Мониторинг безопасности прикладного уровня систем промышленной автоматизации

Дмитрий Даренский
Руководитель практики промышленной кибербезопасности
Positive Technologies

Уязвимости в промышленных ИТ-инфраструктурах

По данным Positive Technologies, в среднем на промышленном предприятии выявляется от одного до пяти грубых нарушений, таких как:

- Непроектные АРМ с выходом в интернет
- Незащищенные точки доступа
- Не контролируемый, в т.ч. удаленный доступ к ресурсам технологической сети
- Неавторизованные каналы связи
- Отсутствие сегментации сети и паразитный трафик
- Использование паролей по умолчанию и общих учётных записей пользователей

Импортозамещение и актуальные угрозы АСУ ТП

Заблокированный вендором сервисный доступ в работающих АСУ ТП для специалистов предприятия

Не декларируемые каналы удалённого доступа вендоров и их партнёров к АСУ ТП на площадке

Сложность проверки и отсутствие доверия к патчам и обновлениям от вендоров АСУ ТП

Де-факто не доверенные СЗИ на периметре и внутри АСУ ТП

Отсутствие контроля доступа к критичной информации со стороны иностранных вендоров

Отсутствие контроля за действиями сторонних сервисных инженеров.

Какие возможности это даёт злоумышленникам

Угрозы безопасности **прикладного уровня** систем промышленной автоматизации способы их реализации в БДУ ФСТЭК:

Выполнение не легитимных и не корректных пользовательских операций в среде исполнения АСУ ТП

УБИ.3

СП.18.1, СП.18.2, СП.19.1, СП.19.2, СП.19.3, СП.19.4, СП.19.5, СП.21.1, СП.21.2, СП.21.3, СП.23.1, СП.23.2, СП.24.2,1

Не легитимное и не корректное использование инженерного ПО, среды разработки SCADA, проектов PLC и Safety

УБИ.3

СП.18.1, СП.18.2, СП.19.1, СП.19.2, СП.19.3, СП.19.4, СП.19.5, СП.21.1, СП.21.2, СП.21.3, СП.23.1, СП.23.2, СП.24.2,1

Подмена/модификация конфигураций и проектов SCADA, PLC и Safety терминалов

УБИ.4

СП.18.1, СП.18.2, СП.19.1, СП.19.2, СП.19.3, СП.19.4, СП.19.5, СП.21.1, СП.21.2, СП.21.3, СП.23.1, СП.23.2, СП.24.2,1

Деструктивные воздействия изнутри и извне систем управления

УБИ.2 , УБИ.6

СП.21.2, СП.21.3, СП.23.1, СП.23.2,

Сокрытие следов своей деятельности в прикладном ПО

УБИ.5

СП.2.2, СП.2.7, СП.2.8, СП.2.11,

Негативные последствия

Негативные последствия БДУ ФСТЭК, реализуемых, в том числе, через атаки на **прикладной уровень** систем промышленной автоматизации:

Н.14
Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса

Н.25
Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)

Н.32
Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения

Н.41
Вредные воздействия на окружающую среду

Н.44
Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонент

За примерами ходить не далеко

Нефтебаза

Слив из хранилища и вывоз десятка автовозов с нефтепродуктами.

Сокрытие следов в SCADA

экономический ущерб

АЭС
(дружественное государство)

До 20 разновидностей ВПО в системе контроля радиационного фона атомного энергоблока

Потенциальный ущерб государству, населению, экологии

Центр переработки ТБО

Незаконный ввоз и разгрузка ТБО на территорию центра.
Доступ к системе СКУД у водителей с незадекларированным грузом.
Разгрузка в обход систем контроля

экономический ущерб

Нефтепровод

Получение неучтённых остатков нефти при транспортировке
Слив и вывоз с территории ППН неучтённых остатков

экономический ущерб

Металлургический комбинат

Пьяный сотрудник удалённо отключил ПАЗ и взял управление козловым краном.

Уронил его, вывел из строя производство, погиб специалист находившийся на площадке

экономический ущерб

гибель человека

Меры защиты

Меры защиты систем промышленной автоматизации Приказа №239 ФСТЭК, реализация которых распространяется в том числе и на **прикладной уровень**

V. Аудит безопасности (АУД)				
АУД.4	Регистрация событий безопасности	+	+	+
АУД.5	Контроль и анализ сетевого трафика			+
АУД.7	Мониторинг безопасности	+	+	+
АУД.9	Анализ действий отдельных пользователей			+

VII. Предотвращение вторжений (компьютерных атак) (СОВ)				
СОВ.1	Обнаружение и предотвращение компьютерных атак		+	+

XII. Реагирование на компьютерные инциденты (ИНЦ)				
ИНЦ.1	Выявление компьютерных инцидентов	+	+	+
ИНЦ.2	Информирование о компьютерных инцидентах	+	+	+
ИНЦ.3	Анализ компьютерных инцидентов	+	+	+
ИНЦ.4	Устранение последствий компьютерных инцидентов	+	+	+
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	+	+	+
ИНЦ.4	Устранение последствий компьютерных инцидентов	+	+	+

Недопустимые события

Покрытие решениями Positive Technologies

Достаточно для формального и практического соответствия требования по защите ОКИИ
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

Что такое "промышленная экспертиза“ в по понимании Positive Technologies?

Поддержка АСУ ТП в продуктах Positive Technologies за счёт Обширной базы экспертных знаний о структуре, компонентах, уязвимостях, отраслевой специфике и особенностях эксплуатации систем автоматизации отдельных вендоров

ИССЛЕДУЕМ

- Как работает система автоматизации
- Особенности использования в отдельных отраслях
- Протоколы обмена данными между
- Структура и форматы журналов событий
- Уязвимости и нештатное использование функций ПО
- Подбор режимов сканирования серверов контроллеров, рабочих станций, сетевого оборудования

РАЗРАБАТЫВАЕМ

- Анализируем и систематизируем знания
- Тестируем прототипы решений на стендах вместе с вендорами АСУ ТП
- Закладываем знания в продукты в виде:
  - Анализаторов траффика
  - Эмулированных программных сред
  - Скриптов и профилей сканирования
  - Корреляций
  - Базы уязвимостей

АДАПТИРУЕМ

- Типовые решения для применения в различных отраслях

…ведь АЭС отличается от НПЗ, которая отличается ГОК, который отличается от метро

- Типовые интегрированные решения с наиболее распространёнными платформами автоматизации

…ведь Siemens отличается от Honeywell, который отличается, от АтомикСофт, который отличается Прософт

Пример:
Мониторинг событий безопасности Alpha.Platform

- Поддержка протокола для разбора сетевого трафика
- Подмена или попытка изменить конфигурацию проекта сервера данных
- Подмена конфигурационного файла сервера данных
- Фиксация остановки сервера данных
- Обнаружение изменений конфигурации Alarms, Trends, Historian, openLDAP, mdb openLDAP, Alpha.HMI
- Обнаружение изменений файлов базы данных AlphaHistorian
- Обнаружение изменение требований к паролю в AlphaSecurityConfigurator по умолчанию
- Обнаружение изменение конфигурации Alpha Security
- Обнаружение изменение исполняемых файлов AlphaPlatorm
- Обнаружение запуска процесса среды разработки Alpha.HMI
- Обнаружение завершение процесса среды визуализации Alpha.HMI

Технологическое партнёрство

АМТ-Груп	**Техническая совместимость и функциональная применимость InfoDiode с MaxPatrol SIEM и PT ISIM**	✓
ЦИФРА ЦИП	Совместимость Платформы ZIIoT с PT ICS	🕒
	Совместимость АИС Диспетчер с PT ICS	🕒
B&R	Совместимость ПТК АСУ ТП с PT ISIM	✓
ЧЭАЗ	Совместимость ПТК «КВАНТ-ЧЭАЗ» с MaxPatrol SIEM	✓
АдАстра	Пакеты экспертиз для программного обеспечения Trace Mode в продуктах платформы PT ICS, Совместимость с MaxPatrol SIEM	✓
AVEVA	Пакеты экспертиз для программного обеспечения Wonderware в продуктах платформы PT ICS, Совместимость с MaxPatrol SIEM	✓
SIEMENS	Пакеты экспертизы для программного обеспечения WinCC, PCS7, Simatic NET networks в продуктах платформы PT ICS	✓
Schneider Electric	Интегрированные решение на базеPT ISIM software & Magelis hardware	✓
Атомик Софт	Совместное комплексное решение на базе компонентов ALPHA Platform и PT ICS	✓
ФГУП ЭЗАН	Совместимость с SCADA «СОНАТА» MaxPatrol 8, MaxPatrol SIEM	🕒
ИнСАТ	Совместимость Master SCADA с PT ICS	✓
PRO SOFT System	Совместимость ПТК на базе платформы Redkit SCADA с PT ICS	🕒
	Совместимость ПТК на базе ПЛК REGUL с PT ICS	🕒
100+ Protocols	Siemens, Schneider Electric, Rockwell Automation, Yokogawa, Emerson, B&R, Bombardier, MOXA, B&R, Honeywell, Mitsubishi …	✓
Технологии Движения	Совместимость ПТК ДЦ ММ с PT ICS	✓
1520 Сигнал	Совместимость ПТК МПЦ с PT ISIM	✓
PLC Technology	Совместимость ПТК TOPAZ с PT ICS	🕒
ЭКРА	Совместимость ПТК ЭКРА с PT ICS	🕒
СПИК СЗМА	Совместимость ПТК АСУ ТП на базе АРБИТР.SCADA с PT ICS	✓

Что такое "промышленная экспертиза“ в продуктах Positive Technologies?

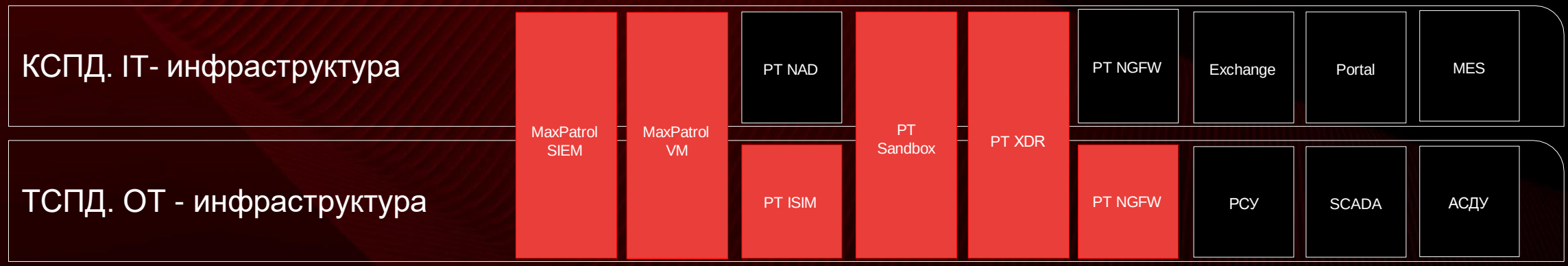
		Siemens	AdAstra	AVEVA	Мастер Скада	Rockwell	Yokogawa	Schneider Electric	«Атомик Софт»	ПроСофт REGUL RedKit
MaxPatrol VM	▪ Сканеры SCADA, firmware ▪ Обнаружение уязвимостей	✓	🕒	✓	🕒	🕒	✓	✓	🕒	🕒
MaxPatrol SIEM	▪ Транспорты к проприетарному software и firmware ▪ Нормализации событий SCADA, Firmware ▪ Кейс-ориентированные корреляции	✓	✓	✓	✓	🕒	✓	🕒	🕒	🕒
PT ISIM	▪ Поддержка промышленных сетевых протоколов ▪ Детекты новых угроз и атак ▪ Цепочки инцидентов в технологическом трафике	✓	N/A	✓	N/A	✓	✓	✓	✓	✓
PT Sandbox	▪ Эмуляция технологических сред ▪ Обнаружение АСУ ТП-специфичного ВПО	✓	✓	✓	🕒	🕒	🕒	✓	🕒	🕒
PT XDR	▪ Совместимость с промышленным hardware/software ▪ Правила обнаружения, работающие на конечных узлах ▪ Инвентаризация, сканирование, ИТ-мониторинг	🕒	🕒	🕒	🕒	🕒	🕒	🕒	🕒	🕒
PT NGFW	▪ Поддержка промышленных сетевых протоколов ▪ База правил обнаружения событий безопасности на периметре технологической сети	🕒	🕒	🕒	🕒	🕒	🕒	🕒	🕒	🕒

PT ICS - комплексное решение для защиты АСУ ТП

PT ISIM	Глубокий анализ трафика в промышленных ИТ-инфраструктурах, IIoT средах, DICOM системах и сетях
MaxPatrol SIEM	Для SOC: сбор и анализ событий безопасности с прикладного уровня систем АСУ ТП: серверов SCADA, контроллеров, АРМ
MaxPatrol VM	Выявление уязвимостей в промышленных системах и управление процессом их устранения
PT Sandbox	Поведенческий анализ файлов и антивирусная проверка файлов из трафика и с рабочих станций
MaxPatrol EDR	Обнаружение целевых и сложных угроз на рабочих станциях и серверах
PT NGWF	Межсетевой экран нового поколения, сочетающий в себе производительность, надежность и простоту эксплуатации

PT ICS. Базовая архитектура

Уровень ИТ-инфраструктуры

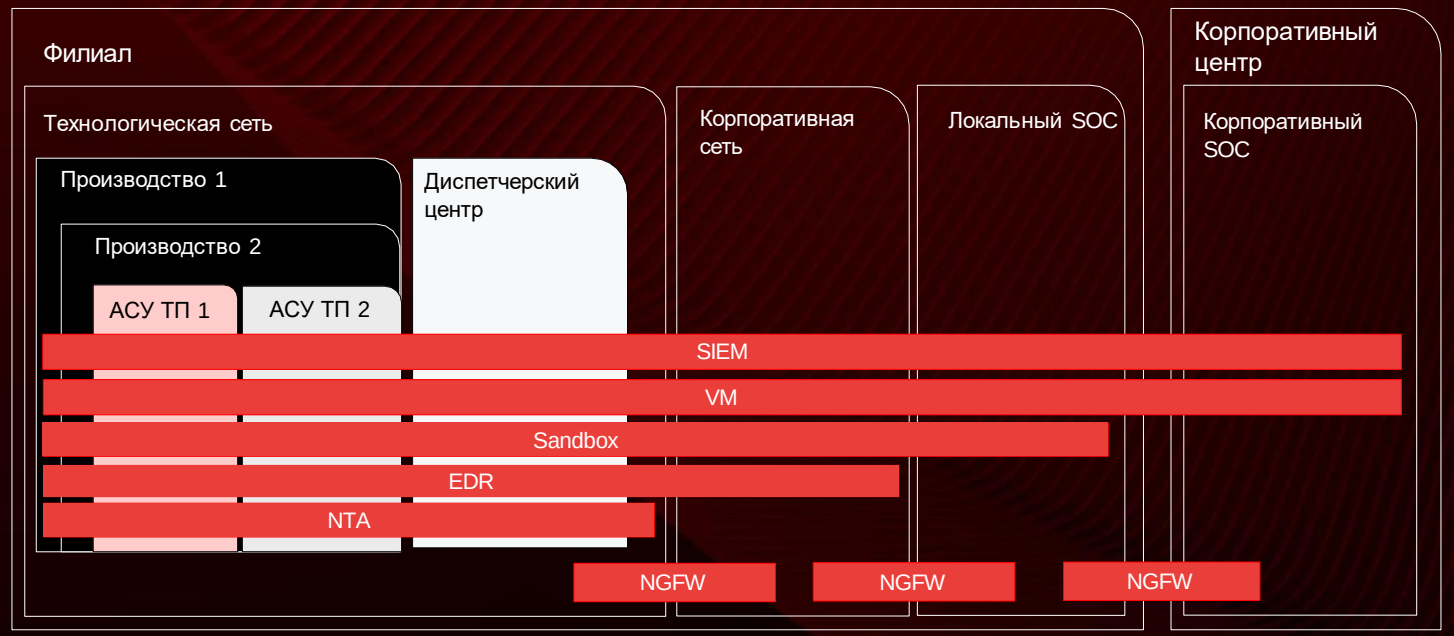


КСПД – корпоративная сеть передачи данных
ТСПД – технологическая сеть передачи данных
IT-инфраструктура –стандартные и бизнес системы
OT - инфраструктура – системы управления технологическими и производственными процессами

АСУ ТП - Автоматизированные системы управления технологическими процессами
РСУ – Распределённые Системы Управления
SCADA – Supervisory Control And Data Acquisition
АСДУ – Автоматизированная Система Диспетчерского управления

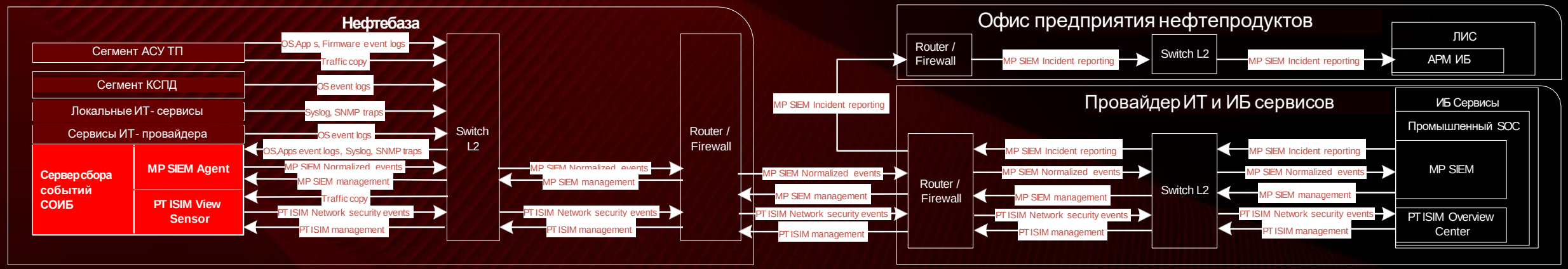
Базовая архитектура PT ICS

Уровень производственной инфраструктуры



- Сквозные процессы управления безопасностью во всей компании – от CISO до инженера эксплуатации АСУ и оперативного диспетчера
- Максимальная автоматизация процессов и операций управления безопасностью в масштабе всей компании
- Централизация всех функций управления безопасностью.

Пример решения для Нефтебазы



Сервер сбора событий СОИБ

- VM С прикладным ПО PT-MPSIEM-AGT-100
- VM С прикладным ПО PT ISIM netView Sensor
- Среда виртуализации ПК СВ Брест
- Операционная система Astra Linux 1.7 Special Edition

Техническое решение

Класс решения	СОИБ, SOC
Продукты	MP SIEM, Сертификат ФСТЭК №3734
	PT ISIM, Сертификат ФСТЭК №4182
Компоненты	PT MPSIEM-AGT-100
	PT ISIM netView Sensor
Форма поставки	ПАК
Объект лицензирования	Прикладное программное обеспечение
Срок действия лицензий	12 мес.
Уровень технической поддержки	Базовый

Пример решения для Нефтебазы

Функциональные возможности	Обнаружение аномалий, вторжений и кибератак	MP SIEM, PT ISIM
	Управление инцидентами безопасности в технологическом сети	MP SIEM, PT ISIM
Решаемые задачи безопасности	Мониторинг безопасности	MP SIEM, PT ISIM
	Обнаружение вторжений	MP SIEM, PT ISIM
	Защита ИТ-активов предприятия	MP SIEM, PT ISIM
	Предотвращение инцидентов и кибератак	MP SIEM, PT ISIM
	Реагирование на инциденты	MP SIEM, PT ISIM
Поддерживаемые процессы	Управление событиями	MP SIEM, PT ISIM
	Управление инцидентами	MP SIEM, PT ISIM
	Управление непрерывностью производственных и технологических процессов	MP SIEM, PT ISIM
Решаемые прикладные задачи	Контроль легитимности управляющих и сервисных команд	MP SIEM, PT ISIM
	Контроль легитимности и корректности пользовательских операций	MP SIEM, PT ISIM
	Контроль легитимности и корректности использования инженерного и диагностического ПО, среды разработки SCADA и PLC проектов	MP SIEM, PT ISIM
	Обнаружение попыток модификации критичный файлов, SCADA и PLC проектов	MP SIEM, PT ISIM
	Защита от деструктивных воздействий и операций изнутри и извне (саботаж, использование ресурсов не по назначению)	MP SIEM, PT ISIM
	Контроль целостности сети и сетевого обмена	PT ISIM
	Обнаружение подключение к внешним сетям и интернет	MP SIEM, PT ISIM
	Обнаружение подключения к сети новых сетевых узлов/хостов	PT ISIM
	Обнаружение подмены технологических данных (телеметрии, команд)	PT ISIM
	Ретроспективный анализ событий, инцидентов, изменений сети.	MP SIEM, PT ISIM

Пример решения для Нефтебазы

Обеспечение соответствия требованиям по защите ОКИИ*	Приме
АУД.1 Инвентаризация информационных ресурсов	PT ISIM
АУД.4 Регистрация событий безопасности	MP SIEM, PT ISIM
АУД.5 Контроль и анализ сетевого трафика	PT ISIM
АУД.6 Защита информации о событиях безопасности	MP SIEM, PT ISIM
АУД.7 Мониторинг безопасности	MP SIEM, PT ISIM
АУД.8 Реагирование на сбои при регистрации событий безопасности	MP SIEM, PT ISIM
АУД.10 Проведение внутренних аудитов	PT ISIM
СОВ.1 Обнаружение и предотвращение компьютерных атак	MP SIEM, PT ISIM
СОВ.2 Обновление базы решающих правил	MP SIEM, PT ISIM
ОДТ.3 Контроль безотказного функционирования средств и систем	MP SIEM, PT ISIM,
ОДТ.8 Контроль предоставляемых вычислительных ресурсов и каналов связи	MP SIEM, PT ISIM
ИНЦ.1 Выявление компьютерных инцидентов	MP SIEM, PT ISIM
ИНЦ.2 Информирование о компьютерных инцидентах	MP SIEM, PT ISIM
ИНЦ.3 Анализ компьютерных инцидентов	MP SIEM, PT ISIM
ИНЦ.4 Устранение последствий компьютерных инцидентов	MP SIEM
ИНЦ.5 Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	MP SIEM, PT ISIM
ИНЦ.6 Хранение и защита информации о компьютерных инцидентах	MP SIEM, PT ISIM
УКФ.4 Контроль действий по внесению изменений	MP SIEM, PT ISIM
ПЛН.2 Контроль выполнения мероприятий по обеспечению защиты информации	MP SIEM
ДНС.6 Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	MP SIEM, PT ISIM,

*в соответствии с положениями Приказа ФСТЭК №239 от 25 декабря 2017 г.

PT ISIM
Страница на сайте
ptsecurity.com

PT ICS
Подписывайтесь
на телеграм-канал
продукта

Дмитрий Даренский
Руководитель практики промышленной кибербезопасности
Positive Technologies

Спасибо!