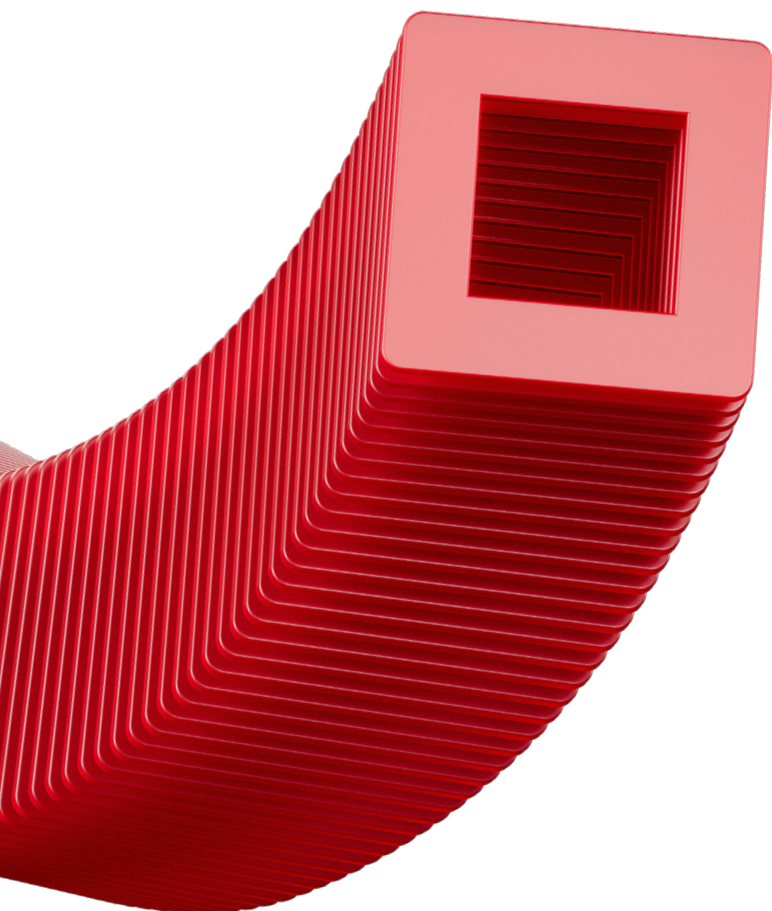




Промышленная экспертиза для **MaxPatrol SIEM**

MaxPatrol SIEM — компонент
PT Industrial Cybersecurity Suite

MaxPatrol SIEM выявляет инциденты ИБ, ведущие к реализации недопустимых событий, и попытки нарушения киберустойчивости компании.

Пакет промышленной экспертизы позволяет **MaxPatrol SIEM** обрабатывать события на уровне прикладного программного обеспечения SCADA и инженерного ПО систем промышленной автоматизации. Благодаря этому **MaxPatrol SIEM** обнаруживает инциденты, некорректные или ошибочные действия эксплуатационного и оперативного персонала и подрядных организаций, способные повлиять на целостность и работоспособность АСУ ТП

Промышленная экспертиза — это правила нормализации и корреляции событий, собираемых с прикладного уровня систем АСУ ТП: серверов SCADA, инженерных рабочих станций

MaxPatrol SIEM в промышленных инфраструктурах

MaxPatrol SIEM с пакетом промышленной экспертизы позволяет выявлять:



Подмену файлов мнемосхемы (проекта) на сервере SCADA



Удаление файлов журналов на сервере SCADA



Неудачные попытки входа пользователя (забытый пароль или брутфорс)



Запуск и остановка ключевых сервисов SCADA-сервера



Подозрительные и опасные операции пользователей в SCADA и инженерном ПО

Возможности **MaxPatrol SIEM**

Контролирует качество настройки системы с помощью встроенного чек-листа

Автоматически заносит в белый список легитимные срабатывания

Отслеживает состояние ИБ в крупных иерархических инфраструктурах

Содержит правила корреляции для популярных АСУ ТП

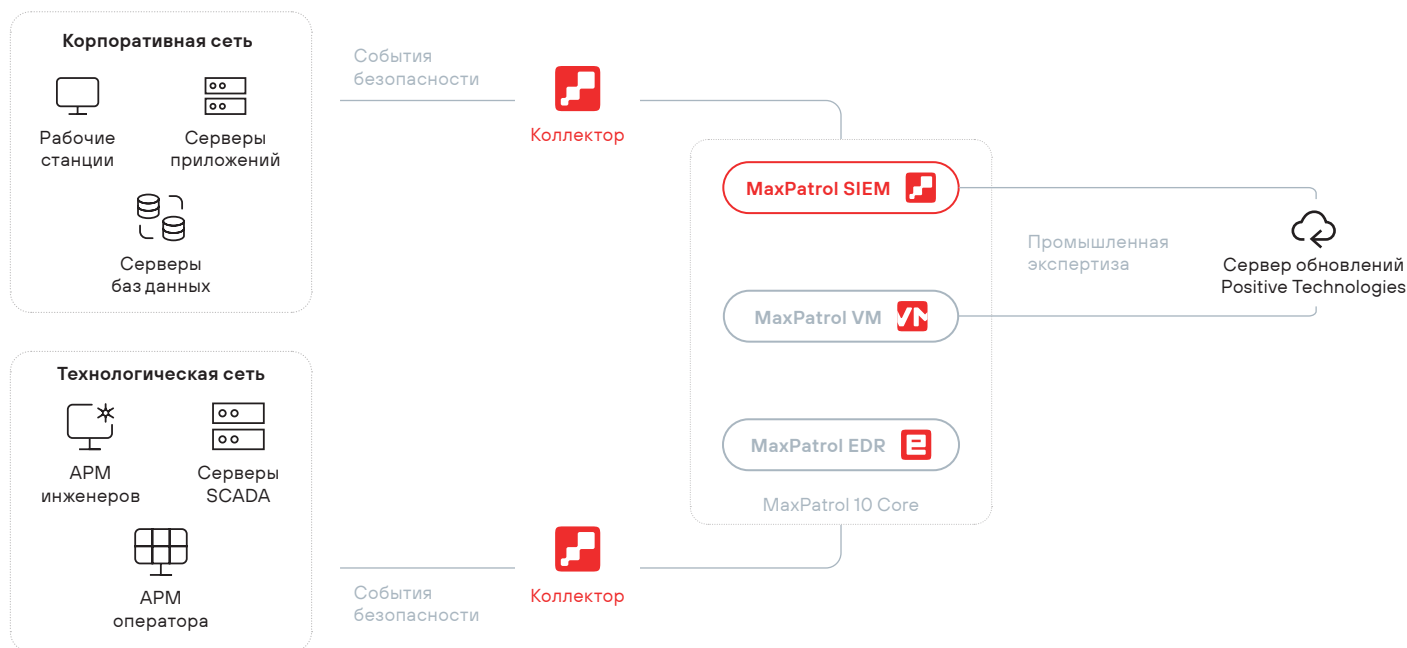
Помогает проверять гипотезы через просмотр связанных корреляционных событий

Видит корпоративную и промышленную инфраструктуру

Позволяет создавать собственные правила корреляции с помощью гибкого конструктора

Ищет данные в сторонних системах и сервисах прямо из карточки события

Пример установки **MaxPatrol SIEM** в технологической сети (ТСПД)



Пакеты промышленной экспертизы распространяются отдельно, их можно догружать в действующие инсталляции **MaxPatrol SIEM**

Для этого нужно:

1. Приобрести одну из лицензий Industrial коллекторов (с префиксом IND)
2. Запросить пакет через портал технической поддержки.

Пакет экспертизы — это файл с расширением .kb. Он содержит правила корреляции событий прикладного уровня для определенной системы конкретной версии, инструкцию по настройке и информацию о пакете.

Поддерживаемые **российские** АСУ ТП

Производитель	Продукт
AdAstrA	SCADA TRACE MODE 6
«Атомик Софт»	«Альфа платформа»
«МПС софт»	MasterSCADA 3.12
«ПРОСОФТ»	AstraRegul
«РЕДКИТ ЛАБ»	Redkit SCADA 2.0

Поддерживаемые **иностранные** АСУ ТП

Производитель	Продукт
AVEVA	Wonderware System Platform 2014, 2017
Siemens	SIMATIC STEP 7 v5
	SIMATIC TIA Portal Advanced/Pro 15.1*
	SIMATIC TIA Portal Basic 15.1*
	SIMATIC WinCC 7.4*
	SIMATIC WinCC flexible 2007–2008
Yokogawa	CENTUM VP R4–R6
	ProSafe-RS R2–R4



Заходите
в телеграм-чат
PT ICS



Отправьте заявку
на пилотный проект

