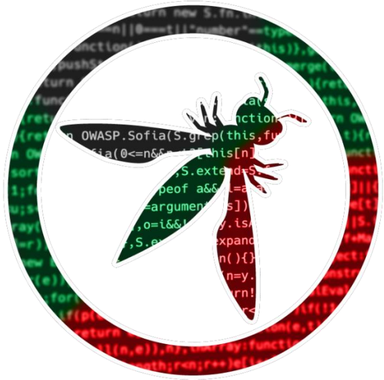


OWASP
SOFIA, BULGARIA

Метрики в киберсигурността – ефективно срещу неефективно докладване

Йонко Йонкофф

Какво наричаме метрика?

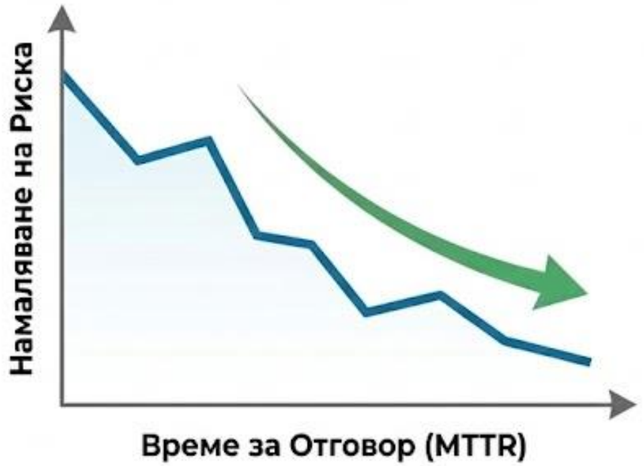
Метриката оценява ефективността на защитата и риска спрямо бизнес целите, като се характеризира с:

- Обективен начин за измерване
- Проследяване на тенденция във времето
- Приложими действия

От повърхностни метрики (Vanity Metrics) до стойностни: Какво реално измерваме?

ПОВЪРХНОСТНИ

СТОЙНОСТНИ



Как изглеждат повърхностните метрики?

- Илюзия за прогрес
- Липса на контекст
- Без последващи действия

Как изглеждат ефективните метрики?

- Насочени към действие
- Тенденция във времето
- Фокус върху резултата

Валидиране на ефективна метрика с помощта на 3 въпроса

1. Приложими ли са действия?

2. Проследима ли е тенденция във времето?

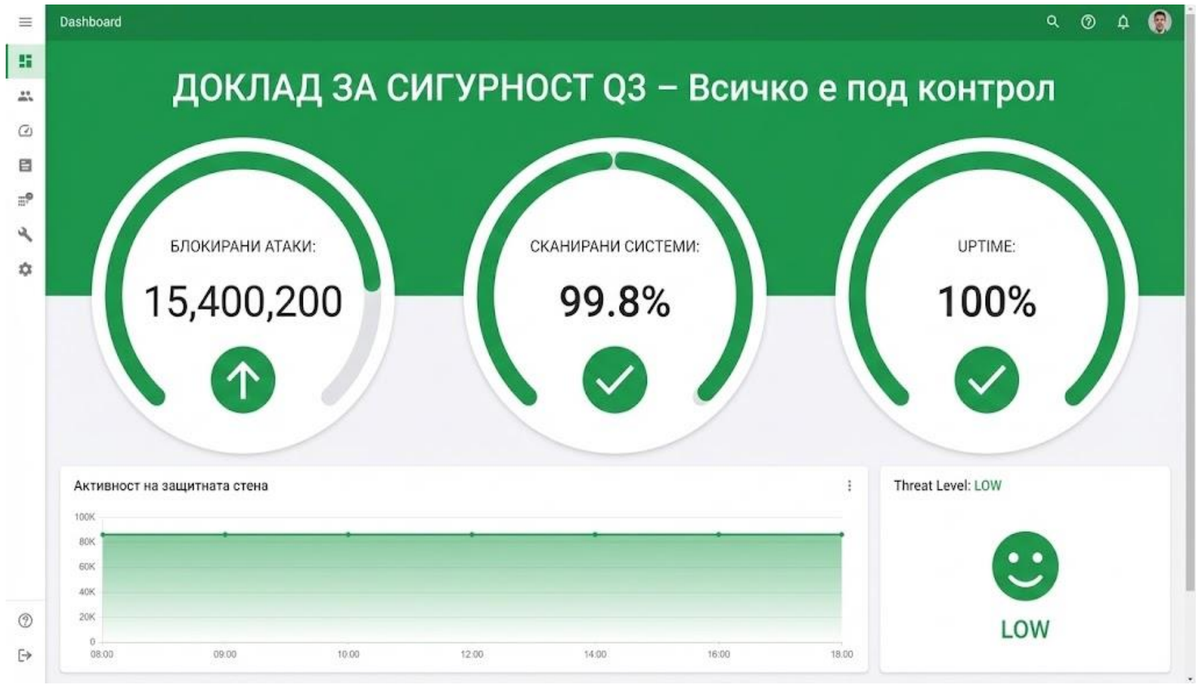
3. Има ли въздействие върху бизнеса?

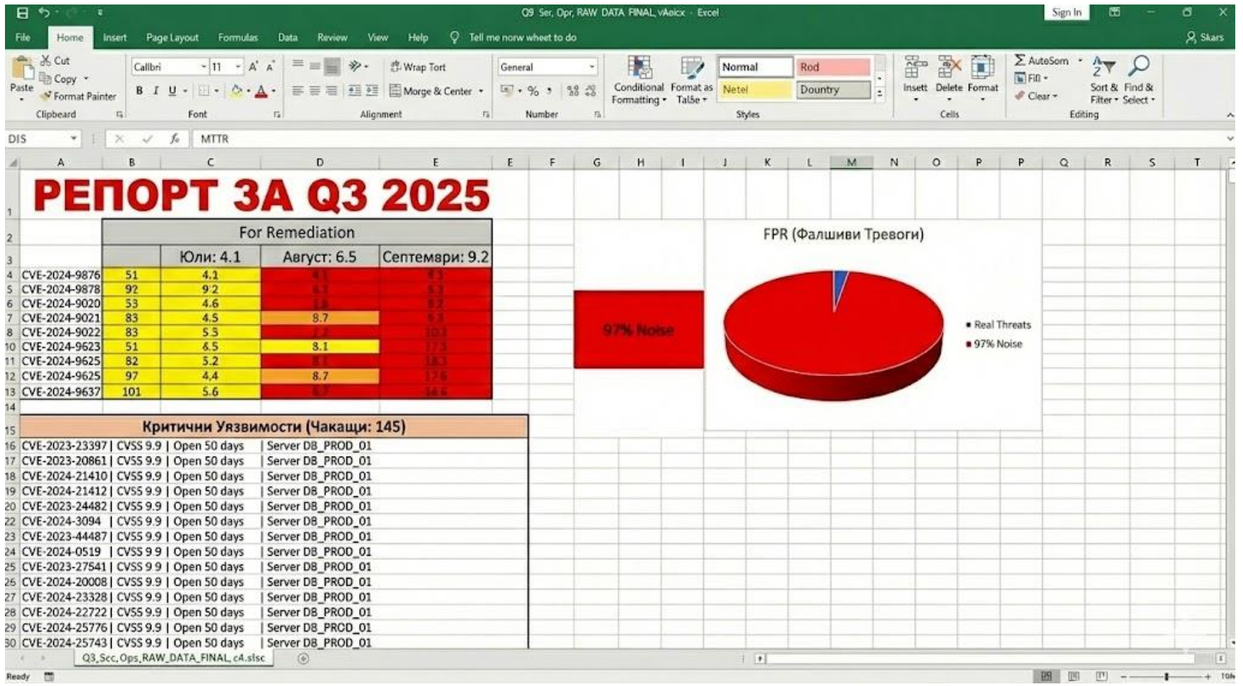
Метрика 2: Средно време за обработка на аларми
[✓]
[✓]
[✓]

Защо са важни докладите?

- Определяне на бюджета
- Приоритизиране на риска
- Доверие в екипа
- Законово и регулаторно съответствие

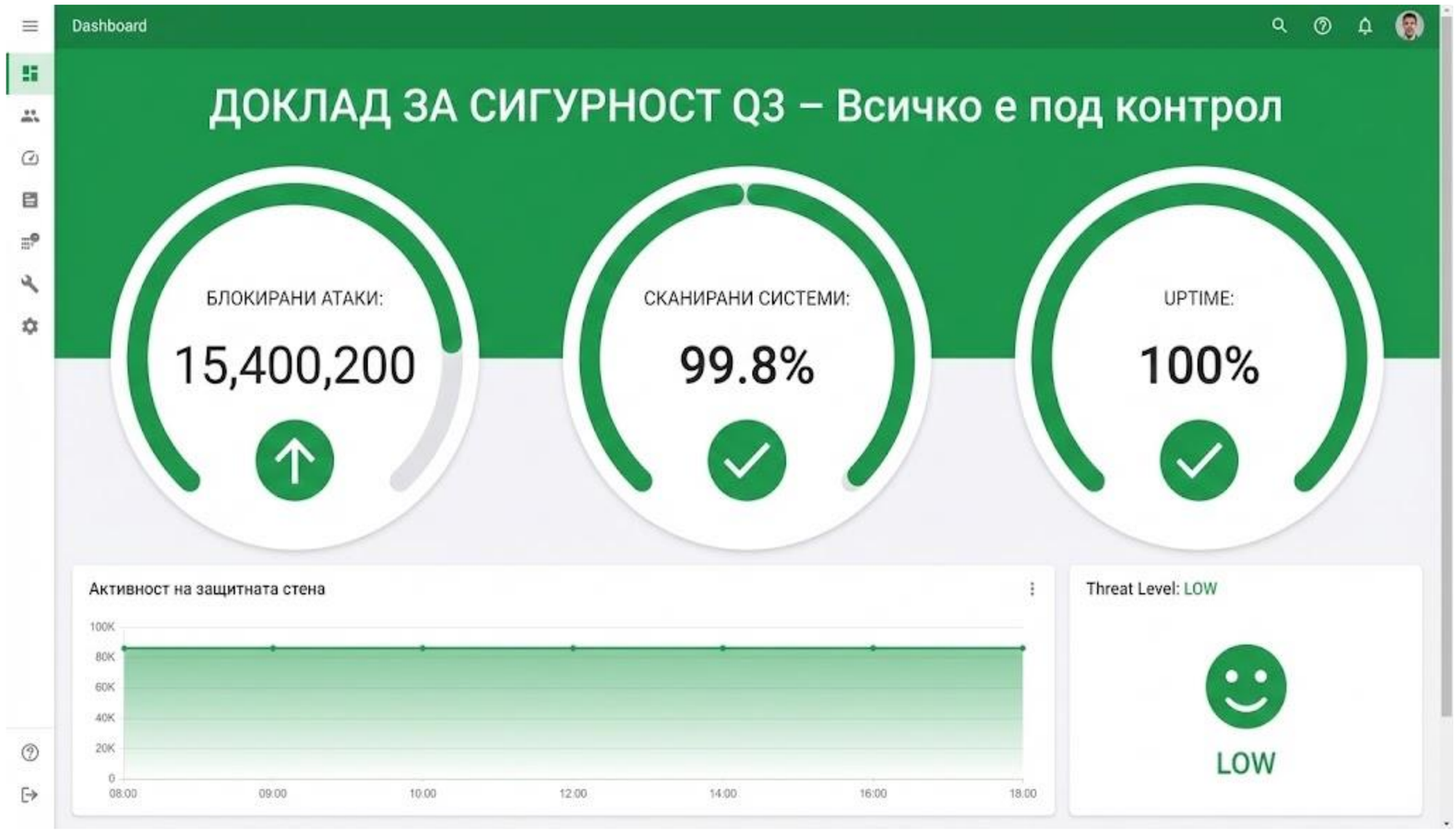
Ефективно срещу неефективно докладване





Ефективно срещу неефективно докладване

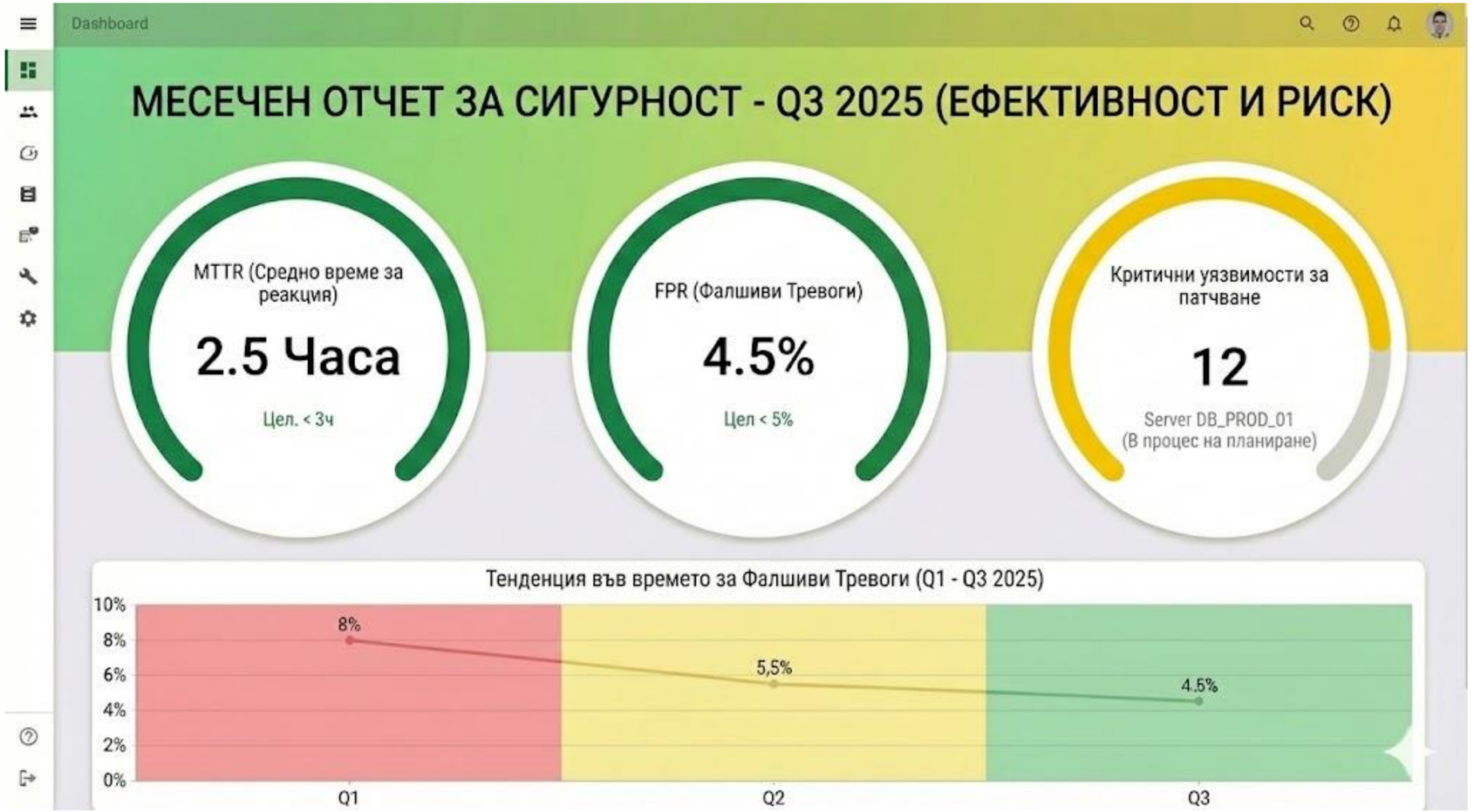
- Добрият дизайн не е достатъчен за оправдаване на бюджета
- Без ефективни метрики визията на един доклад е просто “успокояваща” декорация



Ефективно срещу неефективно докладване

- Правилните метрики без правилната структура са просто шум
- Истината няма стойност, ако е скрита в нечетима таблица, която никой не разбира

Идеалният баланс



Благодаря за вниманието!


Q&A SESSION
ASK A QUESTION:
SUBMIT
LIVE QUESTIONS: