Positive Technologies Industrial Cybersecurity Suite

ptsecurity.com

Дмитрий Даренский

руководитель практики промышленной кибербезопасности

ddarensky@ptsecurity.com

- Образование: автоматизация технологических процессов и производств
- 15 лет опыта строительства технологических сетей и систем связи
- 10 лет опыта создания систем АСУ ТП, ТМ, АСТУЭ, АСКУЭ, СДТУ
- 8 лет опыта создания комплексных систем безопасности в промышленности

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

Эффективная кибербезопасность промышленных предприятий

- Предотвращение недопустимых производственных рисков и событий
- Централизация процессов управления кибербезопасностью предприятия
- Управление производственными и операционными рисками с учетом угроз кибербезопасности в масштабе всей Компании

Путь к практической кибербезопасности

1.

СЦЕНАРНЫЙ АНАЛИЗ И ОПРЕДЕЛЕНИЕ УЩЕРБА

Определение ключевых рисков и недопустимых событий ИБ, а также целей и принципов развития ИБ

2.

АНАЛИЗ РИСКОВ ИТ-ИНФРАСТРУКТУРЫ И АСУ ТП

Определение фактических причин реализации недопустимых событий и формирование эскизной модели ИБ

3.

ФОРМИРОВАНИЕ КОНЦЕПЦИИ РАЗВИТИЯ ИБ

Разработка концепции обеспечения ИБ и маршрутной карты развития ИБ

4.

КИБЕРУЧЕНИЯ И ПОВЫШЕНИЕ УСТОЙЧИВОСТИ

Внедрение мер и средств, исключающих недопустимые для бизнеса события, проведение киберучений

Positive Industrial Cybersecurity Suite

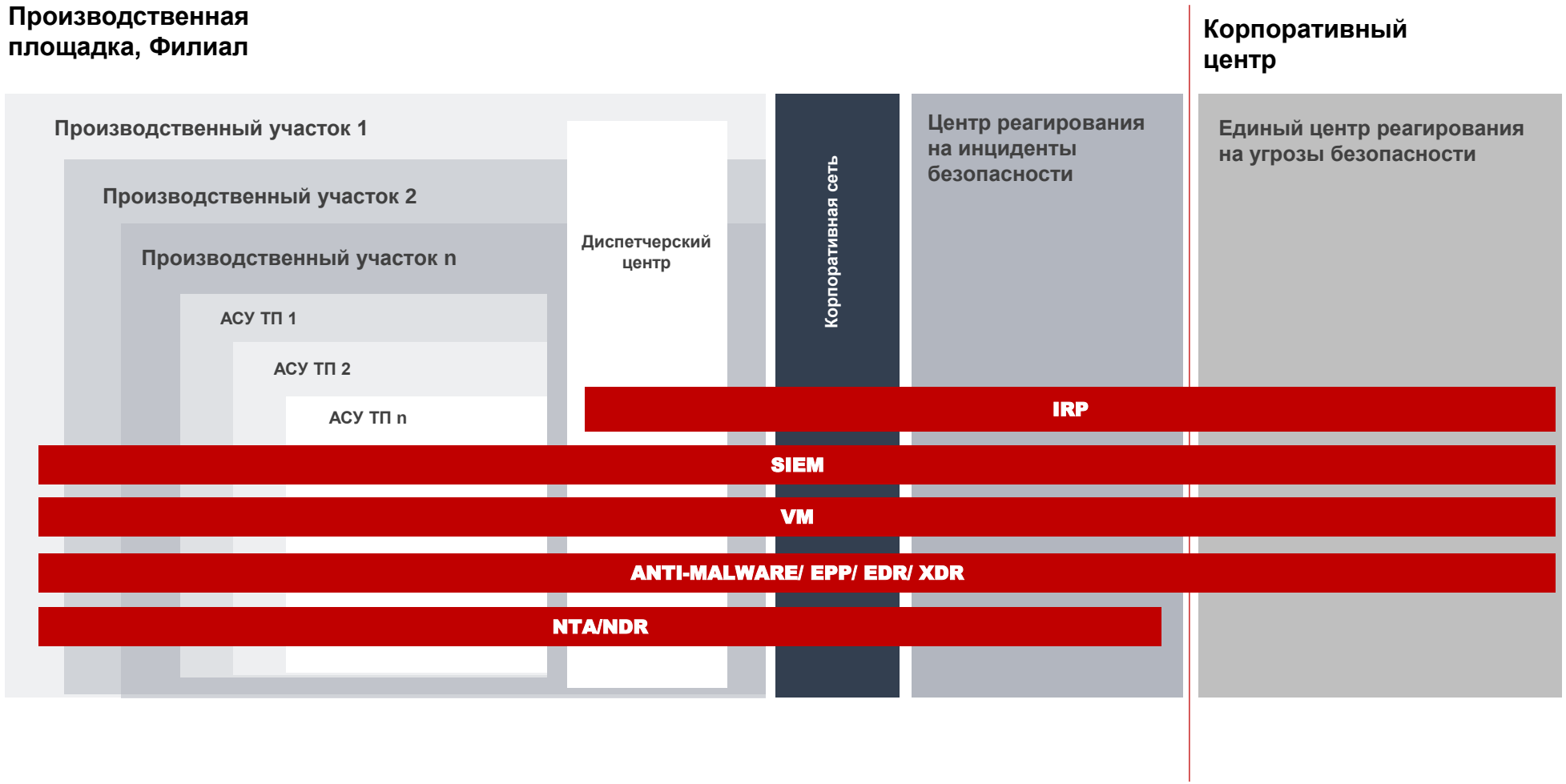
Основные возможности

- **Автоматизация с перспективой роботизации** базовых процессов управления кибербезопасностью
- Расширенная непрерывная визуализация, отчетность
- Обнаружение кибератак **с минимизацией ручного труда**
- Мониторинг защищенности OT/IT сегментов, управление инцидентами
- Обнаружение сетевых, поведенческих и операционных аномалий в OT/IT
- Непрерывное управление уязвимостями, анализ защищенности и соответствия политикам безопасности
- Контроль изменений инфраструктуры и конфигурациях активов в OT/IT сегментах

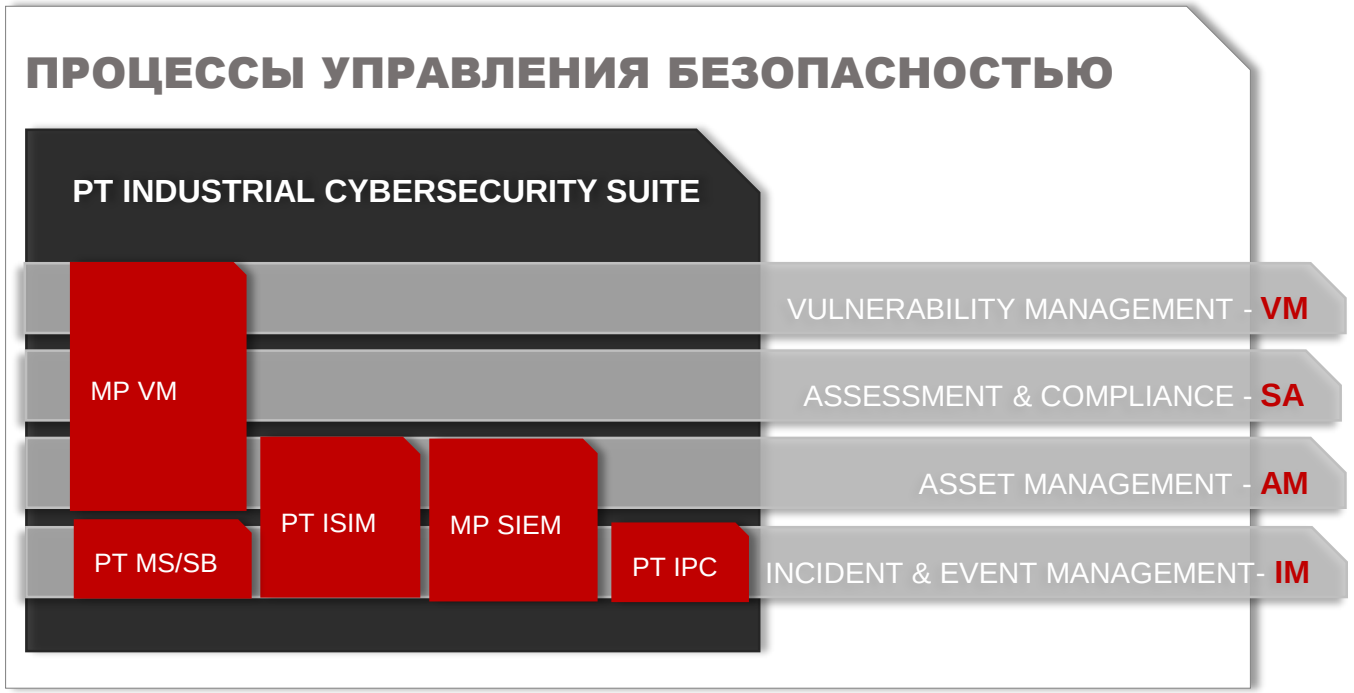
Структура решений

INDUSTRIAL CYBERSECURITY SUITE APPLICATIONS		Функциональное назначение
IRP	PT IPC	Управление процессами обнаружения и реагирования на инциденты
SIEM	MAXPATROL SIEM	Управление событиями и инцидентами безопасности
NTA/NDR	PT ISIM	Глубокий анализ трафика технологических сетей, выявление аномалий
Anti-Malware	PT MULTISCANNER / SANDBOX	Обнаружение вредоносного контента в трафике и ИТ-системах
Vulnerability Management	MAXPATROL VM	Управление уязвимостями и патч-менеджмент

Покрытие инфраструктуры предприятия



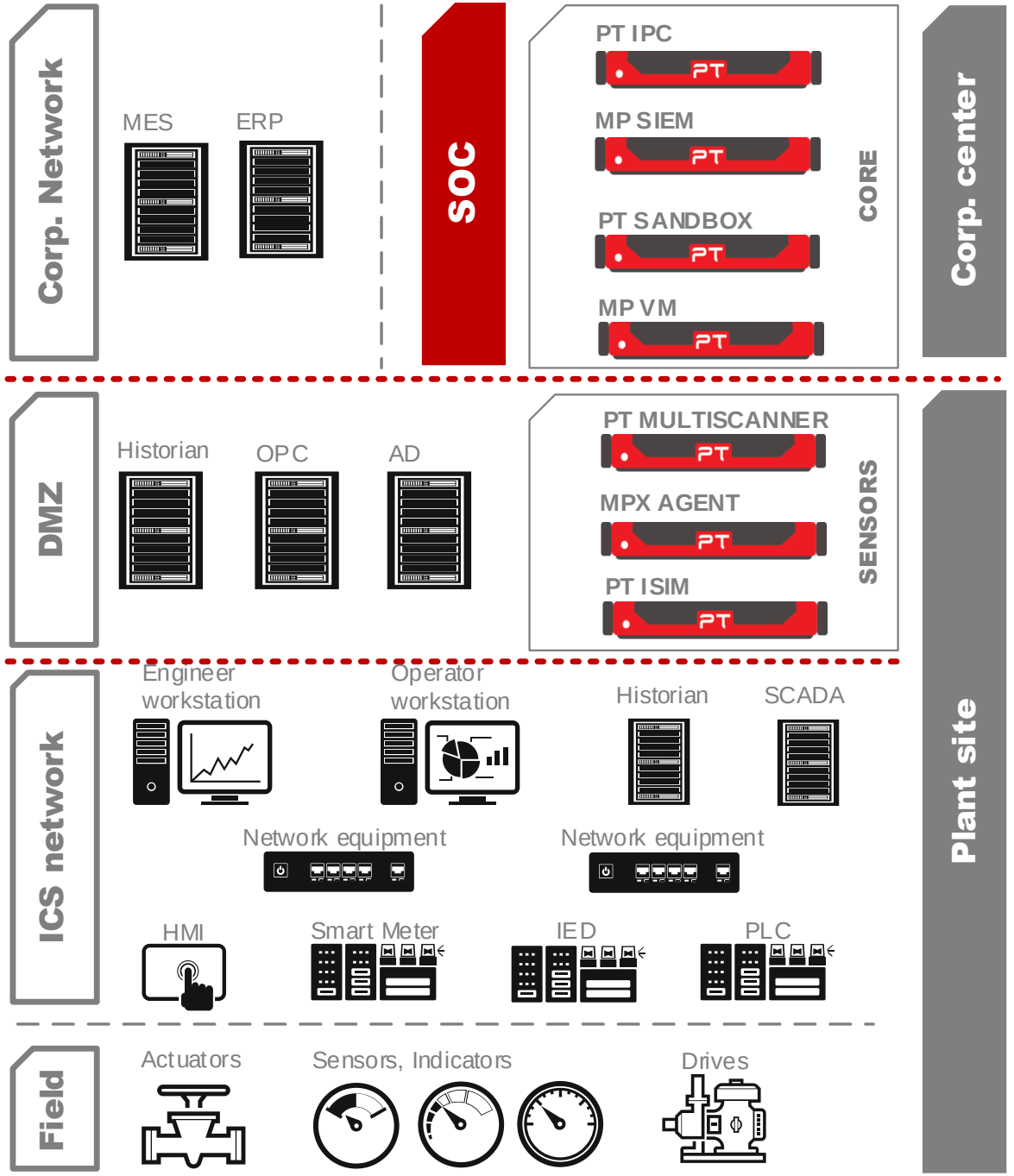
Процессы управления безопасностью



Типовые архитектуры решений

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

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

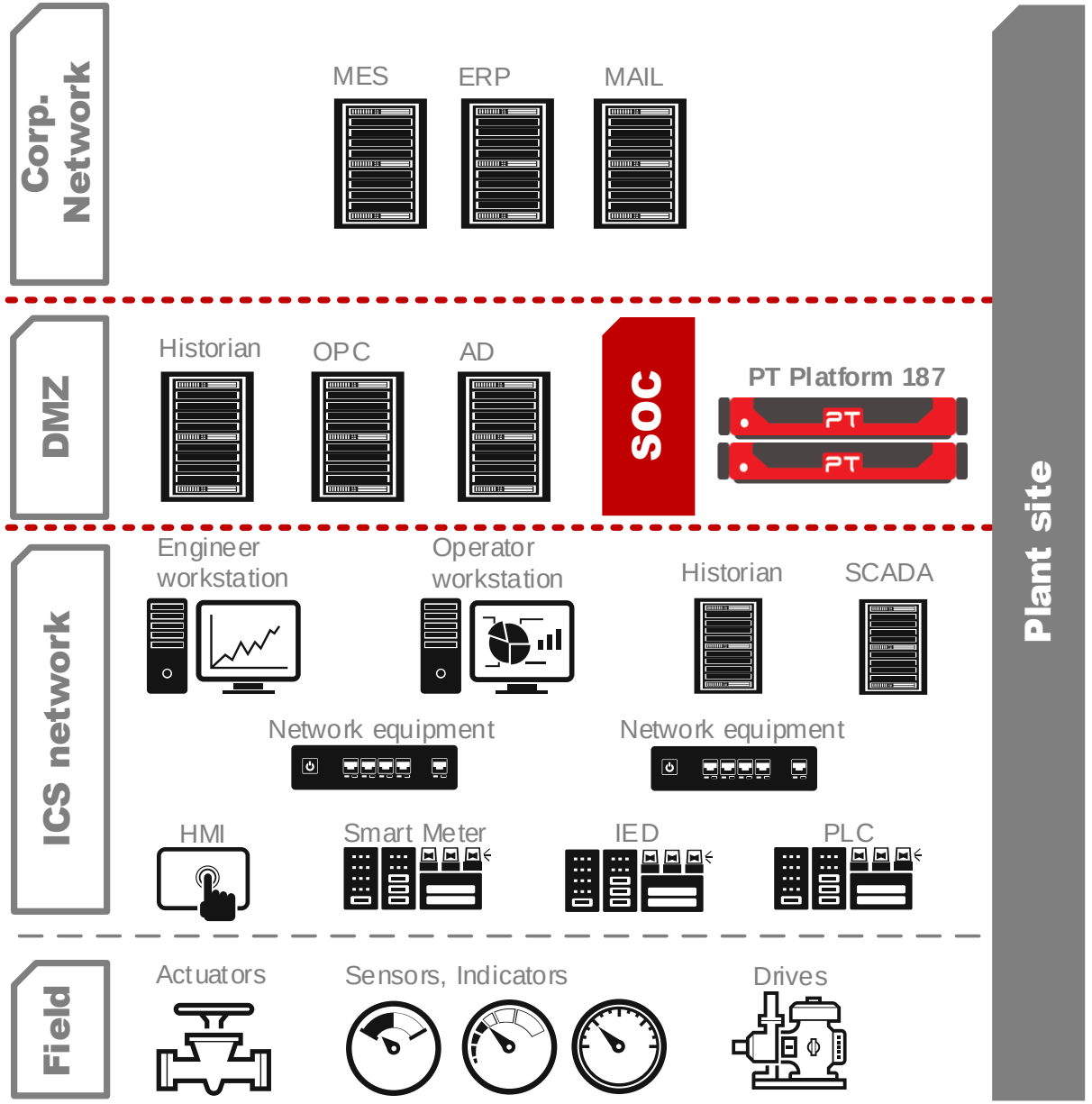


Типовые архитектуры решений

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

PT Platform 187

Программно-аппаратный комплекс для реализации основных задач SOC и выполнения требований законодательства по защите информации



Проекты в промышленности на базе PT Industrial Cybersecurity Suite

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

Свяжитесь с нами:

t: +7 495 744 01 44

sales@ptsecurity.com

ptsecurity.com