positive technologies

Промышленная экспертиза для MaxPatrol SIEM

MaxPatrol SIEM — компонент
PT Industrial Cybersecurity Suite

ВОЗМОЖНОСТИ MAXPATROL SIEM

Отслеживает состояние ИБ в крупных иерархических инфраструктурах

Видит корпоративную и промышленную инфраструктуру

Контролирует качество настройки системы с помощью встроенного чек-листа

Содержит правила корреляции для популярных АСУ ТП

Позволяет создавать собственные правила корреляции с помощью гибкого конструктора

Автоматически заносит в белый список легитимные срабатывания

Помогает проверять гипотезы через просмотр связанных корреляционных событий

Ищет данные в сторонних системах и сервисах прямо из карточки события

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

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

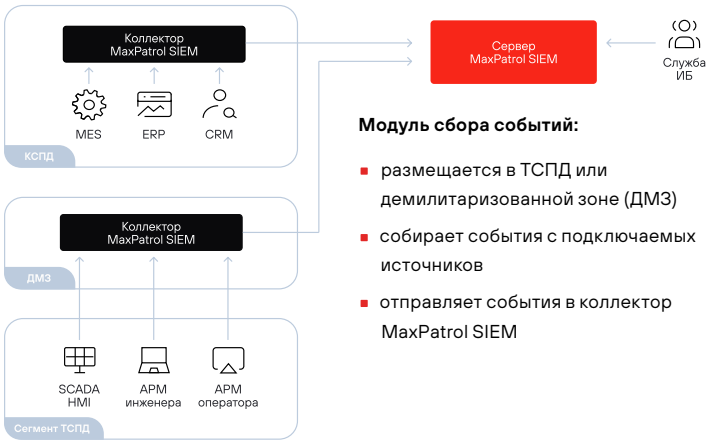
Промышленная экспертиза — это набор правил и сценариев обработки событий, собираемых из протоколов передачи данных, журналов операционных систем, прикладного программного обеспечения АСУ ТП, контроллеров, инженерного ПО, а также данные об известных уязвимостях.

MaxPatrol SIEM в промышленных инфраструктурах

MaxPatrol SIEM с пакетом промышленной экспертизы позволяет выявлять:

- подмену файлов мнемосхемы (проекта) на сервере SCADA
- удаление лог-файлов на сервере SCADA
- неудачные попытки входа пользователя (забытый пароль или брутфорс)
- запуск и останов ключевых сервисов SCADA-сервера
- подозрительные и опасные операции пользователей в SCADA и инженерном ПО

Пример установки MaxPatrol SIEM в технологической сети (ТСПД)



Модуль сбора событий:

- размещается в ТСПД или демилитаризованной зоне (ДМЗ)
- собирает события с подключаемых источников
- отправляет события в коллектор MaxPatrol SIEM

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 АСУТП конкретной версии, инструкцию по настройке и информацию о пакете.

Поддерживаемые российские АСУ ТП

Производитель	Продукт
AdAstrA	SCADA TRACE MODE 6
Атомик Софт	Alpha.Platform (появится в 1-ой половине 2024 года)
МПС софт	MasterSCADA 3.12
ПРОСОФТ	Regul (появится в 1-ой половине 2024 года)

Поддерживаемые иностранные АСУ ТП

Производитель	Продукт
AVEVA	Wonderware System Platform 2014, 2017
Siemens	SIMATIC STEP 7 5.x
	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

ptsecurity.com
pr@ptsecurity.com

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400».

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 200 тысяч акционеров.

Следите за нами в соцсетях (Telegram, ВКонтакте, Twitter, Хабр) и в разделе «Новости» на сайте ptsecurity.com, а также подписывайтесь на телеграм-канал IT's positive investing.

MaxPatrol SIEM_EXP_A4.0002.01.JAN.17.2024