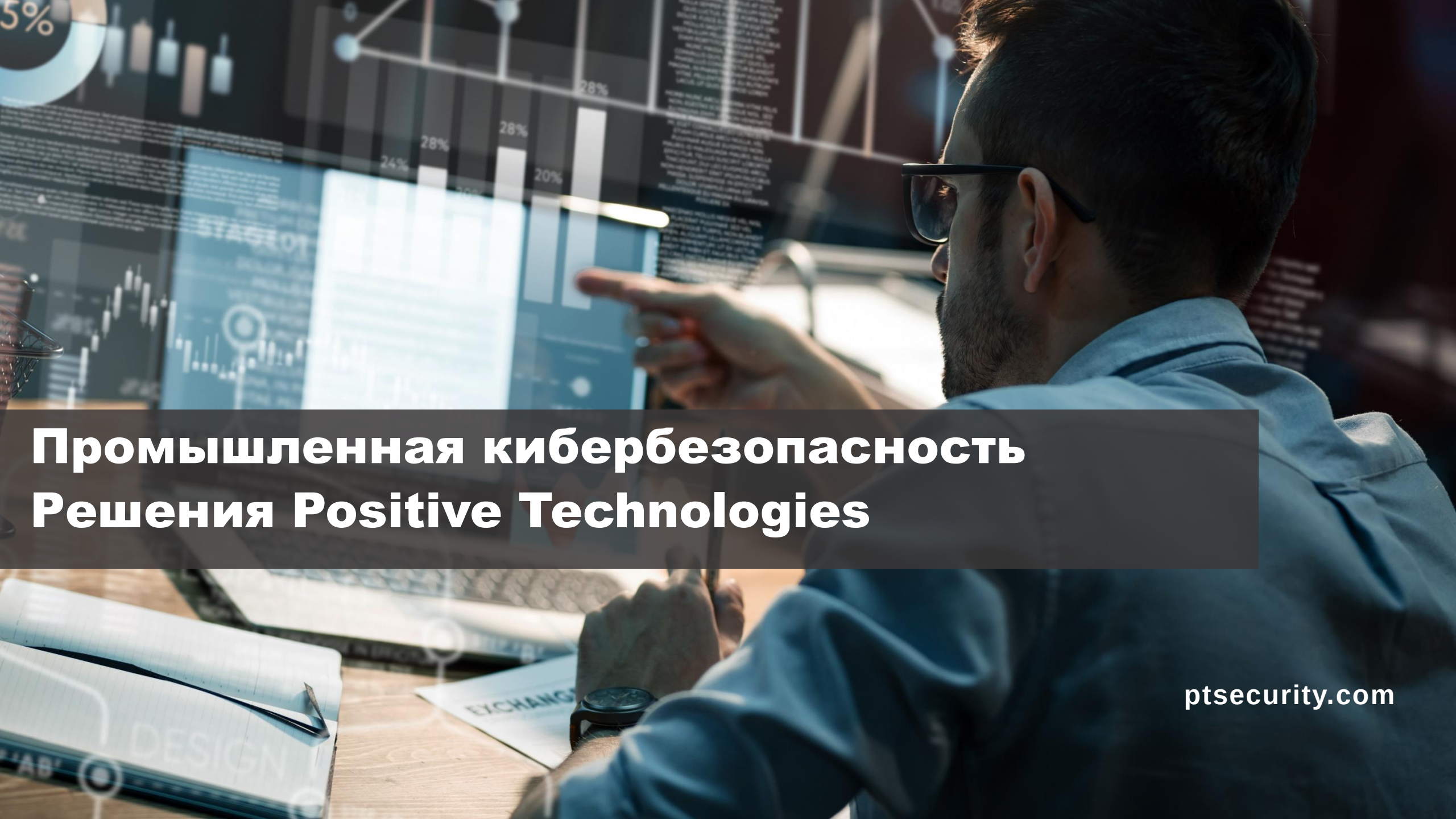


Промышленная кибербезопасность
Решения Positive Technologies

ptsecurity.com

Обеспечиваем **практическую** кибербезопасность бизнеса

18 лет
исследований
и опыта в обеспечении
кибербезопасности

500+
экспертов в крупнейшем
исследовательском
центре в Европе

9 продуктов
для мониторинга
и обеспечения ИБ в нашем
портфолио

в 3 раза
быстрее растем по
сравнению с рынком
в России

80%
отечественных компаний
из списка **Expert 400**
используют наши продукты

9 лет
проводим самые
крупные в Европе
открытые киберучения

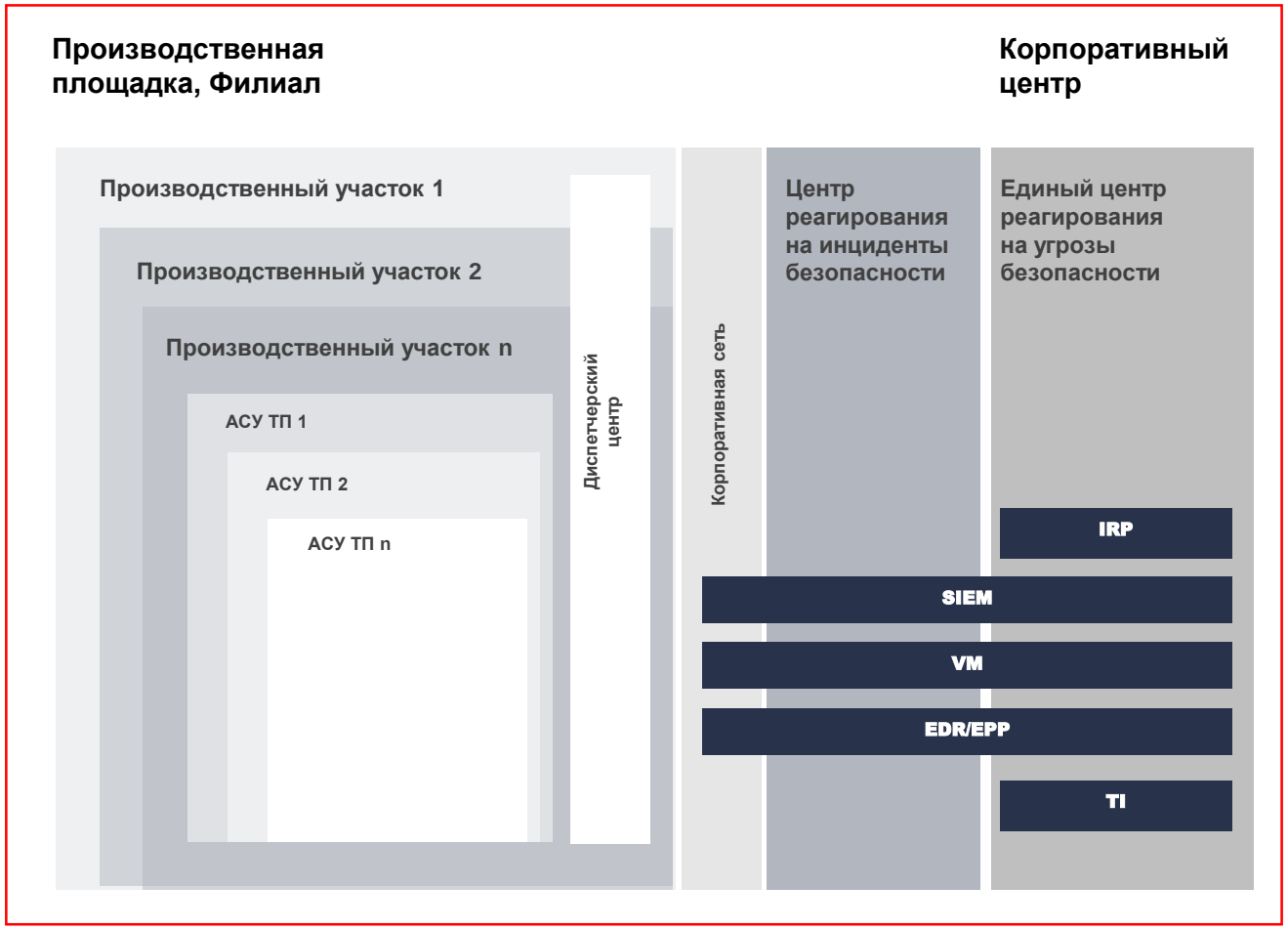
Наши клиенты

Проекты в промышленности на базе PT Industrial Cyber Security Solutions

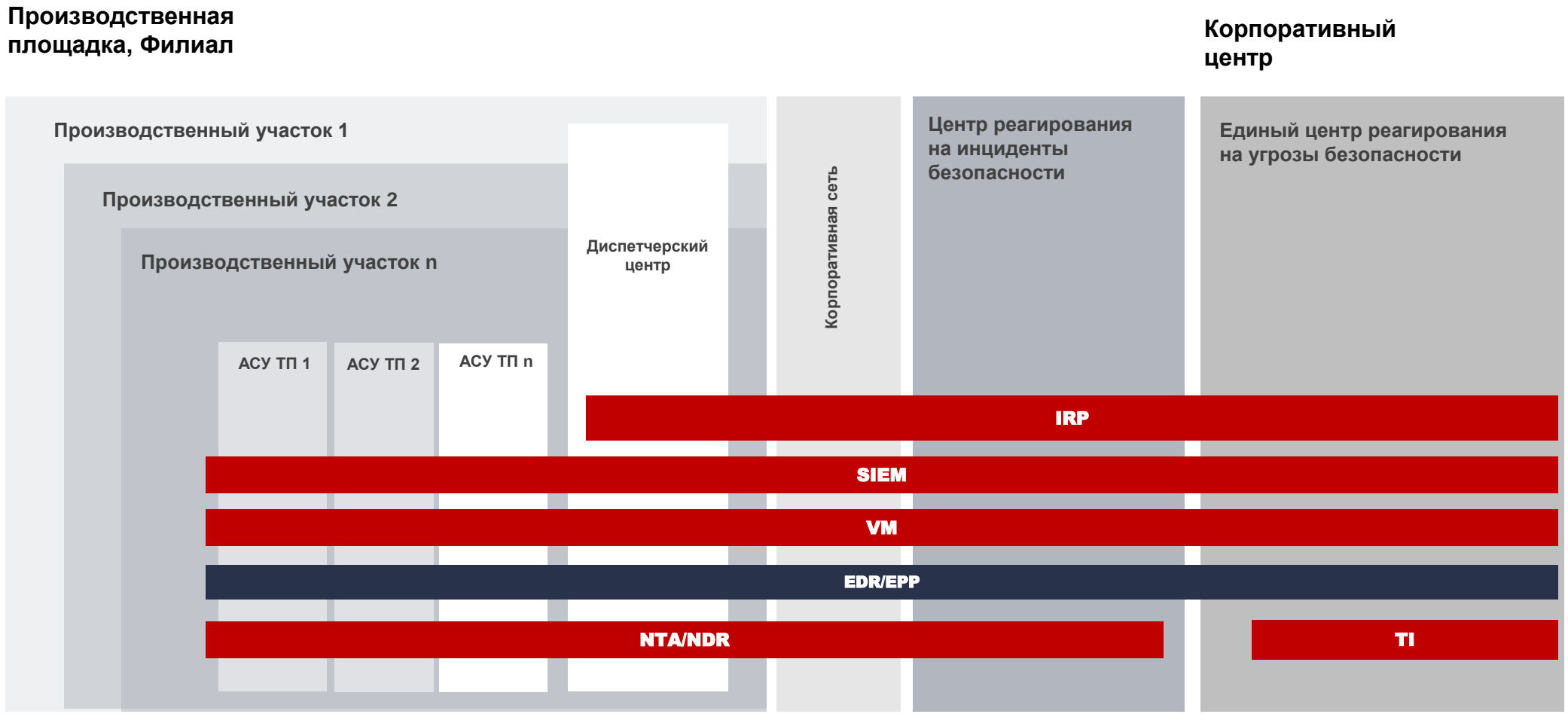
Mining		2 горнодобывающих & 2 металлургических предприятия 1 SOC в 2 металлургических компаниях
Power Generation		60+ электростанций 2 SOC в 2 энергокомпаниях
Hydropower Generation		30+ гидроэлектростанций 2 SOC в 2 гидрогенерирующих компаниях
Power Grids		20+ подстанций 220/110 kV 3 SOC в 3 электросетевых компаниях
Data Centers		1 Дата Центр в национальном телеком провайдере
Railways		100+ железнодорожных станций по всей стране

Технологическая сеть как объект защиты для SOC

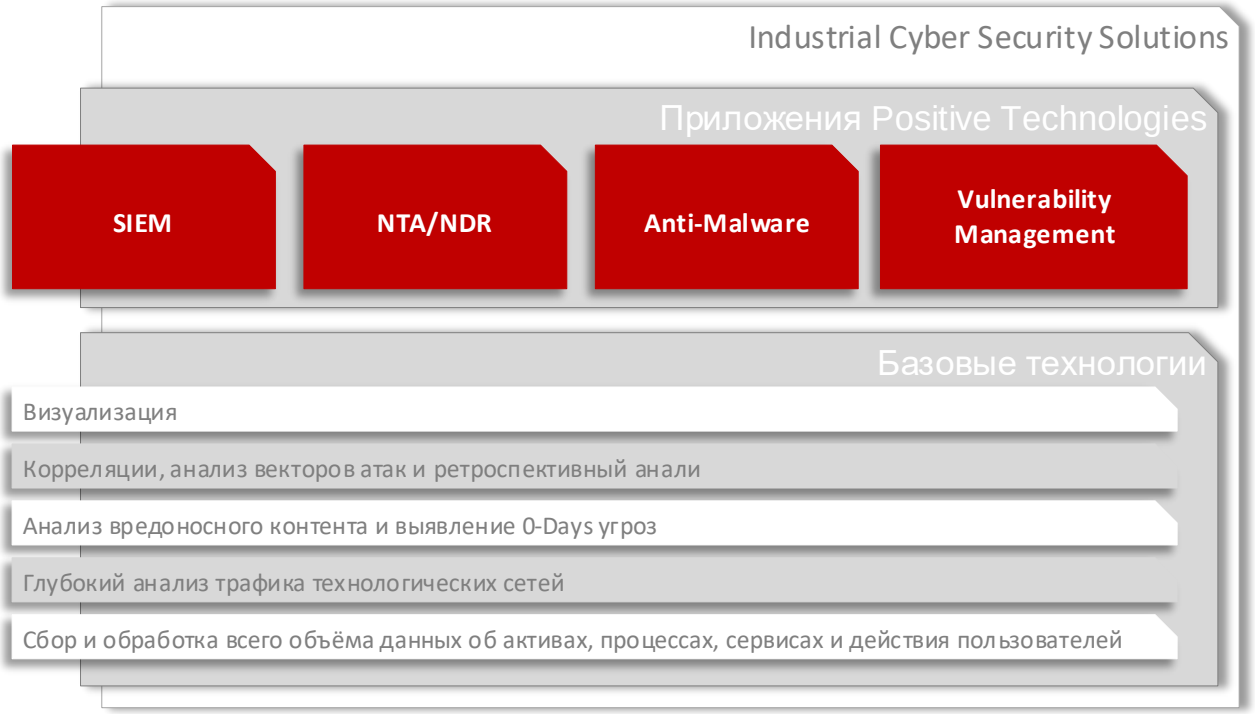
- АСУ ТП – остается серой зоной для Security Operations Center
- Требуется инструмент, делающий происходящее в технологической сети прозрачным
- Необходимы данные о технологических аспектах работы для контроля бизнес-рисков



Комплексный подход к построению Industrial SOC



Positive Industrial Cyber Security Solutions



Основные возможности

Обнаружение сетевых, процессных и операционных аномалий в OT/IT

Обнаружение кибератак

Контроль изменений инфраструктуры и конфигурациях активов в OT/IT сегментах

Непрерывное управление уязвимостями, анализ защищенности и соответствия политикам безопасности

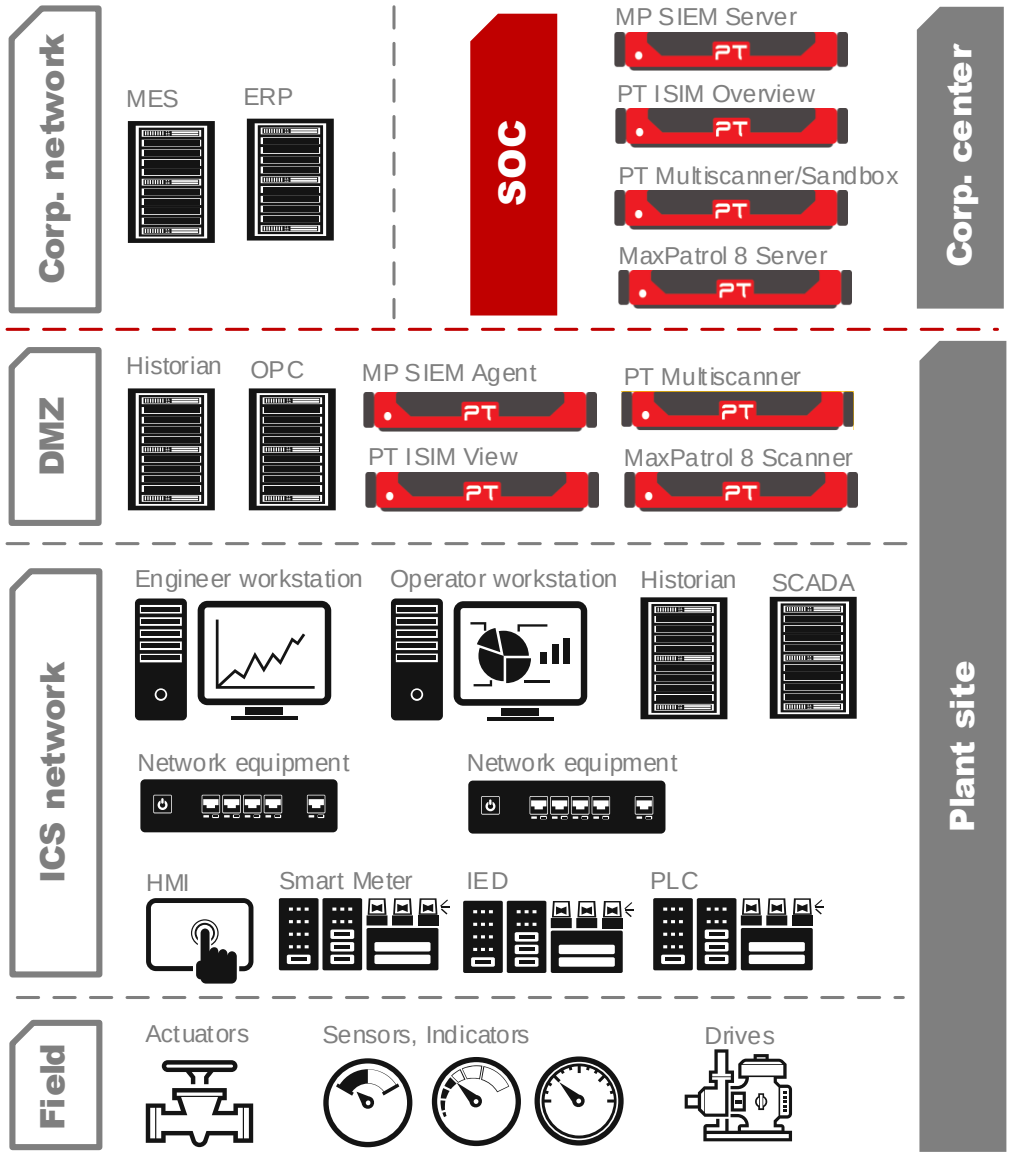
Расширенная непрерывная визуализация и отчетность

Мониторинг защищенности OT/IT сегментов, управление инцидентами

Архитектура

Программные компоненты решений

SIEM	**MaxPatrol SIEM**
NTA/NDR	**PT ISIM**
Anti-Malware	**PT MultiSanner**
Vulnerability Management	**MaxPatrol 8**



Use cases

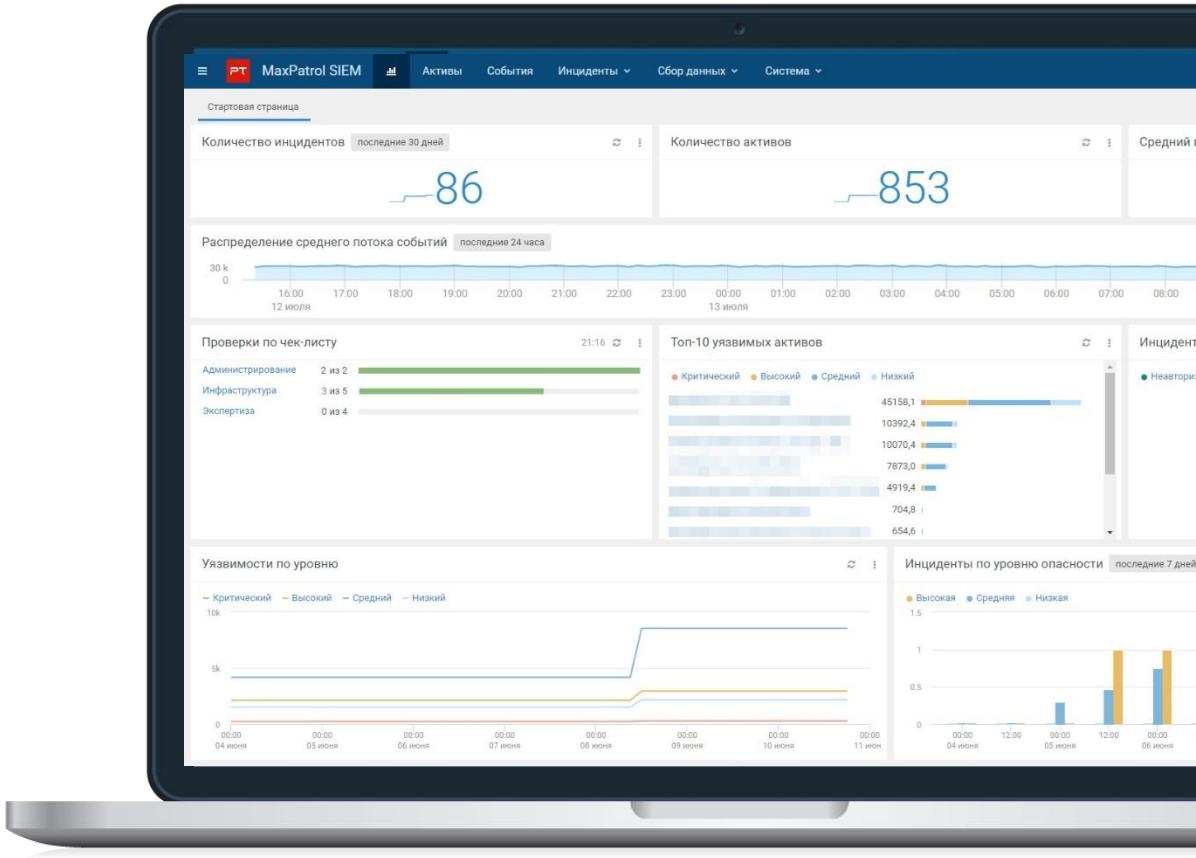
Incident Cases	Event & Data Sources	PT Solution components
Использование USB-устройств на АРМах АСУ ТП	Microsoft System Monitoring	MaxPatrol SIEM
Эксплуатация уязвимостей ассетов АСУ ТП	ПЛК/RTU/IED, SCADA/Historian Network traffic, Microsoft System Monitoring	MaxPatrol 8 MaxPatrol SIEM PT ISIM PT MultiScanner
Изменение технико-экономических показателей и мошенничество	ПЛК/RTU/IED, SCADA/Historian Predictive Analysis Systems	MaxPatrol SIEM PT ISIM PT MultiScanner
Неавторизованное изменение проектов SCADA и ПЛК	ПЛК/RTU/IED, SCADA/Historian, Network traffic, Microsoft System Monitoring	MaxPatrol SIEM PT ISIM PT MultiScanner
Неавторизованное изменение конфигураций и настроек ассетов SCADA и ПЛК	ПЛК/RTU/IED, SCADA/Historian, Network traffic Microsoft System Monitoring, Network equipment firmware	MaxPatrol SIEM PT ISIM PT MultiScanner
ВПО в сети АСУ ТП	Network traffic, Anti-Malware Systems	MaxPatrol SIEM PT ISIM PT MultiScanner
НСД к системам управления и технологической информации	СКУД, Machine Vision Systems, Network traffic, Microsoft System Monitoring, Network equipment firmware	MaxPatrol 8 MaxPatrol SIEM PT ISIM
Аномалии сетевого и прикладного уровня	SCADA/Historian, Predictive Analysis Systems Network traffic, Microsoft System Monitoring	MaxPatrol SIEM PT ISIM PT MultiScanner
Нарушения регламента эксплуатации технологических установок и ПТБ	СКУД, MachineVision, Field Workforce Management	MaxPatrol SIEM

MaxPatrol SIEM

MaxPatrol SIEM

Система выявления инцидентов с уникальным подходом к обеспечению прозрачности IT-инфраструктуры и глубокой экспертизой в обнаружении угроз

- Дает полную видимость IT-инфраструктуры
- Позволяет выявлять самые актуальные угрозы
- Снижает трудозатраты специалистов по ИБ на мониторинг состояния инфраструктуры и написание правил

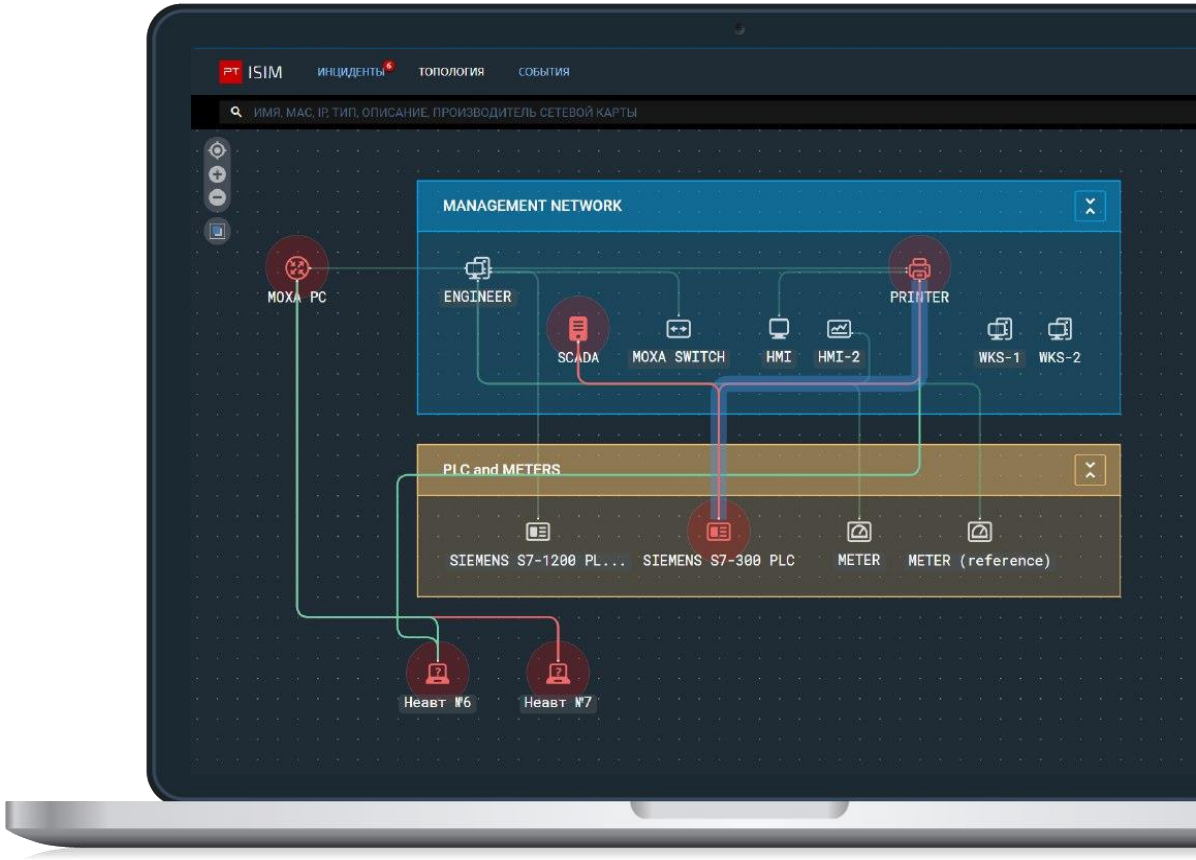


PT ISIM

PT ISIM

Программно-аппаратный комплекс анализа трафика технологических сетей АСУ ТП

- Помогает на ранней стадии выявлять кибератаки и неавторизованные действия персонала
- Позволяет контролировать векторы атак и соблюдение политик ИБ, специфических для конкретного промышленного объекта

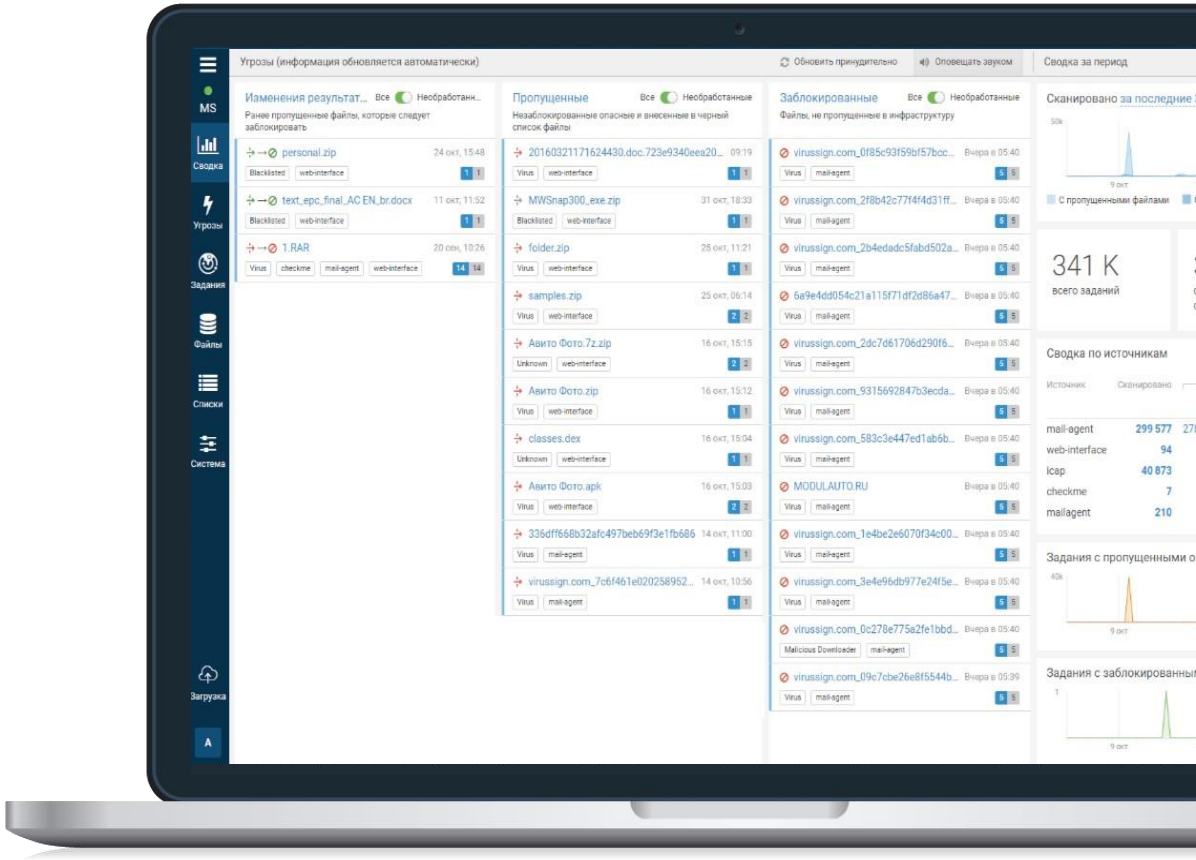


PT MultiScanner

PT MultiScanner

Многоуровневая система защиты от всех типов вредоносных программ

- Обеспечивает защиту от вирусных угроз с помощью мультивендорной антивирусной проверки
- Позволяет быстро локализовывать и устранять угрозы благодаря подробной информации о пораженных узлах



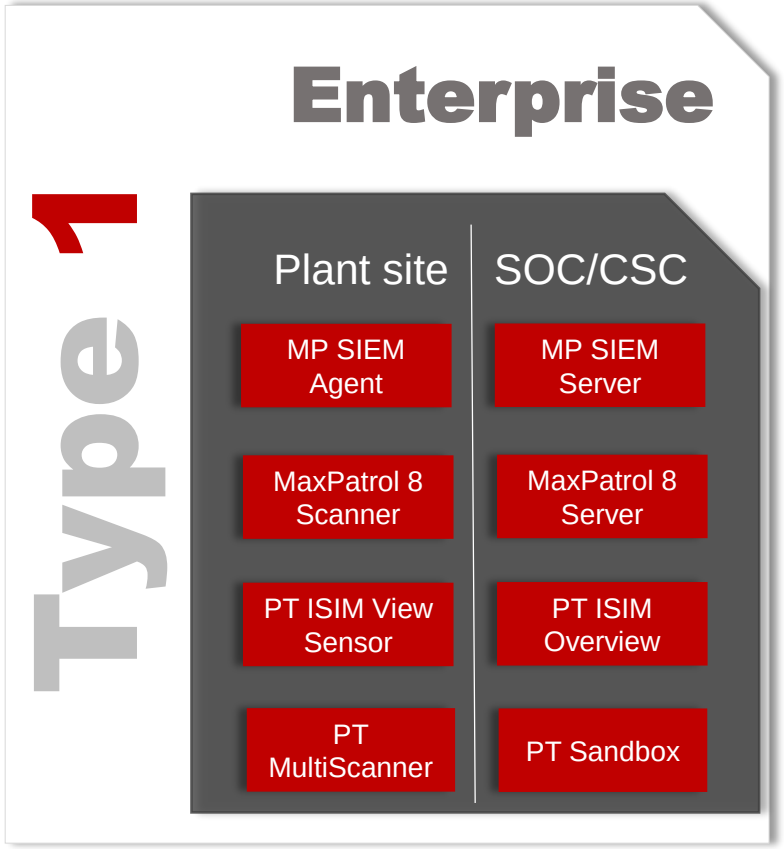
MaxPatrol 8

MaxPatrol 8

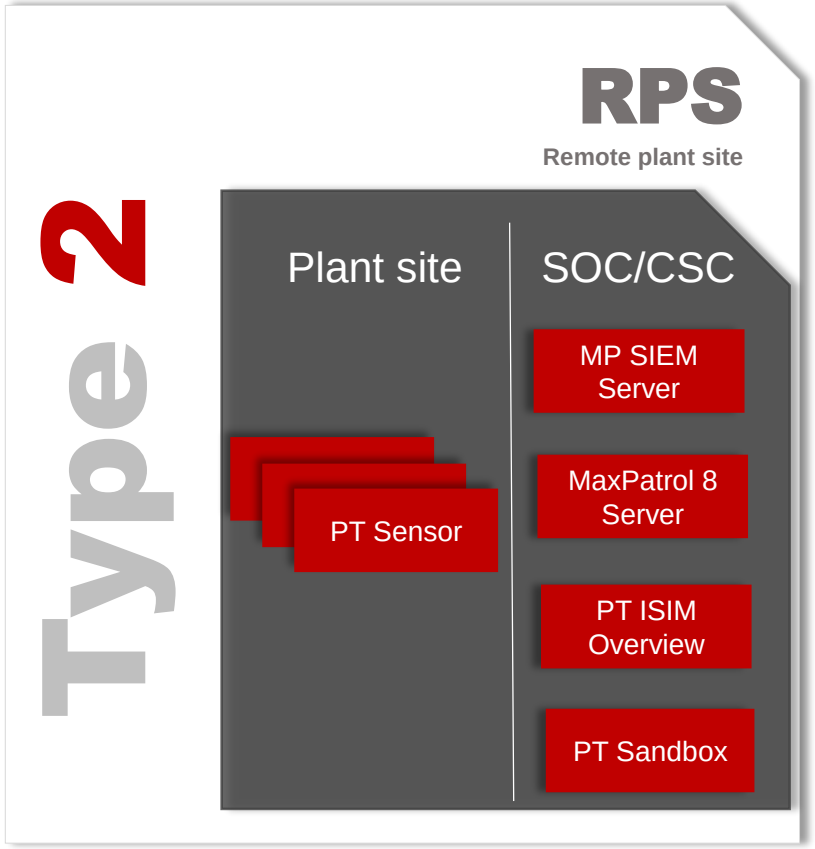
Универсальное средство автоматизированного анализа защищенности и контроля соответствия стандартам

- Позволяет регулярно и комплексно контролировать состояние защищенности всей IT-инфраструктуры
- Позволяет построить процесс управления уязвимостями на KPI, прозрачных для руководства
- Гибко масштабируется и подходит как для небольших компаний, так и для крупных территориально-распределенных предприятий

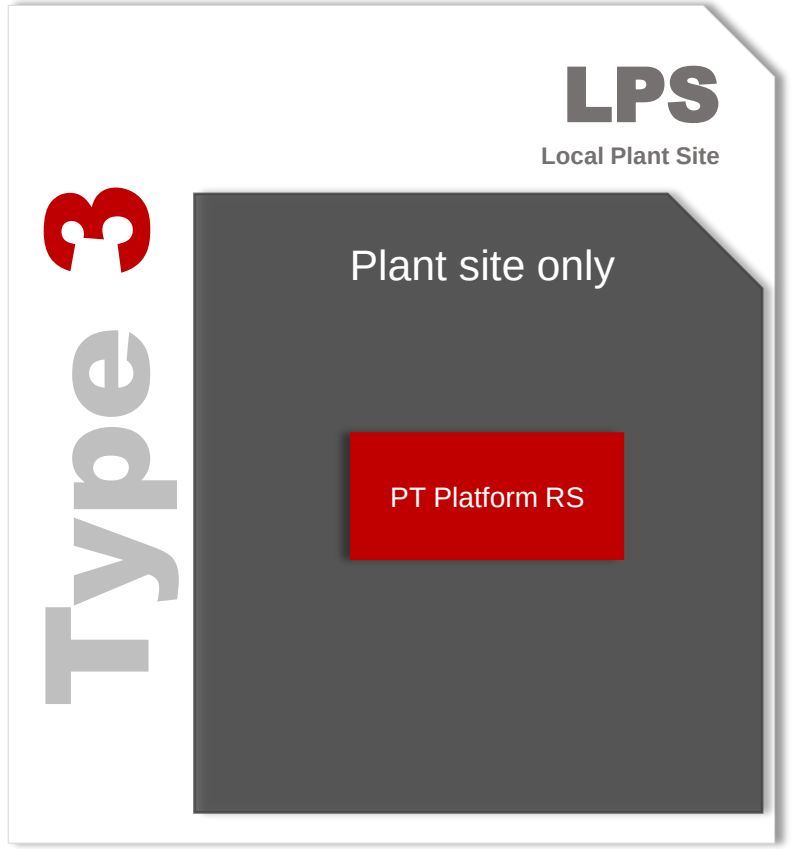
Типовые архитектуры решений



Для крупных промышленных компаний с филиальной структурой и большими пром. площадками

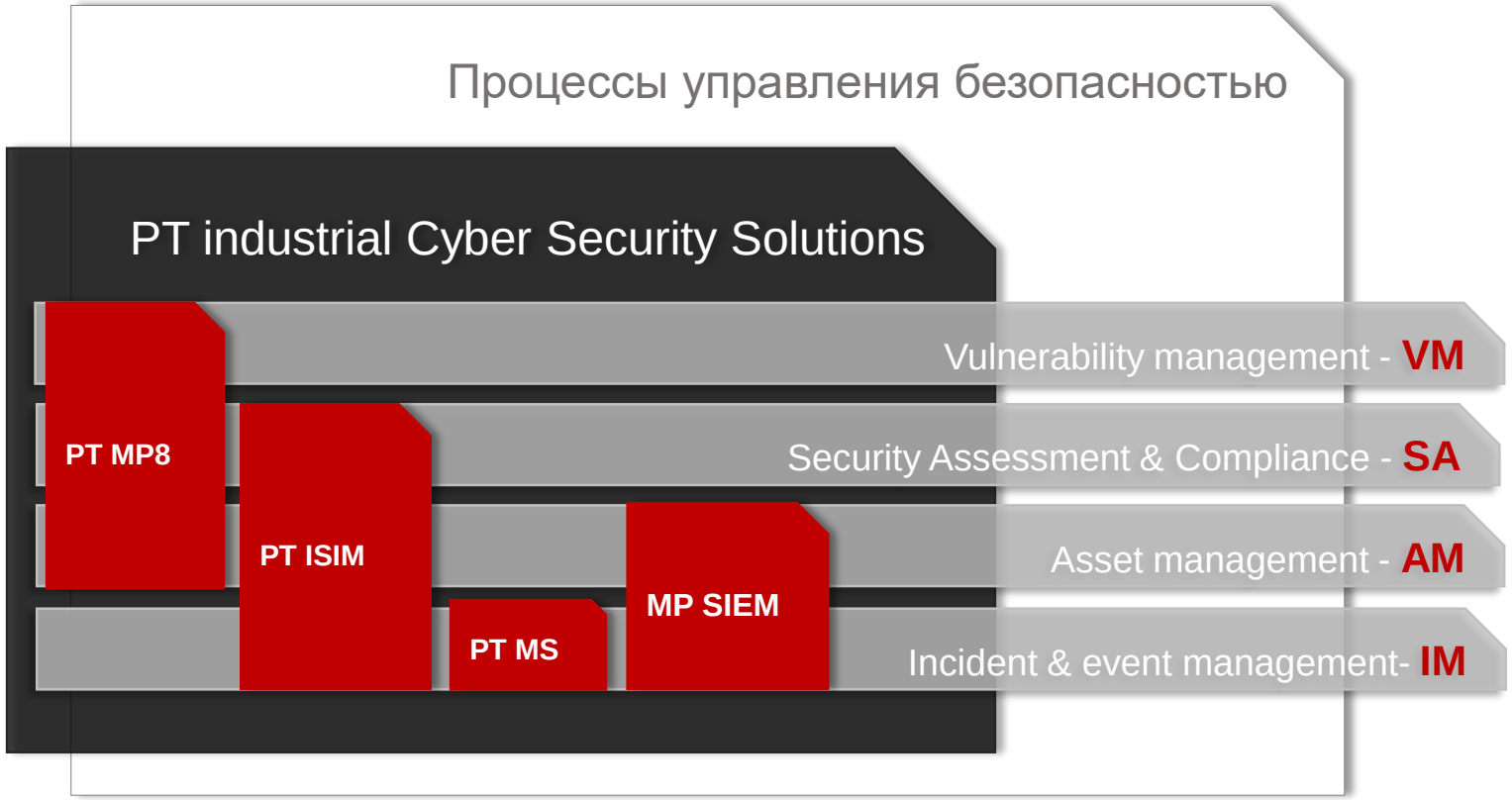


Для крупных и средних промышленных компаний с распределённой инфраструктурой небольших или не обслуживаемых пром. площадок



Для средних и небольших промышленных компаний или филиалов с локальными пром. площадками

Процессы управления безопасностью



Услуги

мониторинг и реагирование на инциденты ИБ

Positive Technologies Expert Security Center — экспертное подразделение, оказывающее услуги по реагированию, расследованию инцидентов и мониторингу защищенности корпоративных систем на базе продуктов PT.

В основе наших услуг более 15 лет опыта в анализе защищенности, расследовании инцидентов и деятельности крупнейших APT-группировок, а также мониторинга безопасности крупных компаний.

Мониторинг периметра

Поможет непрерывно выявлять проблемы, возникающие на сетевом периметре компании

Ретроспективный анализ и поиск ледов компрометации

Выявит следы подготовки к хакерской атаке и признаки компрометации инфраструктуры

Реагирование и расследование

Поможет оперативно локализовать угрозу и быстро восстановить работу бизнеса

Лицензии на деятельность

- **Positive Technologies** — лицензиат ФСТЭК, ФСБ Министерства обороны РФ
- **Продукты сертифицированы** ФСТЭК, Министерством обороны РФ, Газпромсерт
- **Продукты компании** в Едином реестре Российского ПО

Свяжитесь с нами:

t: +7 495 744 01 44

sales@ptsecurity.com

ptsecurity.com