Промышленная кибербезопасность

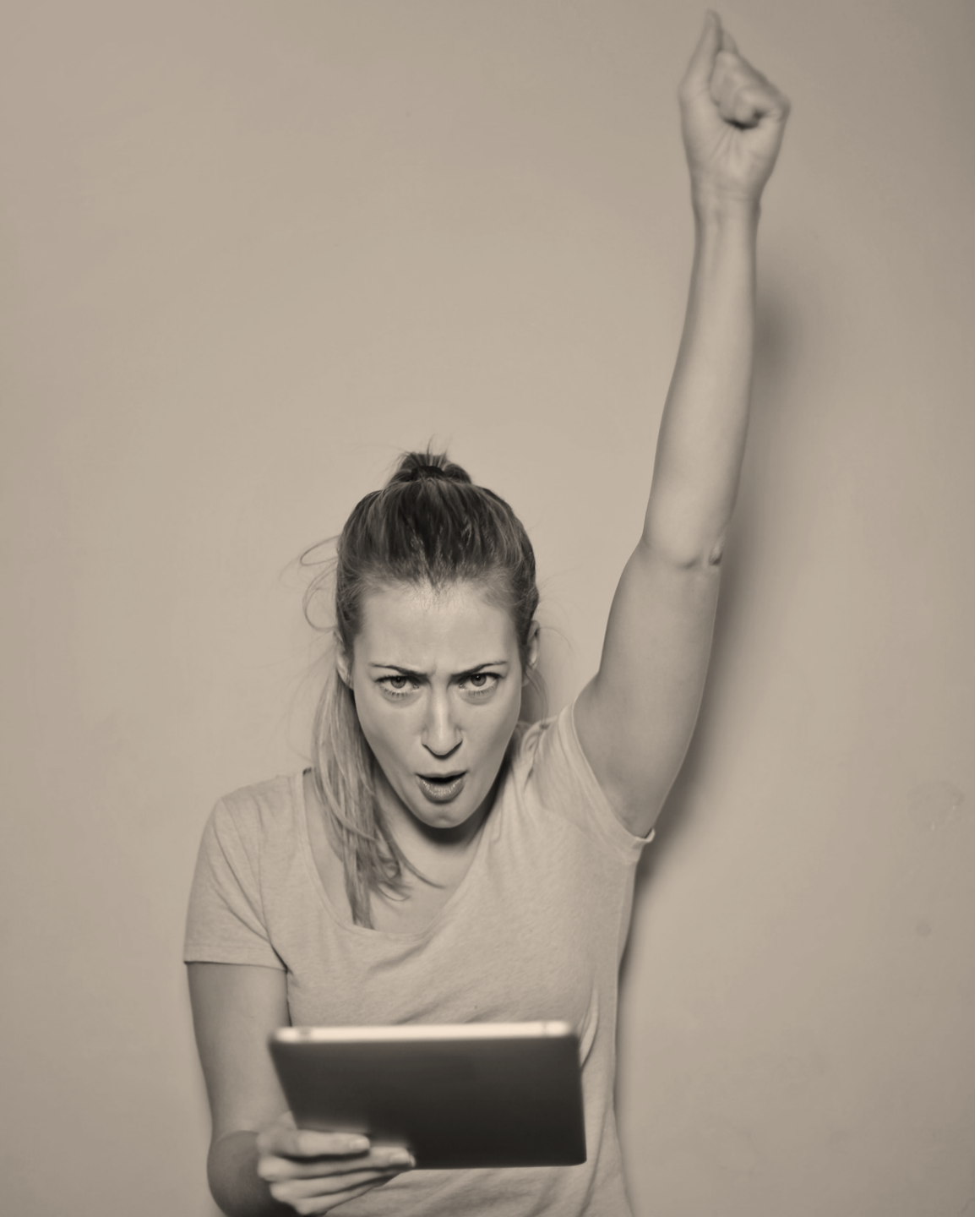
Управлять невозможно игнорировать

Дмитрий Даренский

Руководитель практики промышленной кибербезопасности

ddarensky@ptsecurity.com

ptsecurity.com



БОЛЬШИЕ НАДЕЖДЫ

- Выполнить категорирование
- Определить меры и технологии защиты
- Пропилотировать и выбрать то что нравится
- Построить комплексную систему безопасности
- Построить SOC
- Подключиться к ГосСОПКА

...и доказать бизнесу ценность всего этого

...И БОЛЬШИЕ ПРОБЛЕМЫ

- Применить свои компетенции там, где они раньше были не нужны
- Защищать что-то, что раньше не защищал
- Защитить то, что не в твоей зоне ответственности
- Реагировать на непривычные и «странные» угрозы
- Обучать высоко квалифицированных «не безопасников» безопасности того, что раньше не защищал.

так хорошо всё начиналось

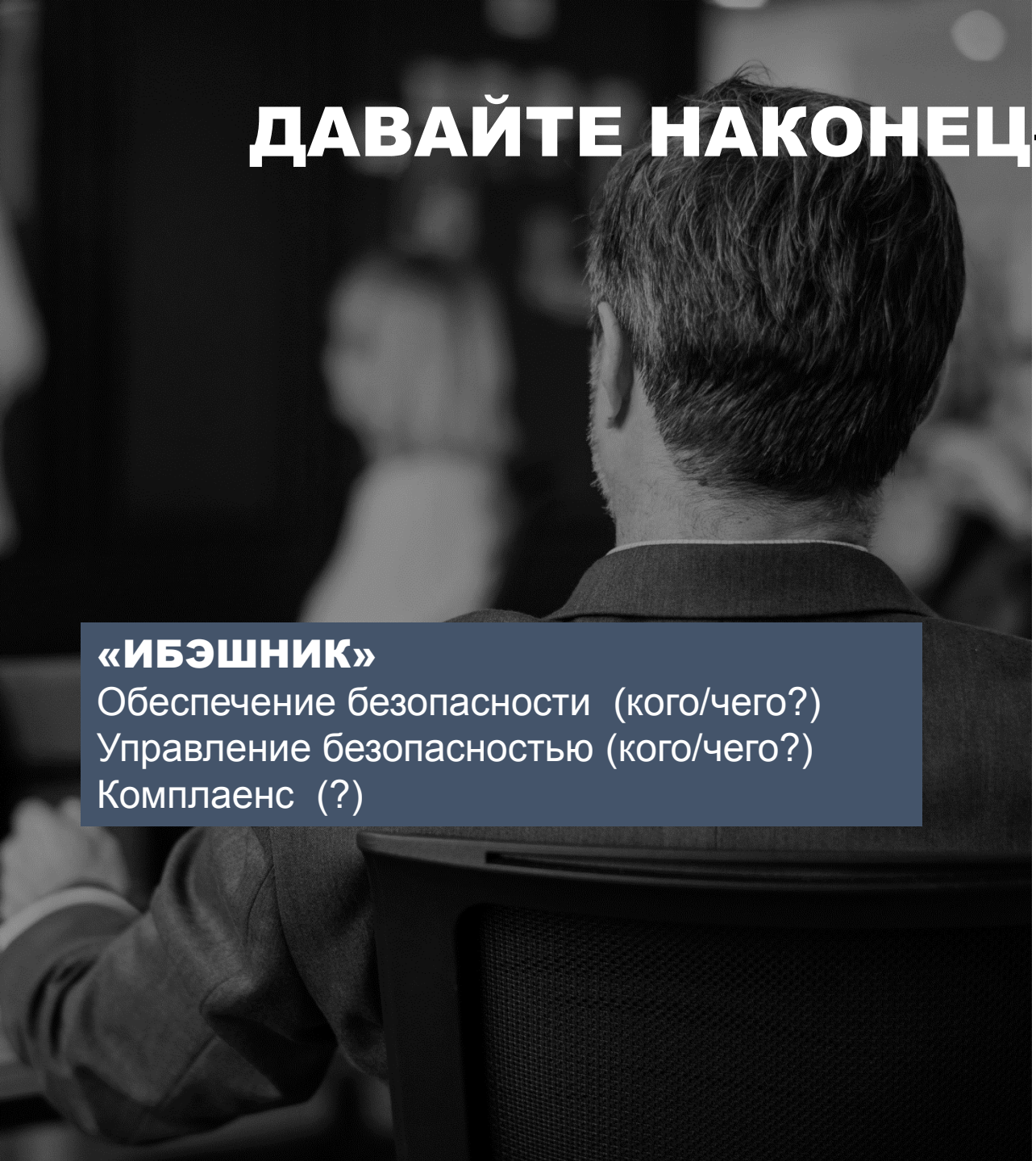
- УРА!!! У нас есть SOC!!!
- Подключили корпоративную ИТ инфраструктуру
- Наняли провайдера на первую/вторую линию
- Написали Playbooks
- Сделали всё в соответствии с лучшими практиками и стандартами

...и тут началось

СЮРПРИЗ,
СЮРПРИИИЗ!!!

- **Объекты КИИ** в основном это **АСУ ТП, а не ИТ системы**
- Как подключать их к SOC – **непонятно**
- Кто подключает – **не определено**
- Что является инцидентом в АСУ ТП – **не договорились**
- Playbooks никто и никогда **на «ЭТО» не писал**
- **КАК**, и главное **КТО** реагирует на инцидент?
- **КТО** отвечает за расследование инцидентов?

ДАВАЙТЕ НАКОНЕЦ-ТО ПОЗНАКОМИМСЯ



«ИБЭШНИК»
Обеспечение безопасности (кого/чего?)
Управление безопасностью (кого/чего?)
Комплаенс (?)

«АСУШНИК»
Обеспечение непрерывности производства
Обеспечение плановых производственных показателей

СТО РАЗ ТАК ДЕЛАЛ, ЧТО СЕЙЧАС НЕ ТАК?

- Определил угрозы ИБ
- Пропилотировал SIEMы
- Выбрал подходящий
- Пошел за финансированием

И...

- **Бизнес не увидел ценность**
- **Асушники ~~послали~~ не увидели пользы**

Fail: **пошли от технологий и угроз, понятных только безопасникам**

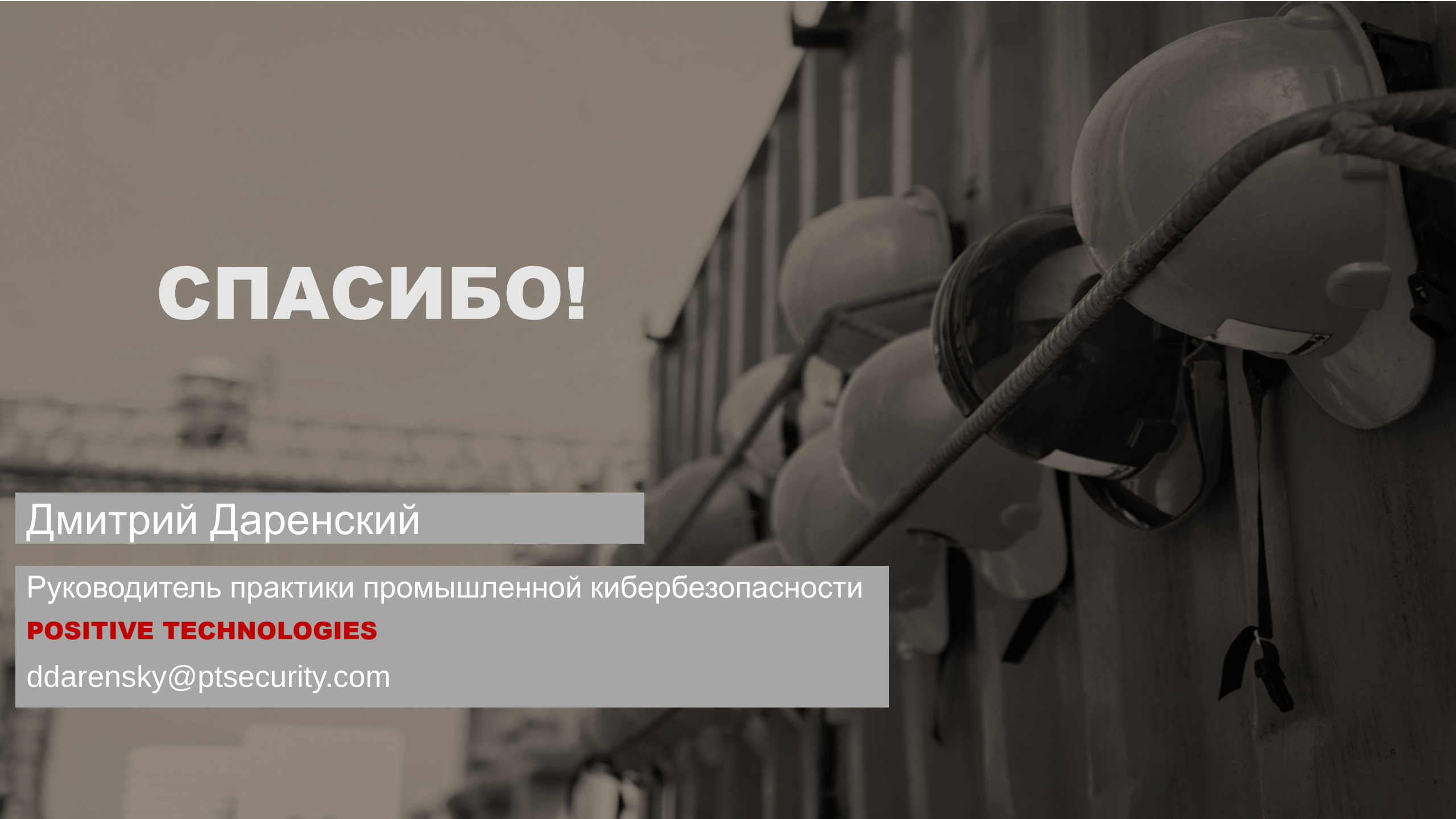
НЕ ИБ ЗАДАЧИ
ИБ СРЕДСТВАМИ

- Непрерывность производства
- Повышение отказоустойчивости
- Предотвращение хищений
- ….

КОМПЛЕКСНЫЙ
МОНИТОРИНГ
В SOC

PROFIT:

- **пошли от задач производственников – получили их поддержку**
- **показали ценность своих компетенций и решений бизнесу– получили финансирование**



СПАСИБО!

Дмитрий Даренский

Руководитель практики промышленной кибербезопасности

POSITIVE TECHNOLOGIES

ddarensky@ptsecurity.com