Industrial Cybersecurity Situation Awareness

Подход Positive Technologies

ptsecurity.com

Дмитрий Даренский

руководитель практики промышленной кибербезопасности

ddarensky@ptsecurity.com

- Образование: автоматизация технологических процессов и производств
- Более 15 лет опыта строительства технологических сетей и систем связи в энергетике и нефтегазе
- Более 10 лет опыта создания систем АСУ ТП, телемеханики, АСТУЭ, АСКУЭ, и диспетчерского управления
- Более 7 лет опыта создания комплексных систем кибербезопасности
- Эксперт рабочих групп РНК СИГРЭ

Как есть сейчас

АСУШНИК

Есть **SCADA** и этого достаточно для управления производством

БЕЗОПАСНИК

Есть **SOC**, и этого достаточно для управления безопасностью

Живущие возле АЭС коты говорят что с экологией у них нет проблем ☺

0,98%

доступность систем

Непрерывность технологических процессов не зависит от корпоративного сегмента ИТ-инфраструктуры

до 3/4

всех хостов

Масштабы и критичность технологических сегментов для бизнеса в разы выше корпоративных

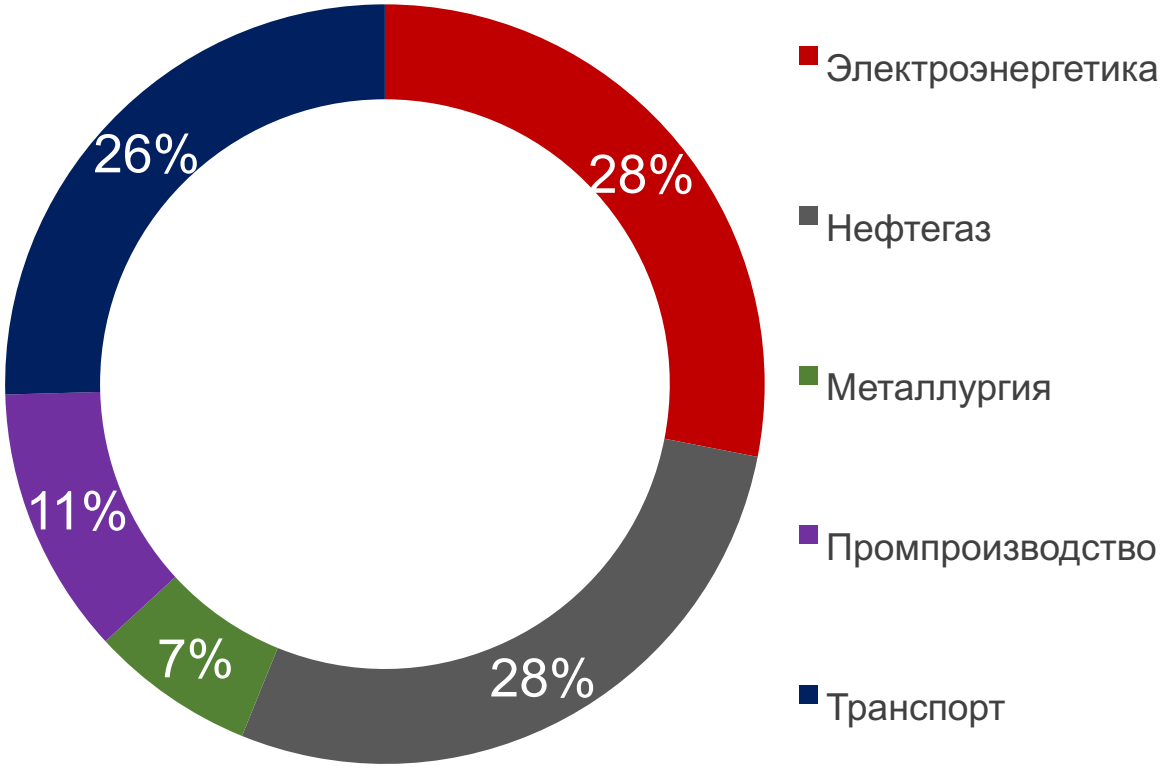
1-3

дня на атаку

Защищенность технологических сегментов ИТ-инфраструктуры хуже корпоративных, **уязвимости** тривиальные и их много

...но бюджеты тратятся в основном на безопасность корпоративного сегмента

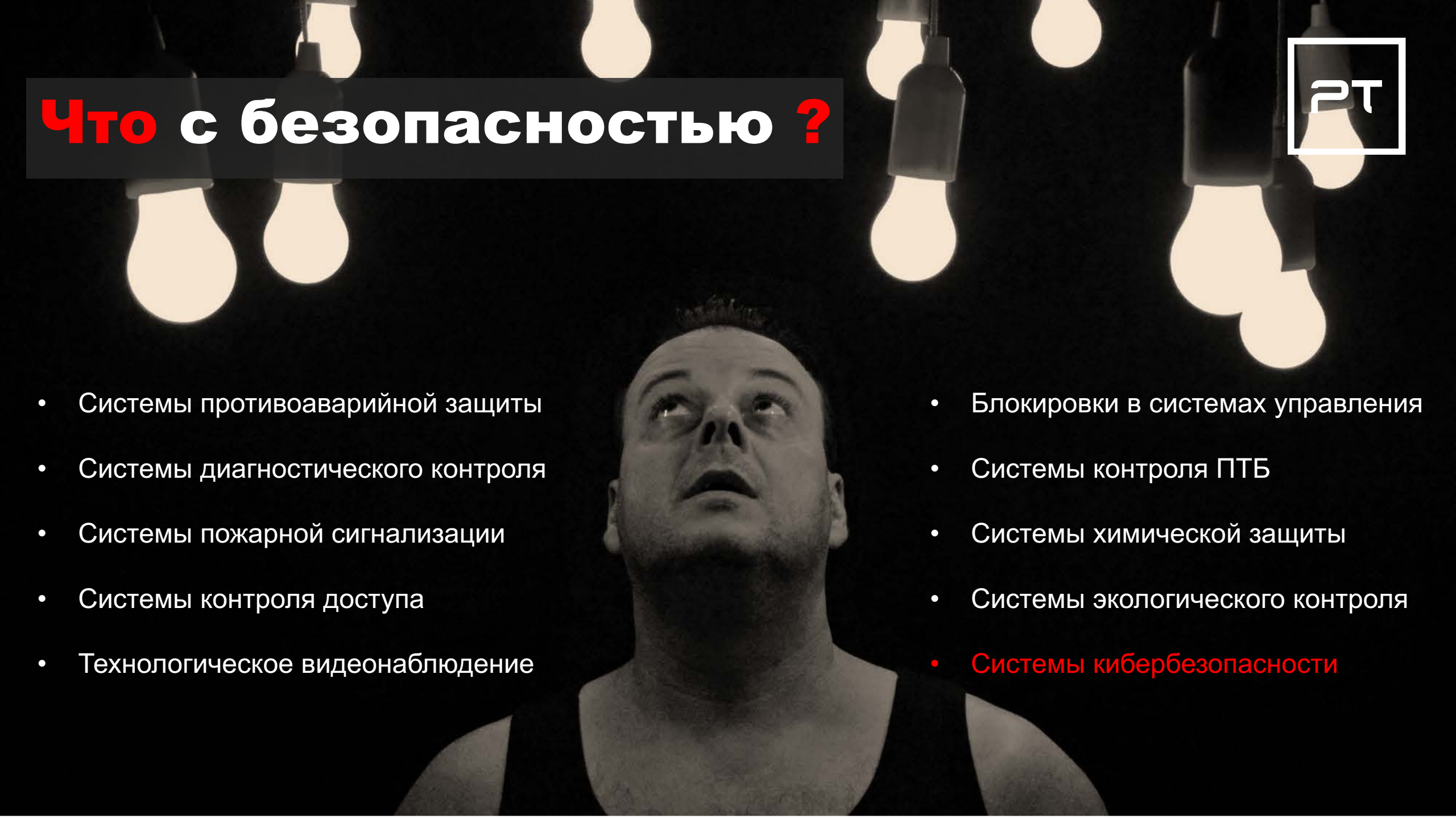
MP SIEM в промышленности 2016-2019 гг.



Объём активированных лицензий в отраслях промышленности

0% предприятий ведущих мониторинг безопасности АСУ ТП и технологических сетей

Что с безопасностью ?



- Системы противоаварийной защиты
- Системы диагностического контроля
- Системы пожарной сигнализации
- Системы контроля доступа
- Технологическое видеонаблюдение
- Блокировки в системах управления
- Системы контроля ПТБ
- Системы химической защиты
- Системы экологического контроля
- Системы кибербезопасности

Industrial Cybersecurity Situation Awareness

ptsecurity.com

Industrial Cybersecurity Situation Awareness

ТЕОРИЯ

MICA ENDSLEY*

Former Chief Scientist of the U.S. Air Force

- **PERCEPTION**

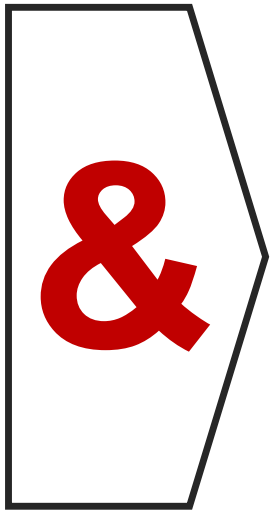
Восприятие элементов окружающей среды во времени и пространстве,

- **ANALYSIS**

Анализ и понимание всего происходящего

- **PROJECTION**

Проекция событий на ближайшее будущее



ПРАКТИКА

POSITIVE TECHNOLOGIES

- **COLLECT & PROCESSING**

Сбор и обработка всего объёма событий и артефактов

- **ANALYSIS & DECISION SUPPORT**

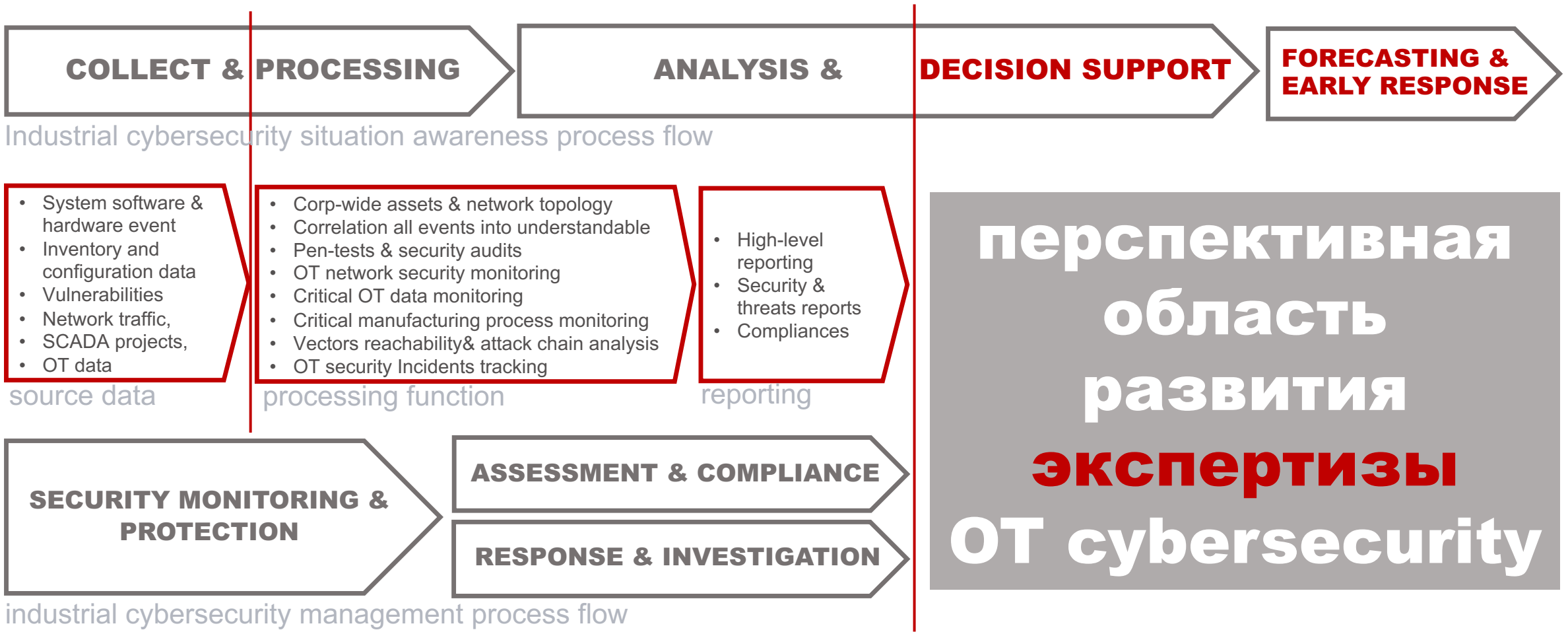
Анализ и получение заключений о ситуации в целом, поддержка принятия решений

- **FORECASTING & EARLY RESPONSE**

Прогнозирование и ранее реагирование с целью обеспечения управляемости процесса или объекта

*https://en.wikipedia.org/wiki/Mica_Endsley

Много букв и стрелок



перспективная область развития экспертизы OT cybersecurity

Удивительное рядом!

Предприятия уже имеют необходимые инструменты и технологии

- SIEM
- NTA
- OT network security monitoring
- Critical OT data & process monitoring
- Security assessment & compliance

Следующий шаг для предприятий

- Определить критичные производственные риски
- Выстроить процессы
- Расширить и формализовать политик

Следующий шаг для поставщиков решений

Перейти от поставок конструкторов к поставкам экспертизы

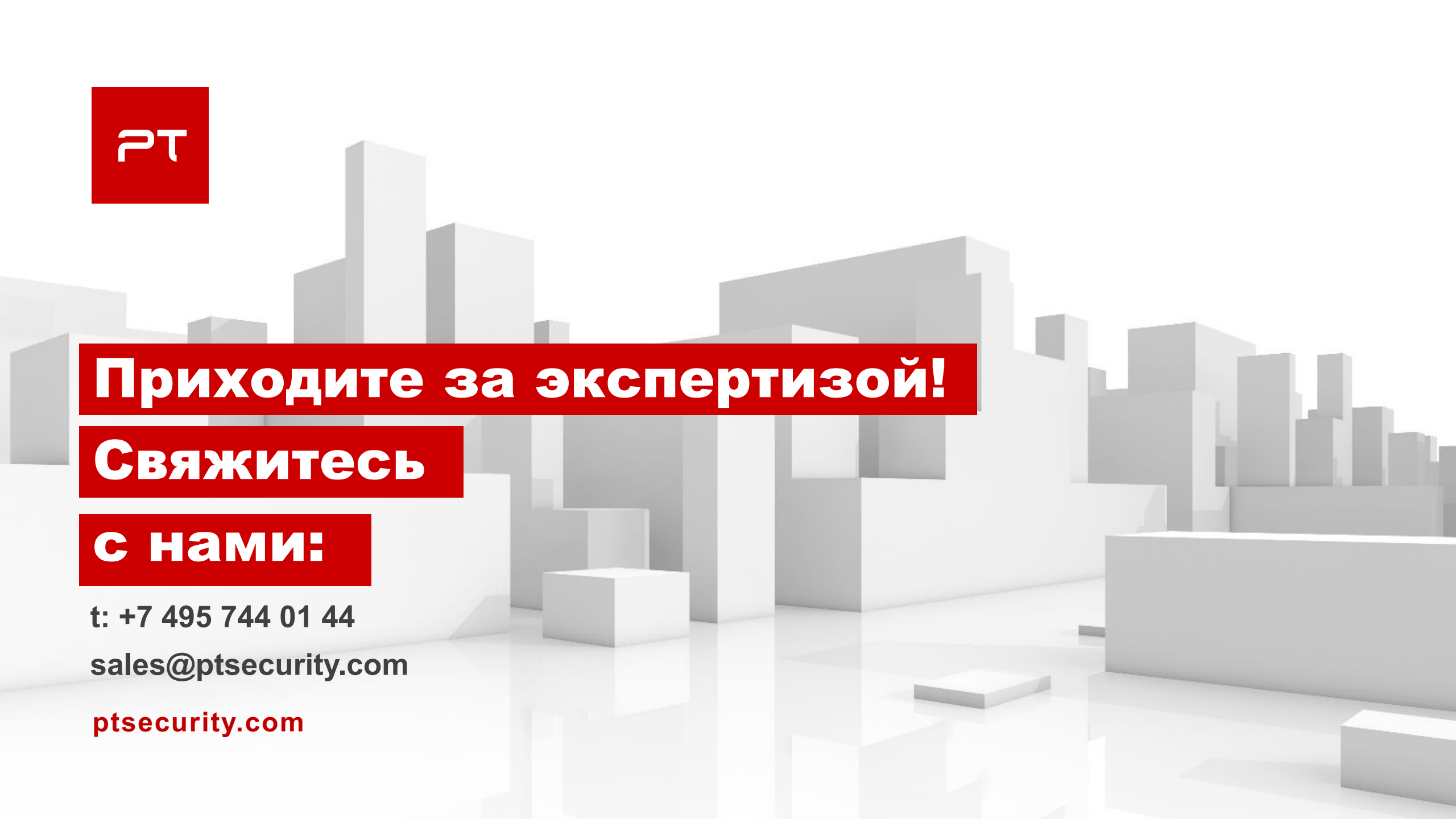
Positive OT cybersecurity solutions

Industrial cybersecurity situation awareness process flow

COLLECT & PROCESSING | ANALYSIS & DECISION SUPPORT | FORECASTING & EARLY RESPONSE

перспективная область развития экспертизы OT cybersecurity

- OT cybersecurity expert packs
- OT cybersecurity compliance
- OT cybersecurity forecasting



Приходите за экспертизой!

Свяжитесь с нами:

t: +7 495 744 01 44

sales@ptsecurity.com

ptsecurity.com