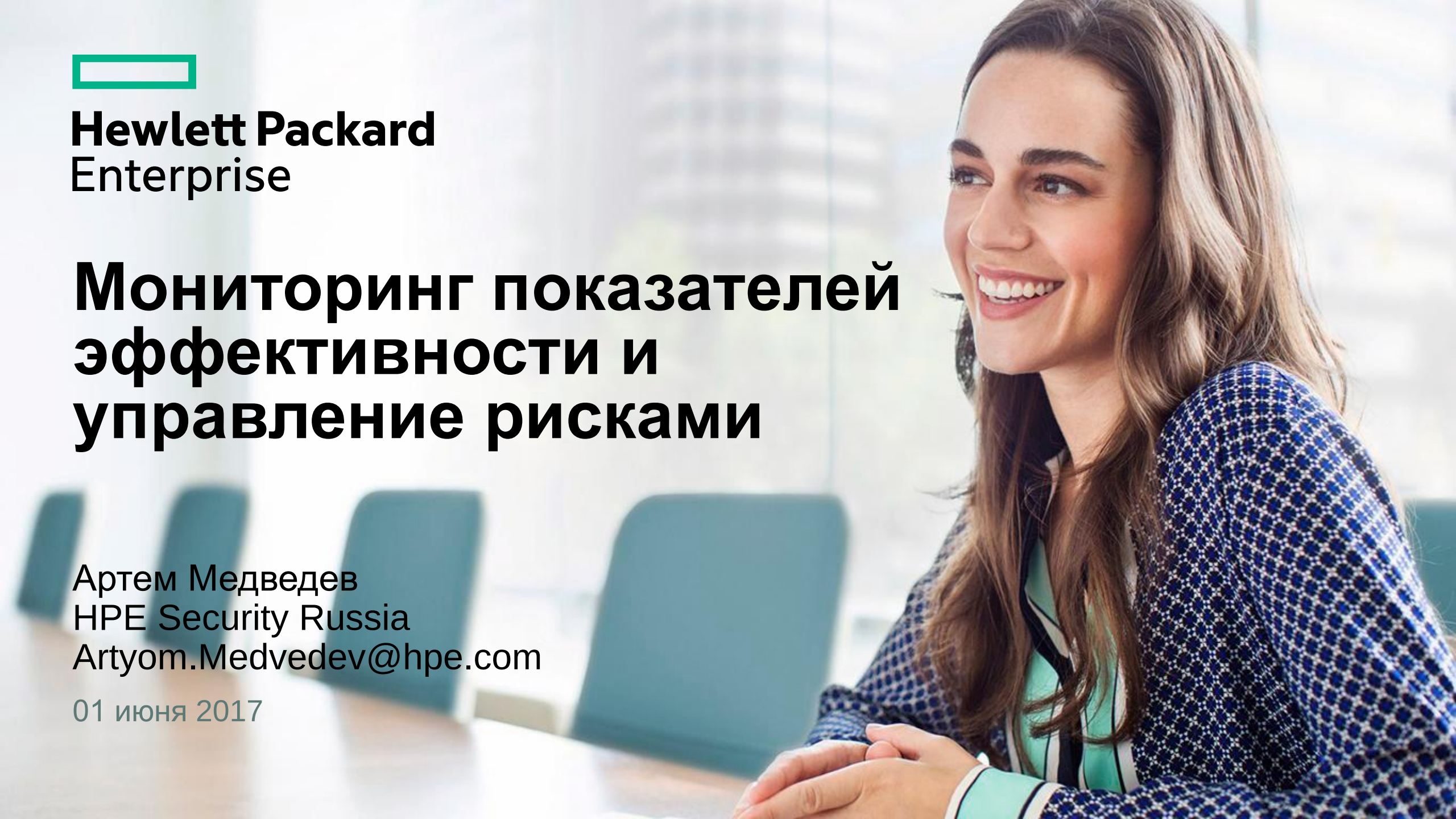
Hewlett Packard Enterprise

Мониторинг показателей эффективности и управление рисками



Артем Медведев
HPE Security Russia
Artyom.Medvedev@hpe.com

01 июня 2017

Подход HPE

Подход HPE к управлению рисками в финансовых организациях основан на выявлении потоков данных, кореляции событий и метрик, визуализации результатов.

Кореляция событий - HPE Arcsight
Визуализация результатов и метрик - HPE BVD
Мониторинг бизнес-процессов – HPE OpsB

Hewlett Packard Enterprise

Нетехнические (организационные) задачи

- Необходим сбор опросных листов и учет кадровой информации с помощью HPE Arcsight или Service Manager.

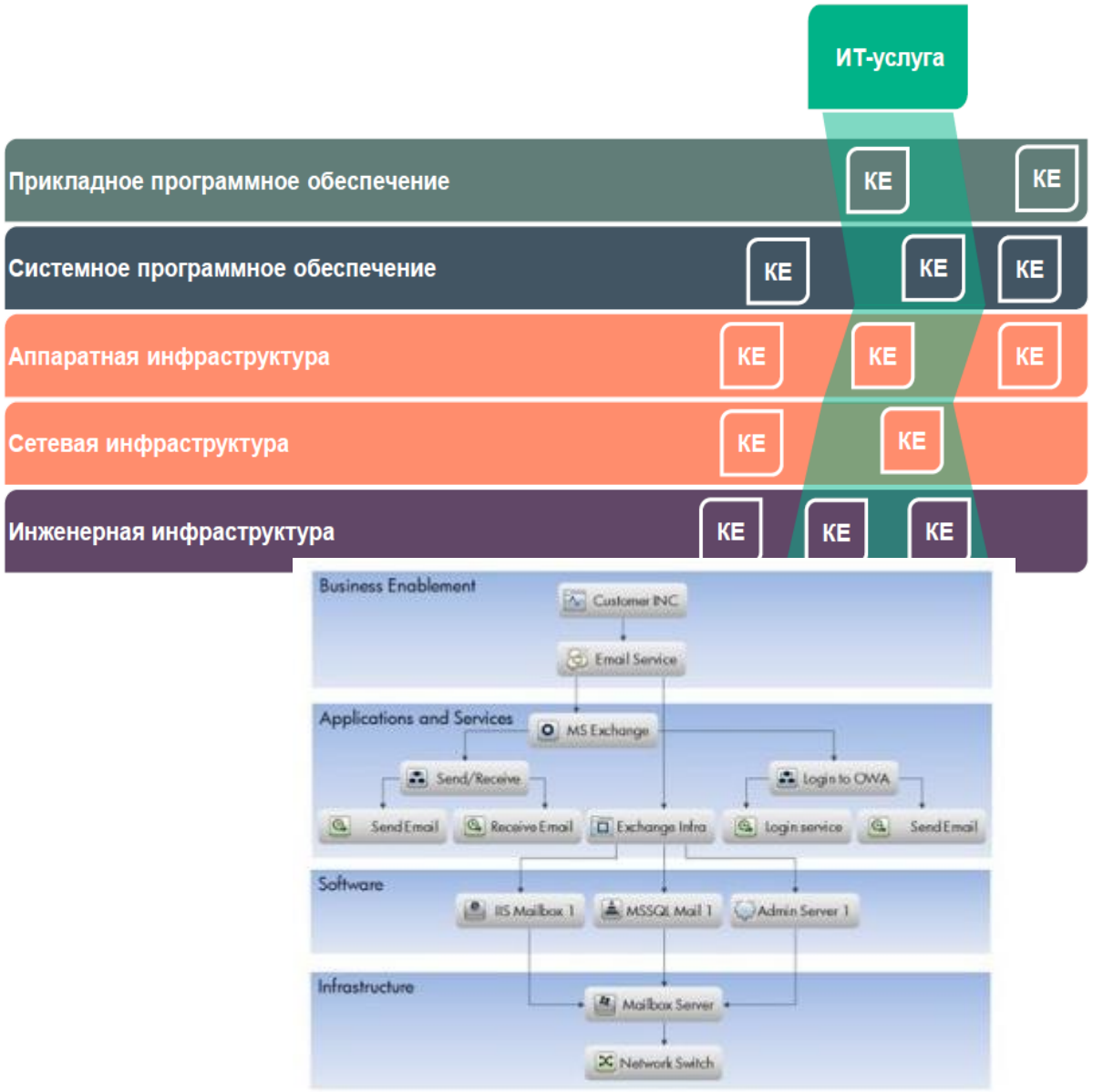
- Набор возможных вопросов указан в ISO 27001 (а также SANS, COBIT, СТО БР и других банковских стандартах).

Hewlett Packard Enterprise

Технические задачи

Для эффективного мониторинга и управления рисками необходима автоматизация наполнения базы конфигурационных единиц (CPM), контроль изменений настроек средств защиты информации.

Задачи выполняются решениями HPE Service Automation, uCMDB, Arcsight.



Hewlett Packard Enterprise

Мониторинг бизнес-процессов (СУИБ)

С помощью решений HPE OpsB возможно описать ключевые бизнес-процессы, а также:

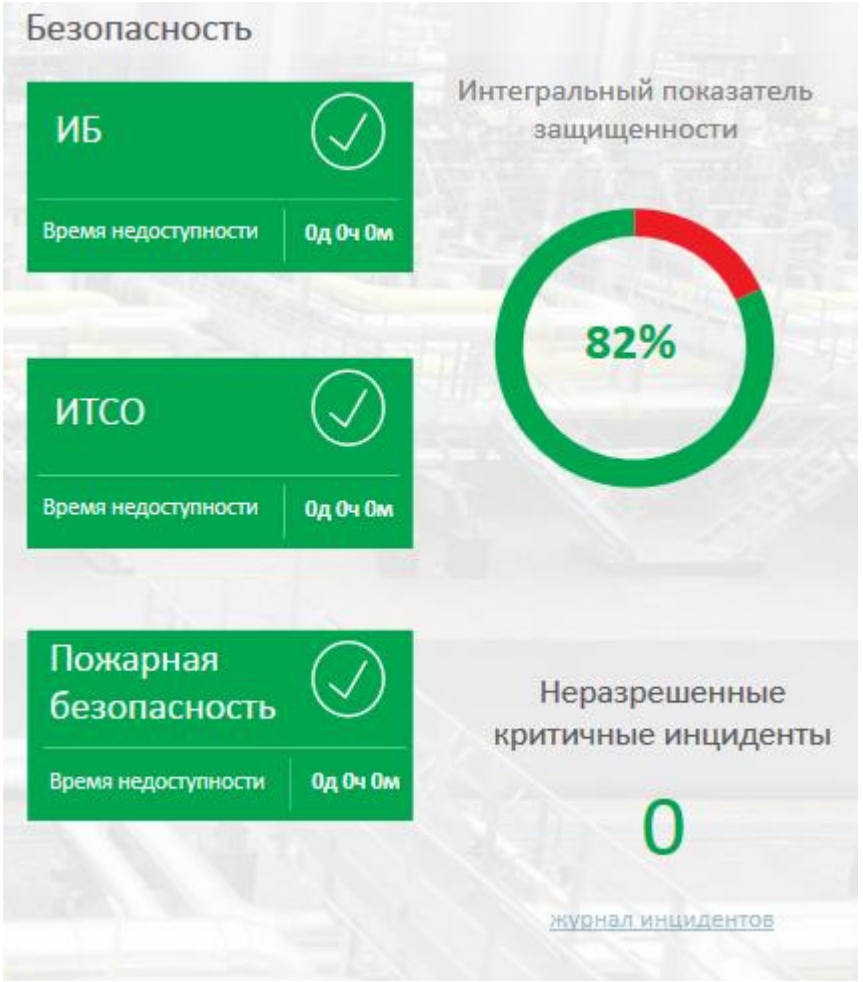
- вести мониторинг системного ПО,
- внутренних систем заявок,
- изменений инфраструктуры

Данные от СЗИ о событиях ИБ собираются и обрабатываются HPE Arcsight с дальнейшей интеграцией и визуализацией в BVD

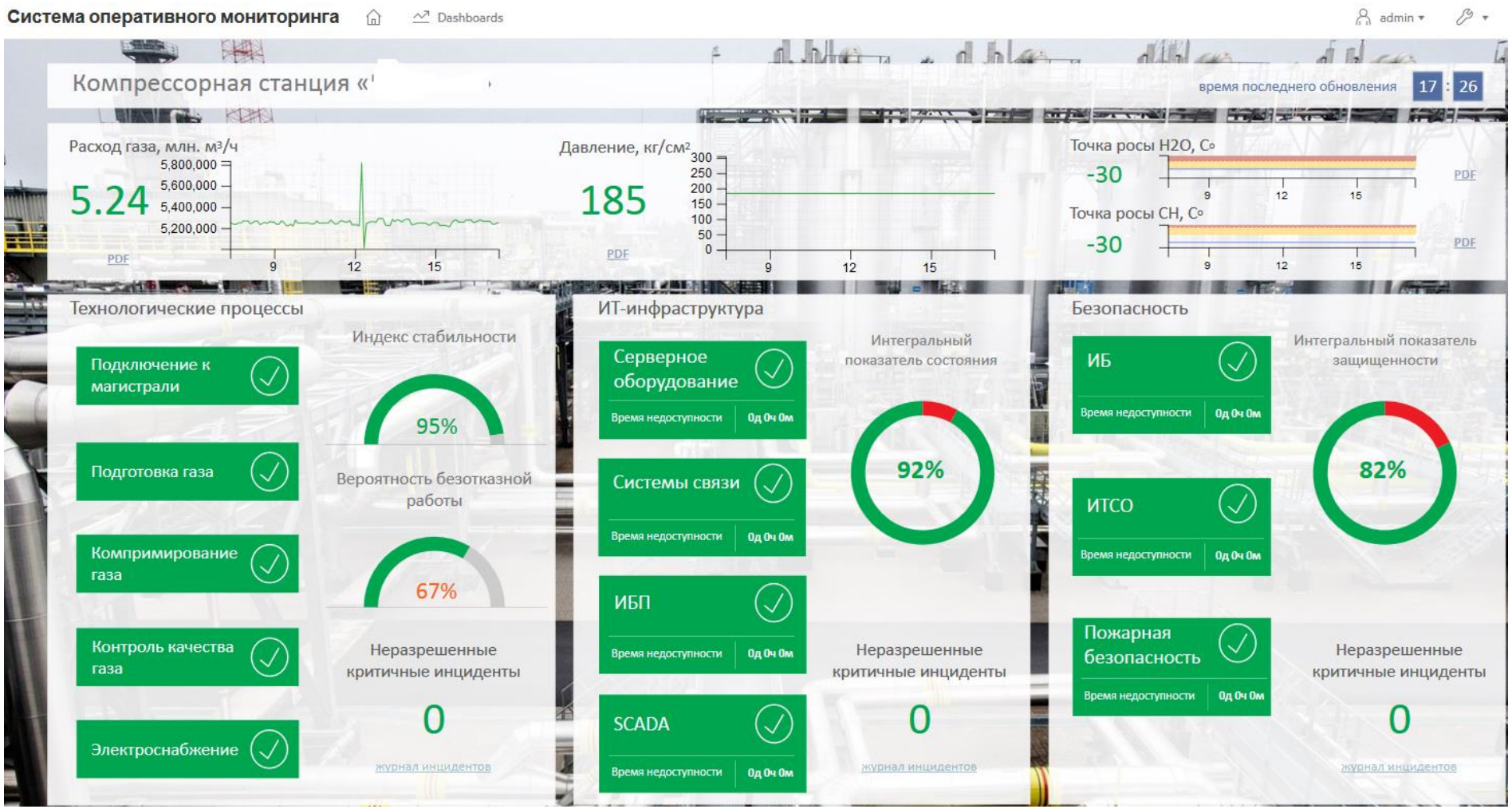
Эффективность работы СЗИ

Ключевой задачей является мониторинг показателей эффективности работы средств защиты информации.

Необходим контроль изменений показателей модели угроз, отслеживание эффективности работы СЗИ путем мониторинга трендов состояний и показателей.
Основной инструмент визуализации - HPE BVD, кореляция – Arcsight.



Интегральные показатели ИТ, ИБ и бизнес-процессов



Предложения по тестированию решения

1. Определить ключевые метрики работы СЗИ
2. Определить показатели эффективности для метрик
3. Настроить сбор и обработку событий в продуктах HPE
4. Настроить необходимые представления визуализации получаемых данных в режиме реального времени
5. Масштабировать полученные результаты

Спасибо!