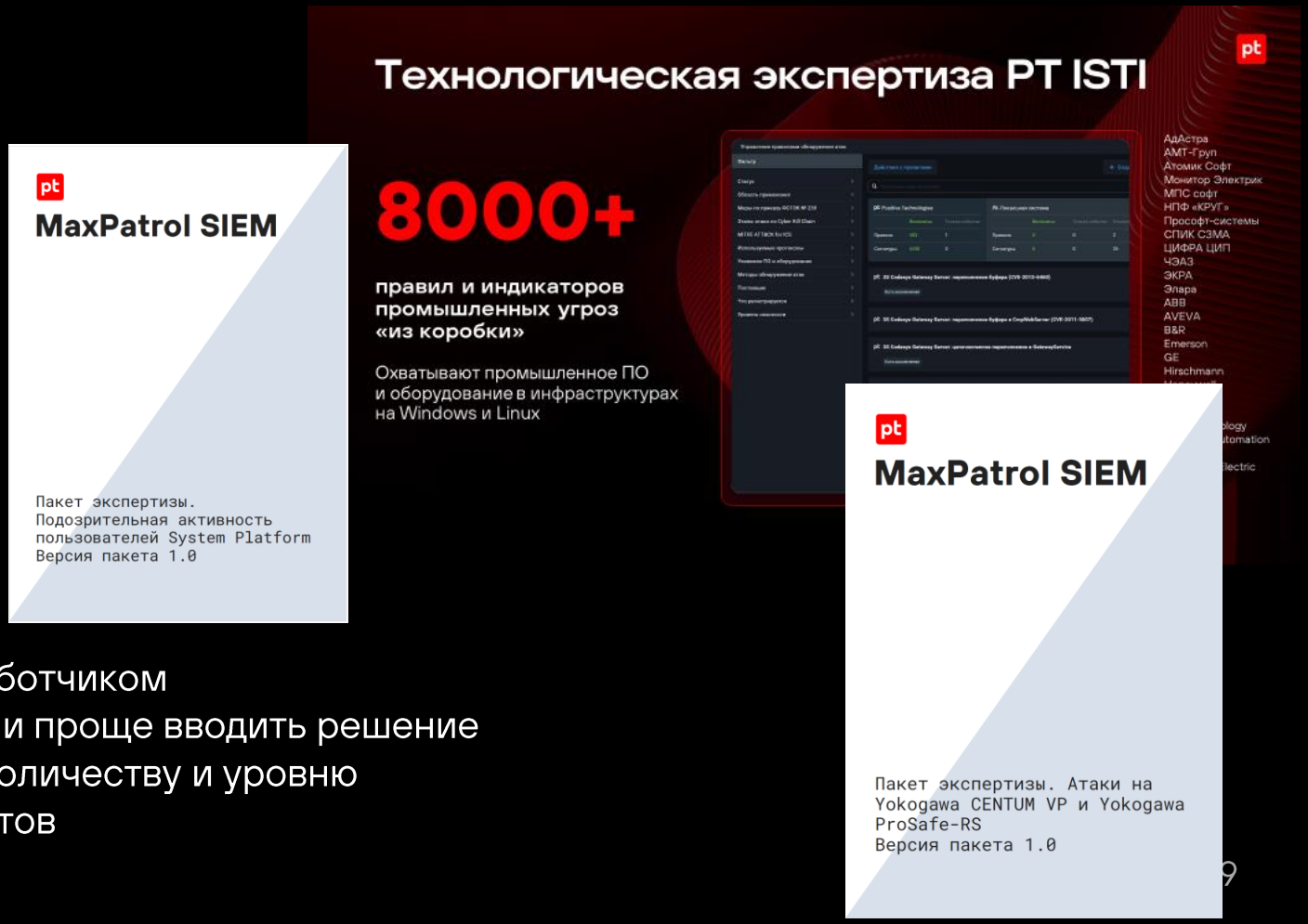
Еще +2 системы

до конца 2024

Корреляция и обнаружение инцидентов в OT 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

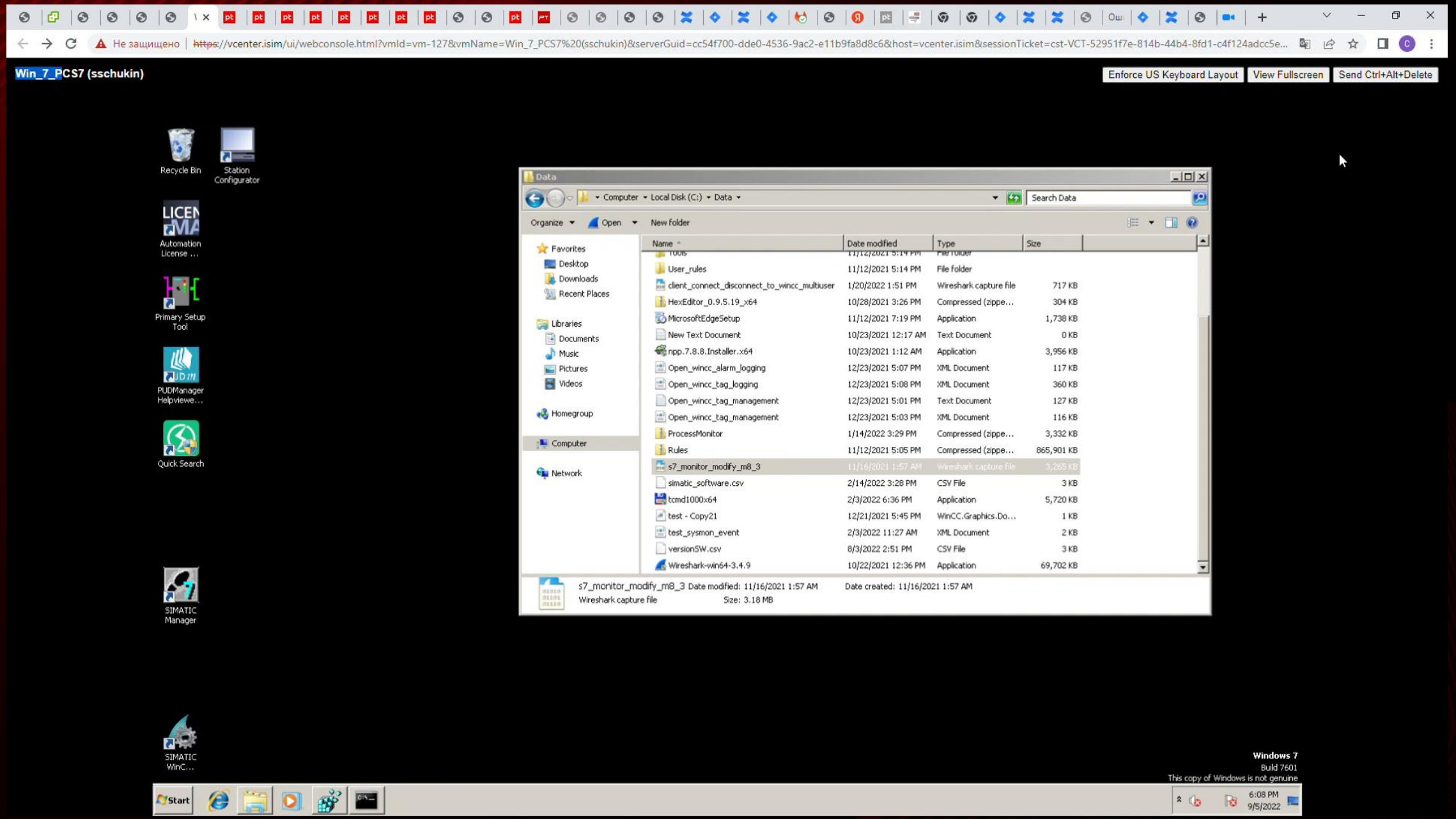


SIEM/ NTA/IDS – чем больше правил разработчиком предоставляется «из коробки» тем быстрее и проще вводить решение в эксплуатацию и тем проще требования к количеству и уровню квалификации эксплуатирующих специалистов

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

20

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




pt@ptsecurity.com
ptsecurity.com