ESCOM
Enterprise ICT Security Solutions

Дигитализация на икономиката в среда на Големи данни

ЦЕНТЪР ПО КОМПЕТЕНТНОСТ

Добри практики за Кибер сигурност в Система за големи данни интегрирана със Суперкомпютри

Суперкомпютър

Система за големи данни

София
17.11.2022

УНИВЕРСИТЕТ ЗА НАЦИОНАЛНО И СВЕТОВНО СТОПАНСТВО

Кибер сигурност на Системата за големи данни и роля при интеграцията й със Суперкомпютър

2хСуперкомпютри (СК)

СИСТЕМА ЗА ГОЛЕМИ ДАННИ (СГД)

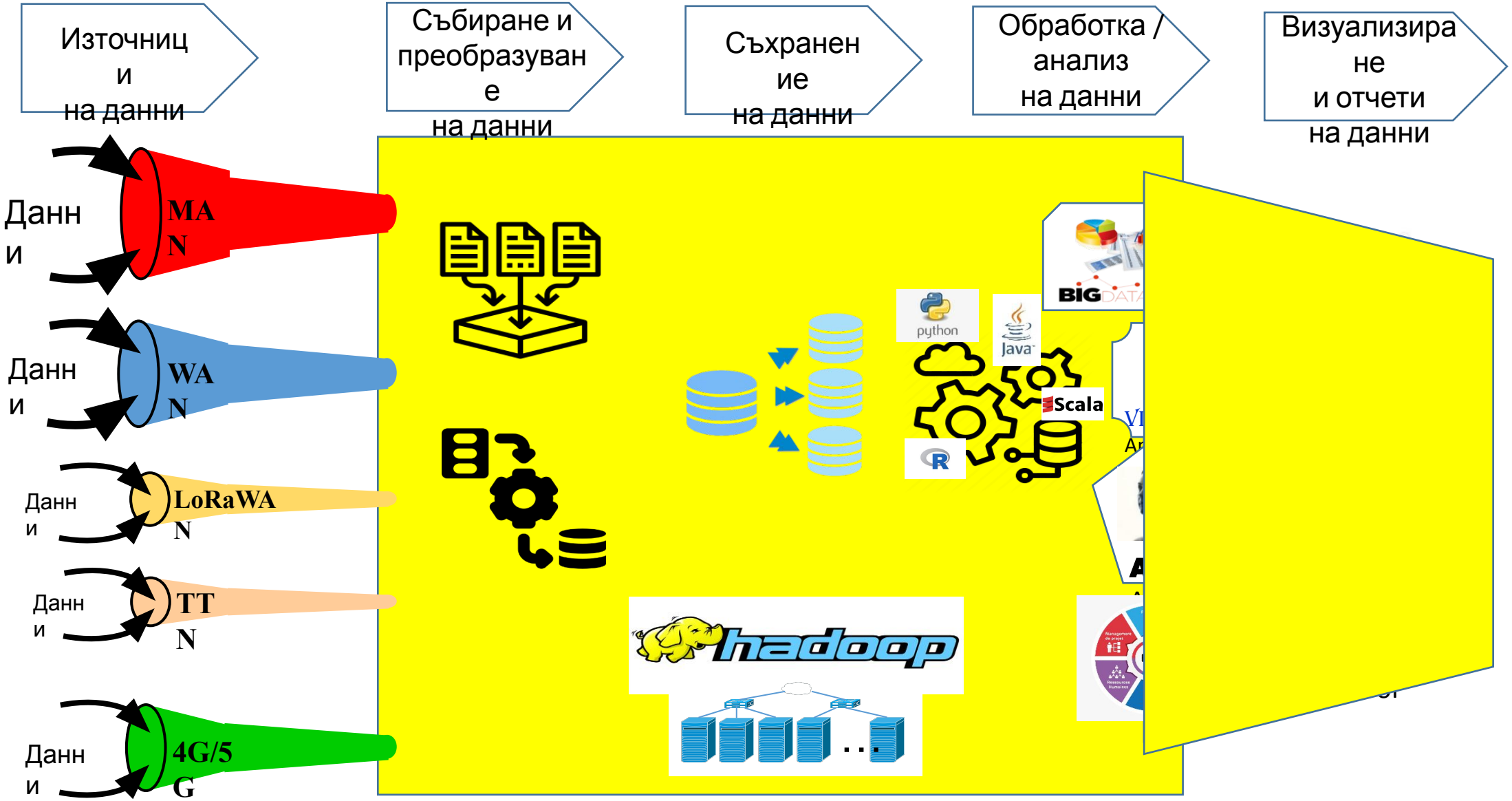
Система за Големи данни като **обект** на Кибер сигурността

- Осигурява сигурност при приемане на данните в СГД
- Осигурява сигурност на съхранението на данните в СГД
- Осигурява сигурност на обработките в СГД

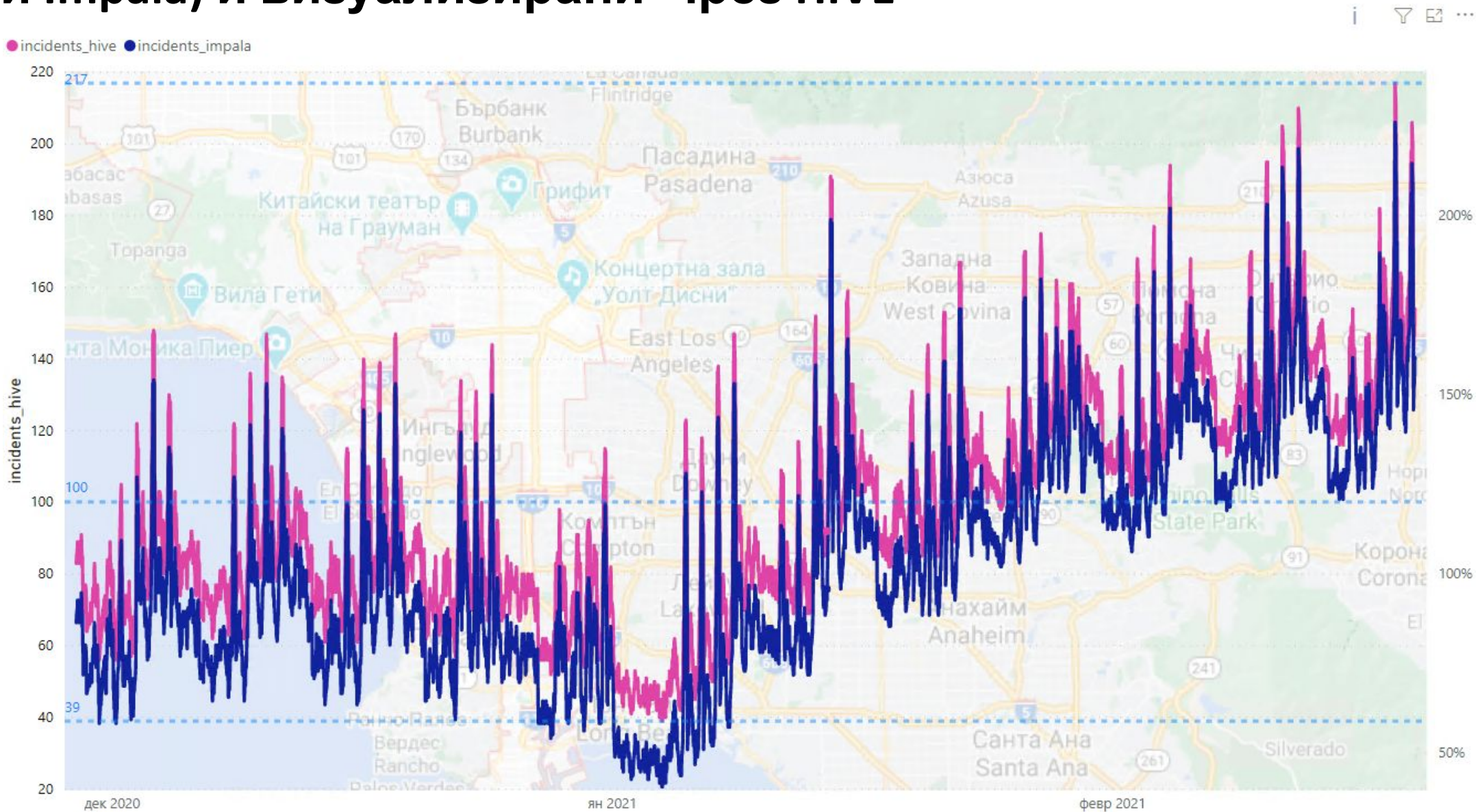
Система за Големи данни като **инструмент** за Кибер сигурността

- Осигурява сигурност на приемане на данните за СК
- Осигурява сигурност на съхранение на данните за СК
- Осигурява голямо и надеждно хранилище на данни за СК

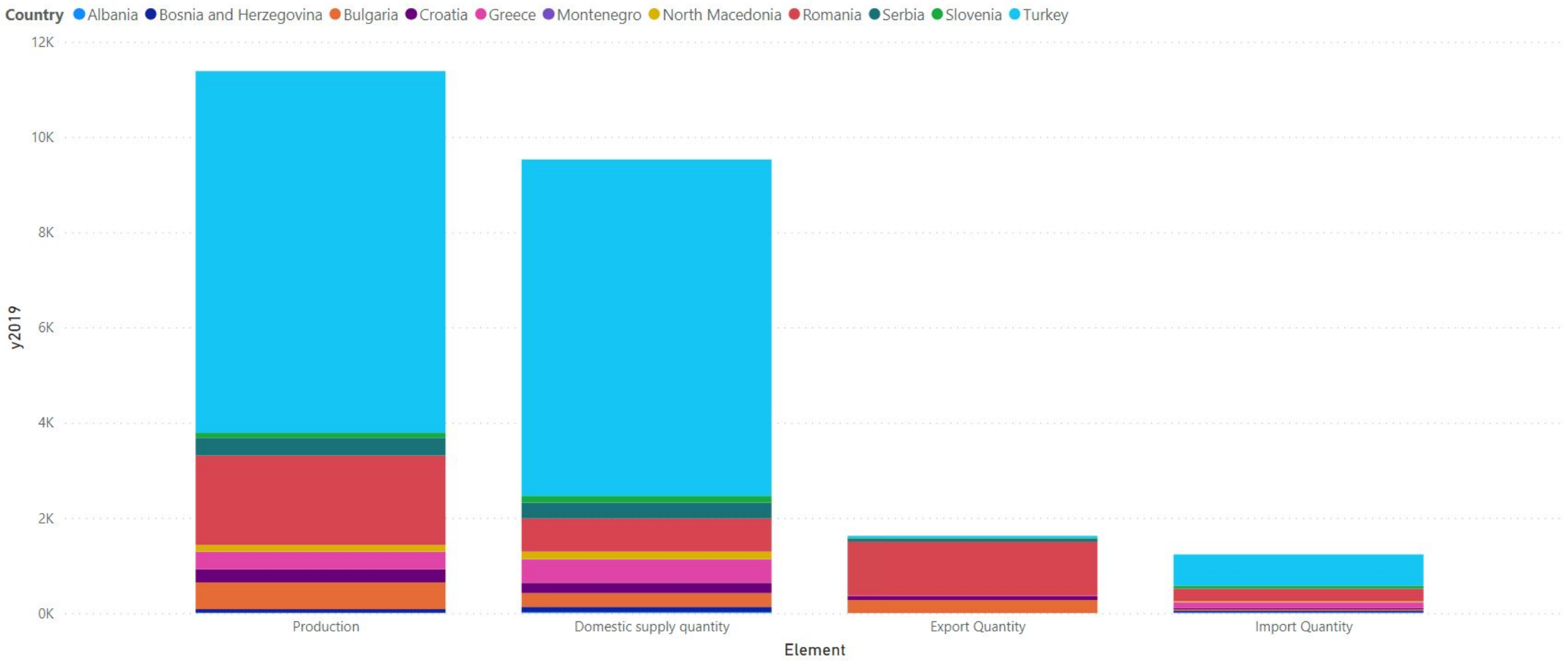
Архитектурен комплекс на изградената Система за Големи данни



Пример – транспортни инциденти в LA областта обработени, чрез Софтуерна/AI Hadoop бизнес сигурност (с участие на NiFi и Impala) и визуализирани чрез HIVE



Пример – Производство и реализация на *ечемик* на Балканския полуостров за 2019 г. с данни обработени, чрез Софтуерна /AI Hadoop бизнес сигурност



Пример за разпознаване на малки промени в снимки, чрез Софтуерна /AI Hadoop бизнес сигурност

=>Може да се стигне до детайлни разлики, например цигли на покриви

В нашата комплексна система за Големи данни използваме следната работна дефиниция

Информационната сигурност е:

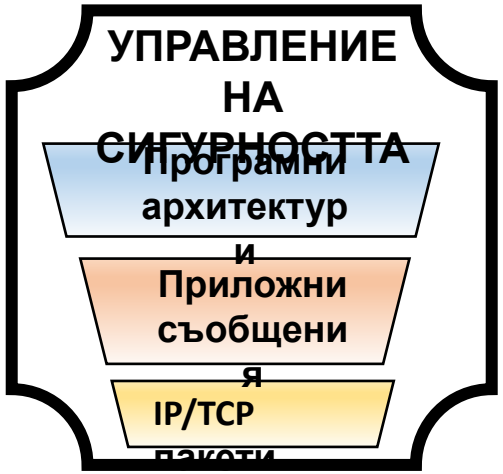
- **балансирана защита на поверителност, интегрираност и наличност на данни и процеси**
- **фокус - върху ефективното прилагане на бизнес политики**
- **управление - на базата на Управление на риска и стандарти**

 Кибер сигурността е част от Информационната сигурност

Развиваме нивата на управление на Кибер сигурността

1. Инфраструктурна сигурност – сигурност, чрез инфраструктурни (включително облачни) средства

- Ниво – TCP/IP
- Фокус – IP и TCP пакети
- Реализация - Чрез „мрежари“ конфигуриращи мрежови и сървърни системи
- **Адаптивна сигурност**



2. Софтуерна бизнес сигурност – сигурност, чрез софтуерни средства прилагащи бизнес правила

- Ниво - Програми архитектури за целите на сигурността (не приложни системи)
- Фокус – софтуерни компоненти и обвързването им (софтуерна архитектура)
- Реализация - Чрез „софтуерни разработчици“, кодиращи сигурност *на*

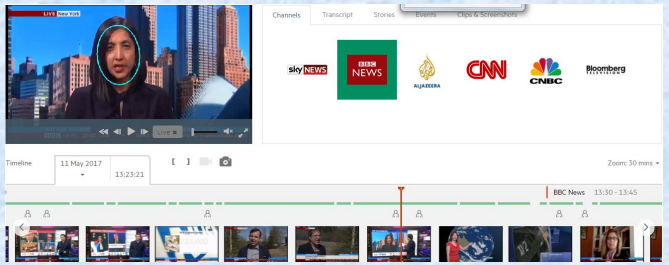
Работим с различни източници на данни при Системата за големи данни, изискващи сигурност

ДАННИ ОТ МРЕЖИ – прилагане на Инфраструктурна сигурност

Адаптивна сигурност

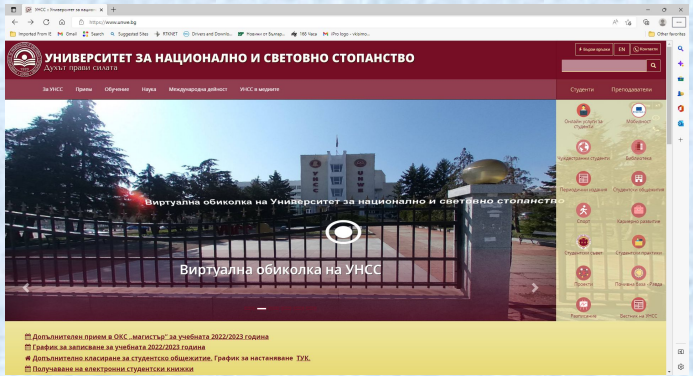
СПЕЦИФИЧНИ ДАННИ – прилагане на Софтуерна бизнес сигурност

Видео/аудио

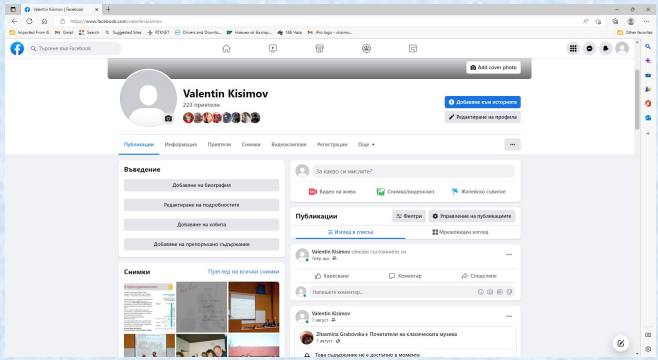


- Разпознаване на лица
- Разчитане на текст от екран
- Съхранение на видео, аудио и техни потоци

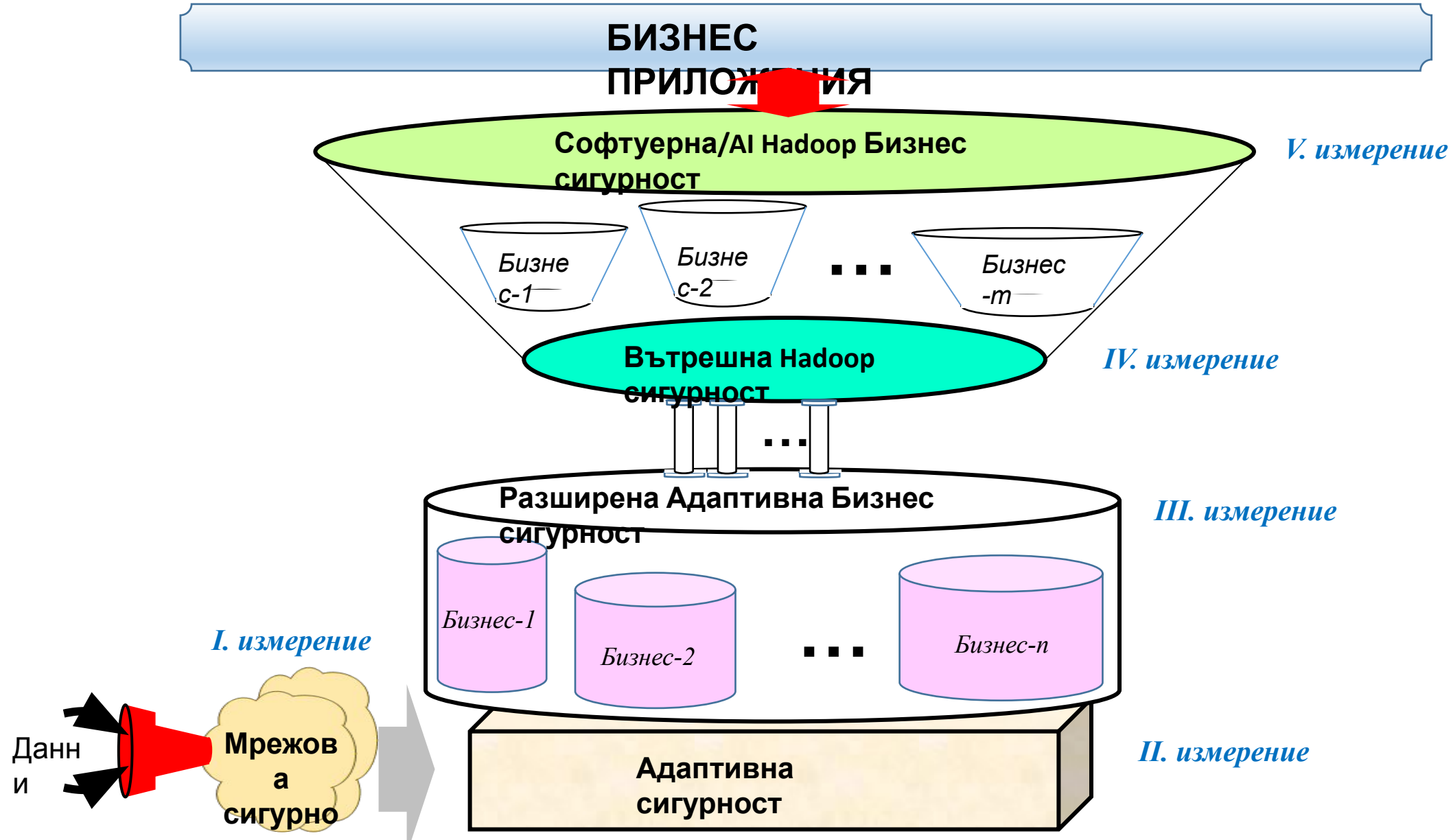
Уеб сайтове / Dark



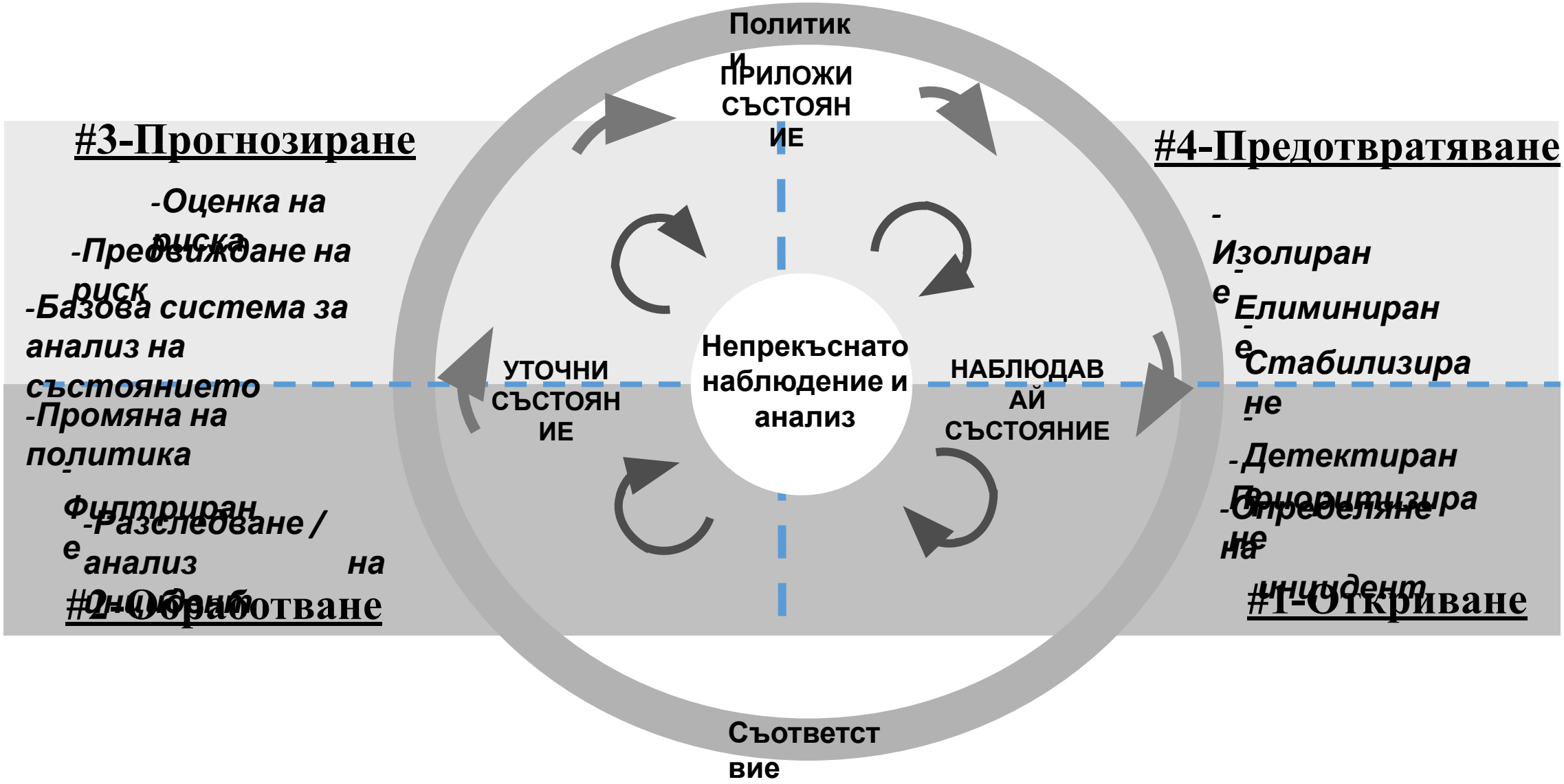
Социални



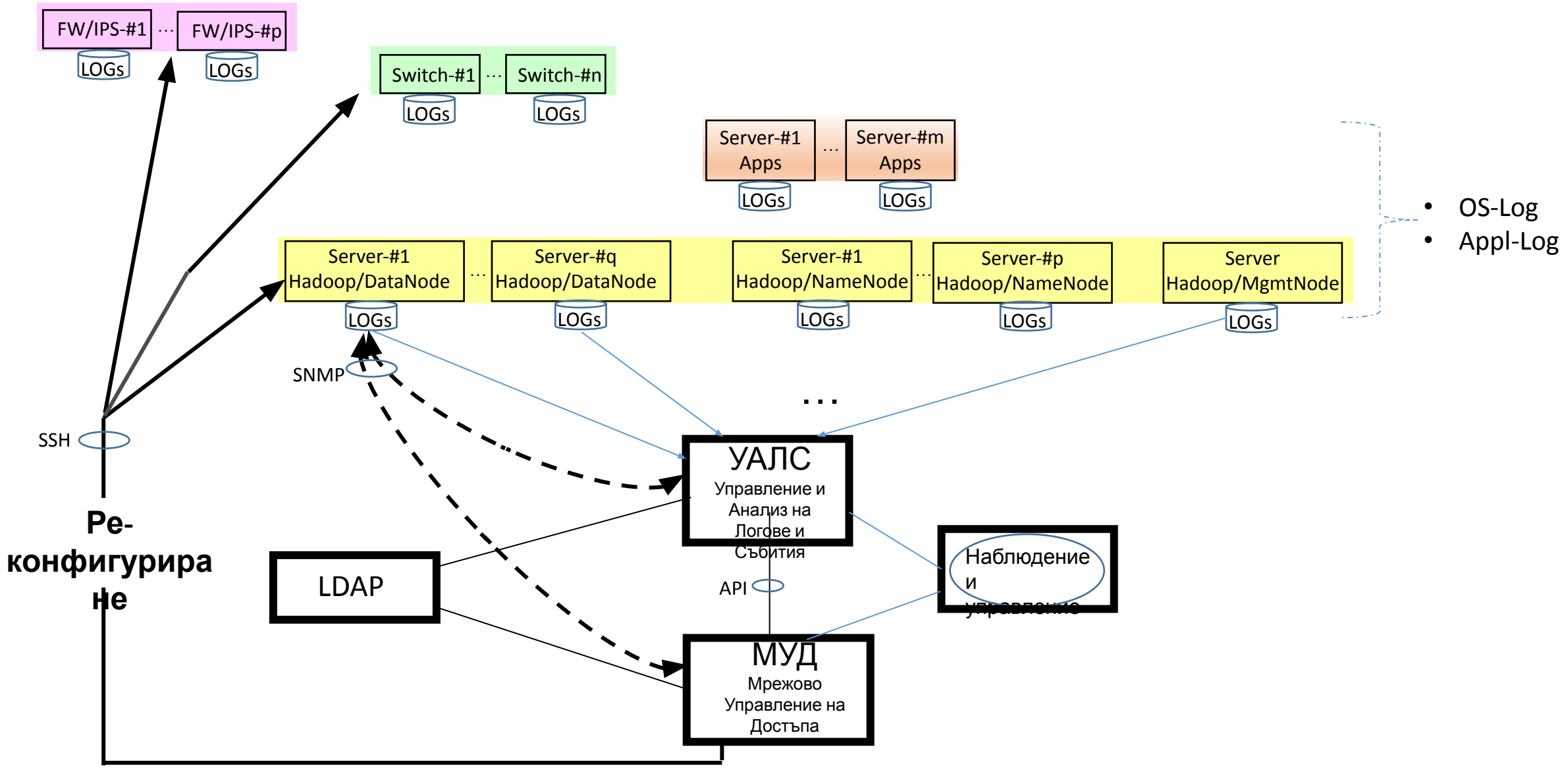
На тази база разработихме Кибер секюрити Архитектура в 5 измерения



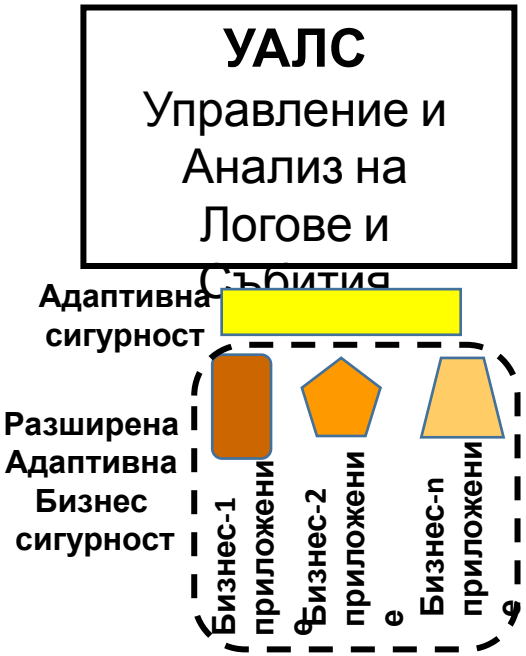
В Инфраструктурната сигурност използваме концепцията за Адаптивна сигурност разработена от Gartner



Разработихме Адаптивна секюрити архитектура за Система за големи данни



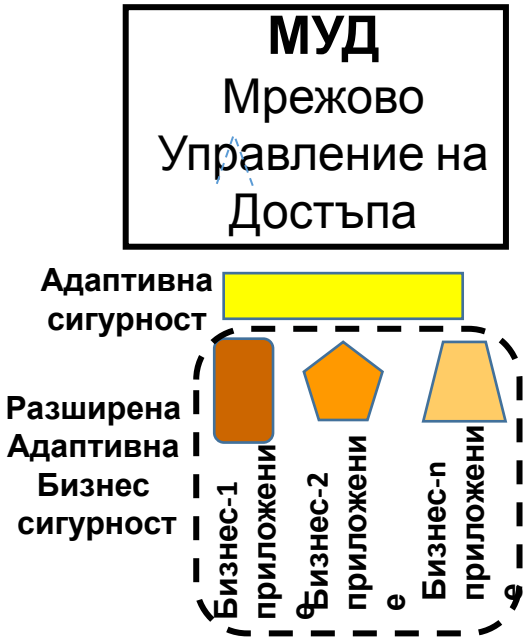
Създадохме Разширената Адаптивна Бизнес сигурност (1 от 2) - чрез УАЛС



- Анализ на логове, събития и аномалии наречени „***одитни данни***“

- използва политики за съхранение на одитни данни
- нормализира одитни данни
- използва таксономична класификация на одитните данни
- контекстно съпоставяне на данните в процеса на събирането им
- дефинира последователност от действия
- извършва корелации и създава правила за корелации
- създава съответствие с нормативни и законови актове, вътрешни политики
- създава е-доклади/отчети за събития
- прилага механизъм за „ранно предупреждение“

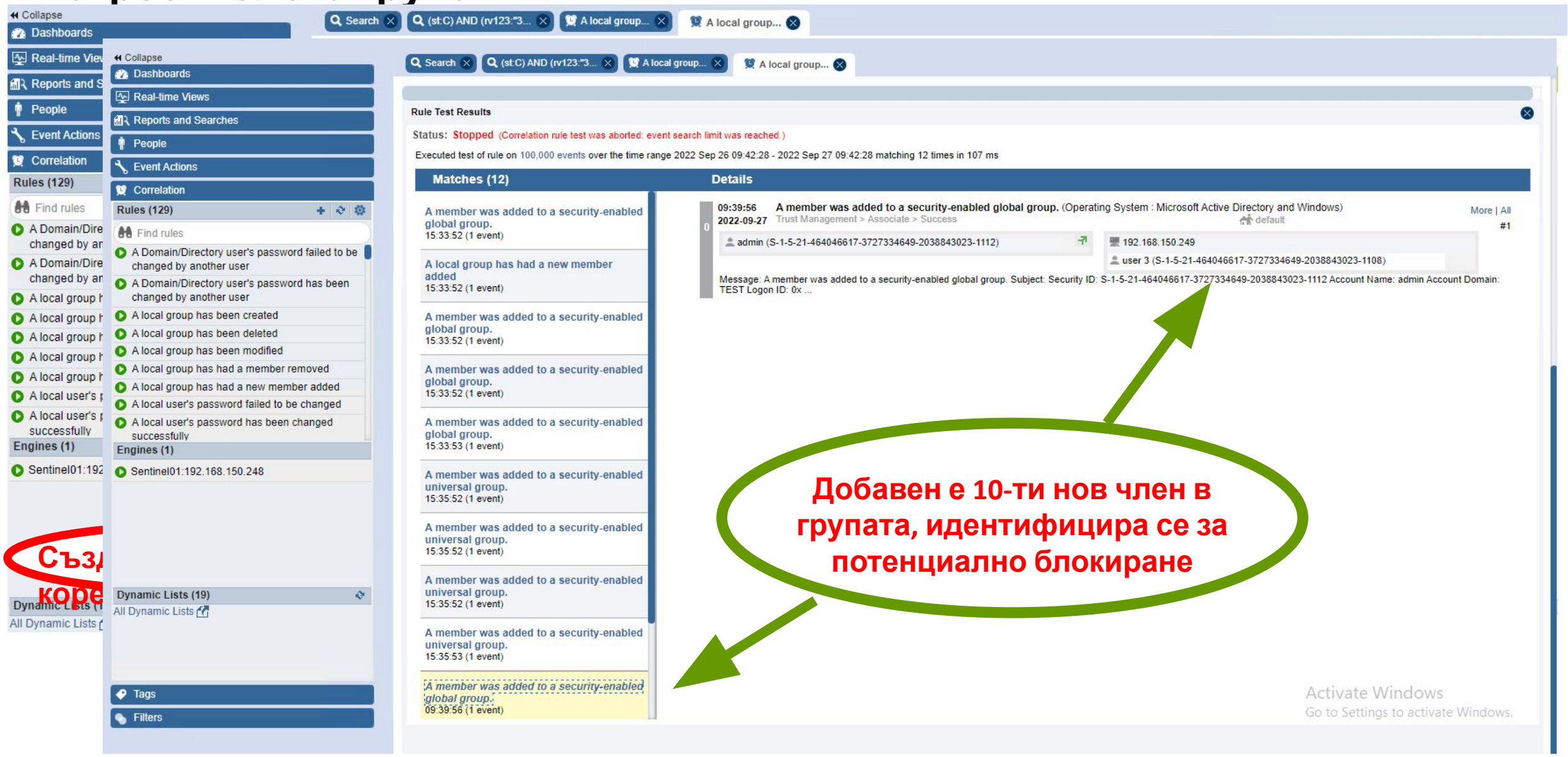
Създадохме Разширена Адаптивна Бизнес сигурност (2 от 2) - чрез МУД



- извлича, чрез API на е-доклади/отчети от УАЛС
- прилага правила за достъп до всички устройства – чрез техен мрежов порт (използвайки SNMP/Telnet/SSH) – *карантинен VLAN*

- анализира системни данни като: име на хост, IP адрес, операционна система
- наблюдава мрежата чрез: сканиране на портовете, сканиране на източниците от ARP (NDP) протокол - MAC-IP съответствие, (не) съвместими отговори от пакети
- извършва филтриране - минимум по IP адрес, име-хост, VLAN
- създава тревога - до деактивиране на мрежов порт
- прави ре-конфигурация, групови конфигурации и нови политики
- прехвърля устройства в карантинен VLAN до изясняване на статуса

Пример за Разширена Адаптивна Бизнес сигурност – създаване на Корелация за Проследяване добавянето на нови членове в потребителска група



Организирахме 7 нива на „Вътрешна Hadoop сигурност“

i. Централизирано автентикиране на потребителите – чрез LDAP и/или Kerberos

ii. Права за достъп на потребител до DataNode сървърите и сегментиране на данните – чрез разпространяване на потребителските акаунти използвайки System Security Services Deamon на Lunix

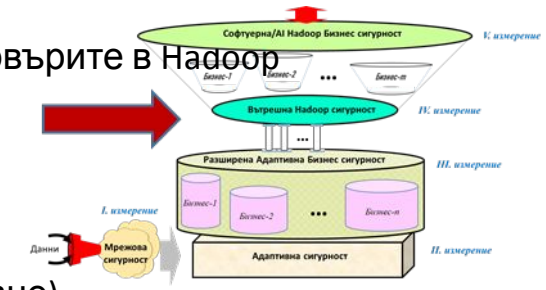
iii. Контрол на достъпа до HDFS директории и файлове - чрез присвояване на потребители или групи потребители на всяка директория и файл

iv. Централизиран Лист за управление на достъпа до Hadoop клъстера – чрез ACL създаден в NameNode

v. Механизъм за пълен одит: за данни (напр. произход) и потребител (напр. IP адрес)

vi. Защита и криптиране на данните намиращи се върху диск “data-at-rest” и на данни в движение “data-in-transit” в Hadoop клъстера – чрез TLS протокола между сървърите в Hadoop

vii. Управление на ключовете за криптиране на Клиент до Hadoop клъстера – чрез Navigator Key Trustee опериращ с ключове вътре в рамките на Hadoop системата (съхраняващ клиентските ключове и когато е нужно ги дава на Клиента за декриптиране)



=>БИЗНЕС ОРИЕНТИРАНИ ФУНКЦИИ ЗА СИГУРНОСТ (ЗА КЛИЕНТ, ПРОЦЕС И ДАННИ)

Развихме понятието „Софтуерната бизнес сигурност“ до „Софтуерна/AI Hadoop бизнес сигурност“ – най-високо ниво на кибер сигурост

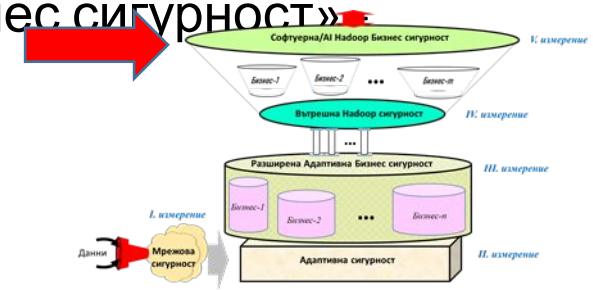
- ДЕФИНИЦИЯ - Мерки за сигурност ***създадени на ниво приложение***, които имат за цел да предотвратят **кражба, неправомерно използване, изтриване**/изчезване на данни или приложения (или част от тях), **модификация** на данни и приложения или **промяна на данни и последователността на изпълнение на процеси**.

- Вграждане на **Статистически методи** – медиана, претеглена стойност, стандартно отклонение, класифициране, групиране, регресия, корелация и пр.

- Вграждане на **Изкуствения интелект** – Spark/Hadoop със специална AI/ML библиотека.

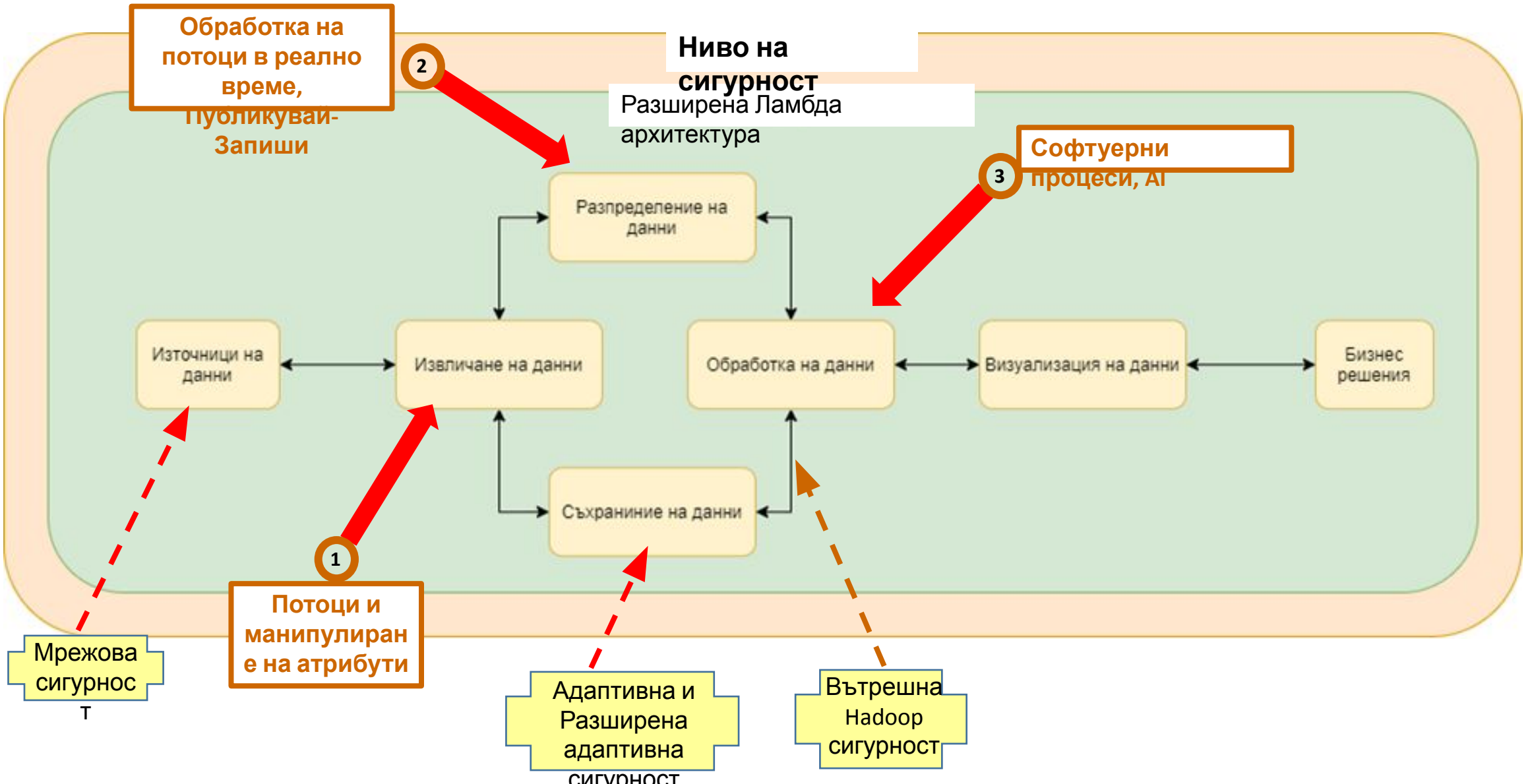
- Правилата за сигурност съответстващи с определен вид бизнес - «Бизнес сигурност» – **Java/Python**

- Включва Бизнес процеси и Управление на бизнес процесите (BPM).

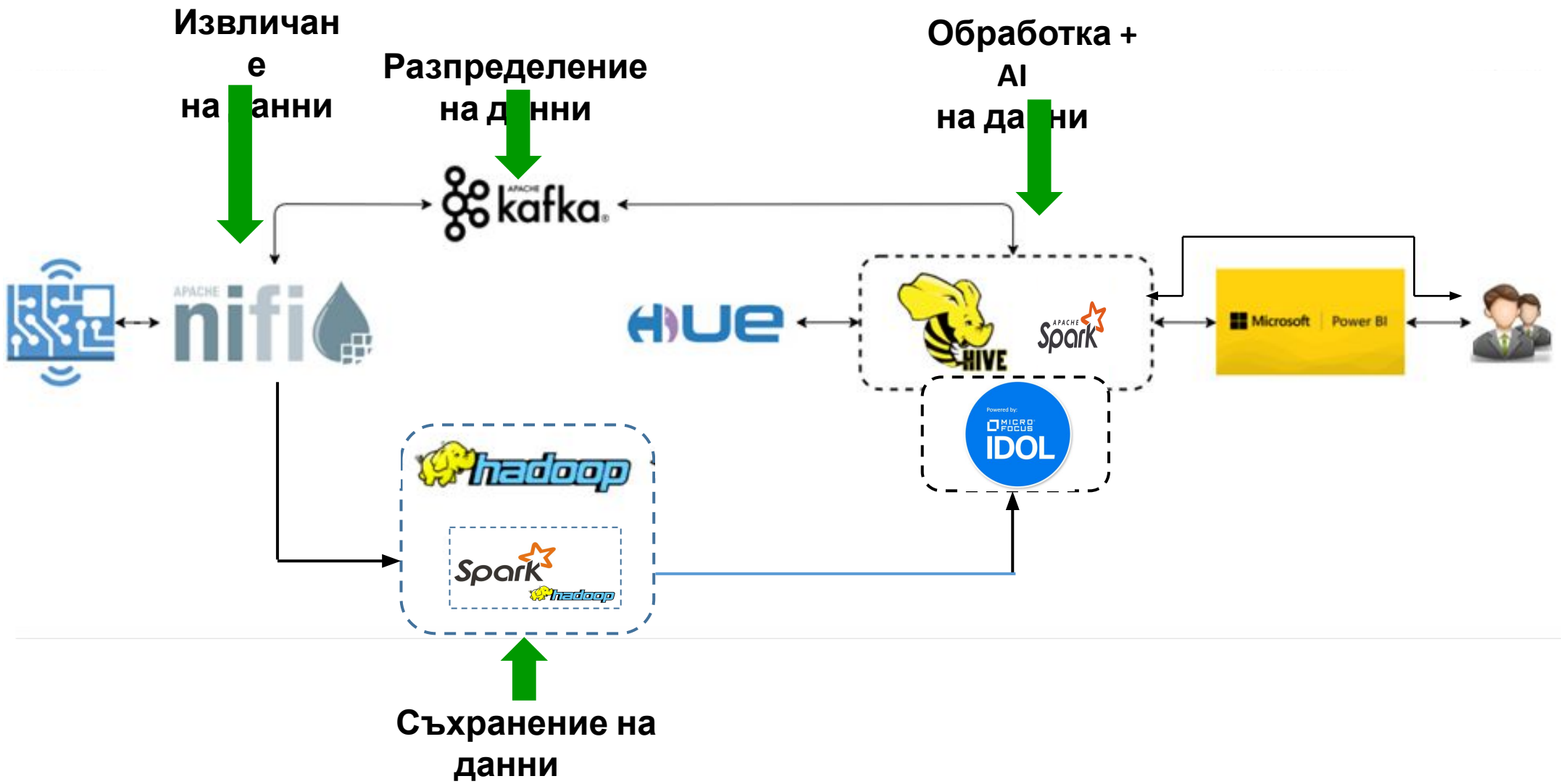


=>Обработва заплахи и събития като размито множество на стриктни бизнес правила

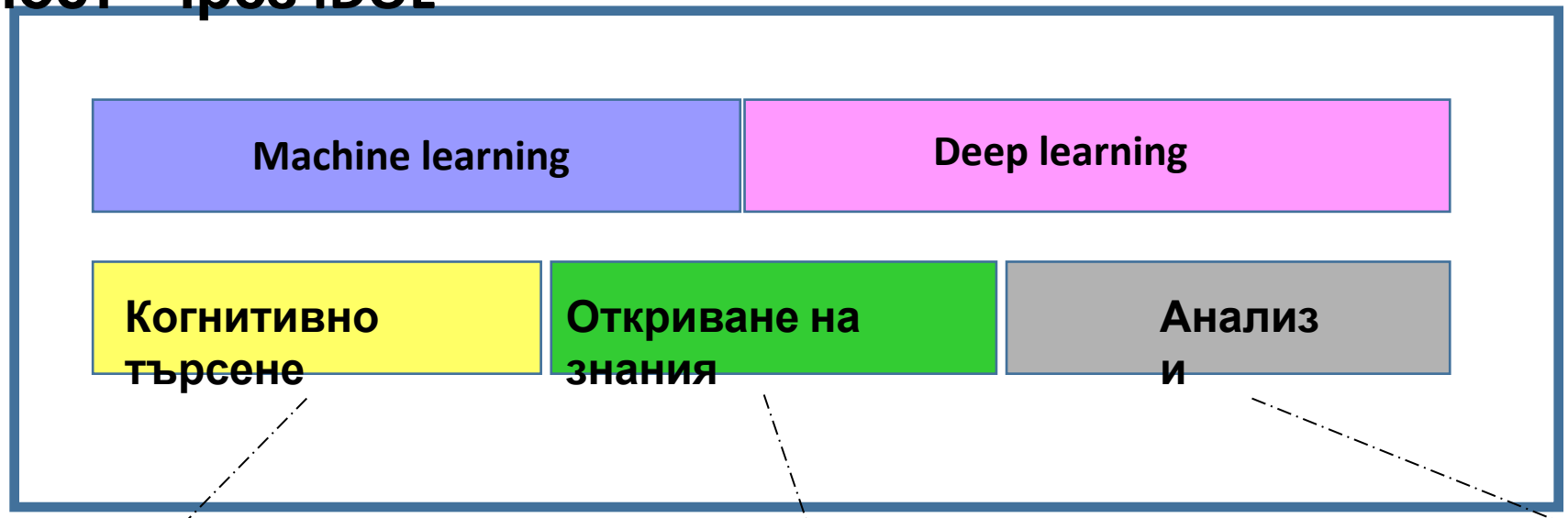
„Софтуерната/AI Hadoop бизнес сигурност“ използва Разширена Ламбда архитектурата



Софтуерна архитектура на „Софтуер /AI Hadoop бизнес сигурността“



Същност на *Усилен изкуствен интелект върху неструктурирани данни* при „Софтуер /AI Hadoop бизнес сигурност“ чрез IDOL

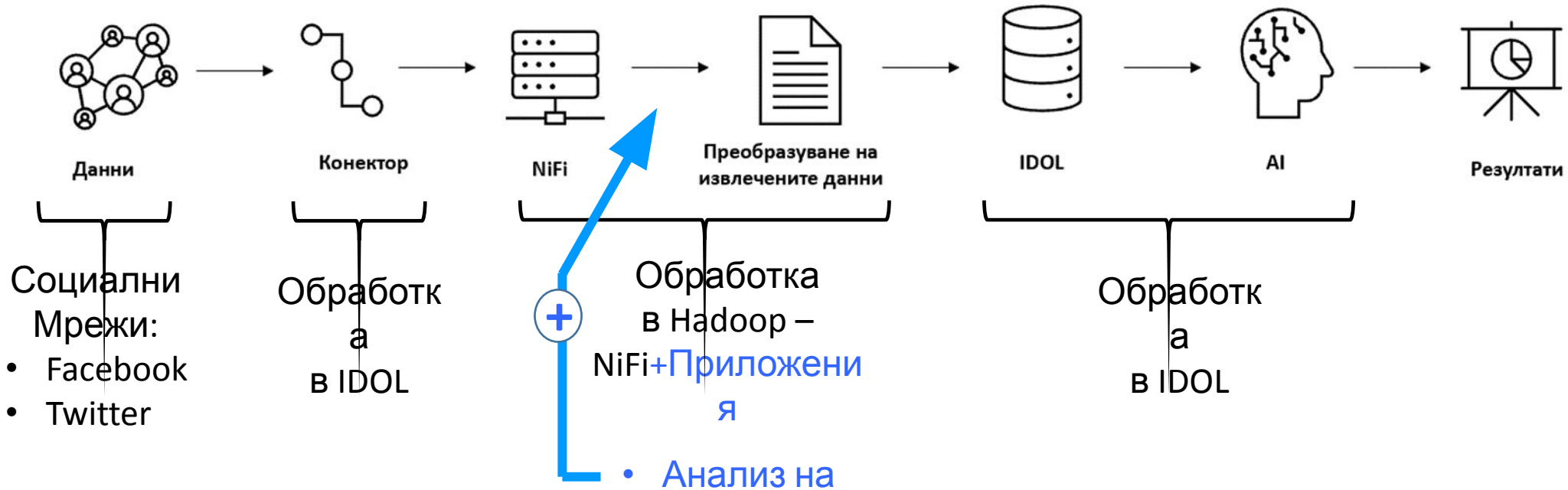


Търсене с използване на AI, търсене с различни видове данни

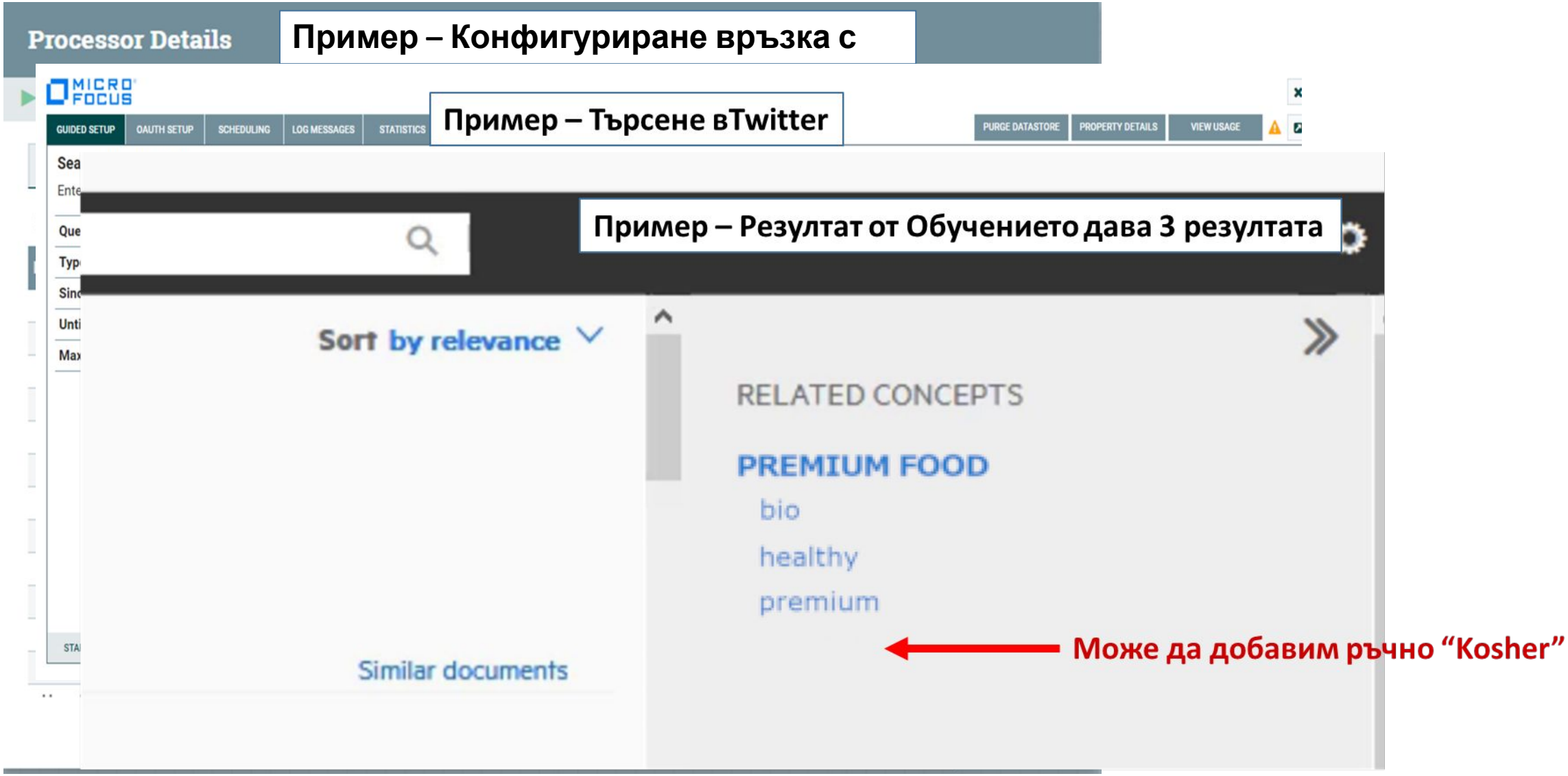
Работи с неформатирани въпроси, използва машинно обучение и дълбоки невронни мрежи за разпознаване на модели, тенденции и взаимоотношения скрити в данните – напр. свързва туитове с разпознат регистрационен номер на кола

Функции за аудио и видео анализ, задвижвани от AI, като откриване на събития, идентификация на човек в събитие, бързо разбиране на контекста и съдържанието на аудио / видео файловете

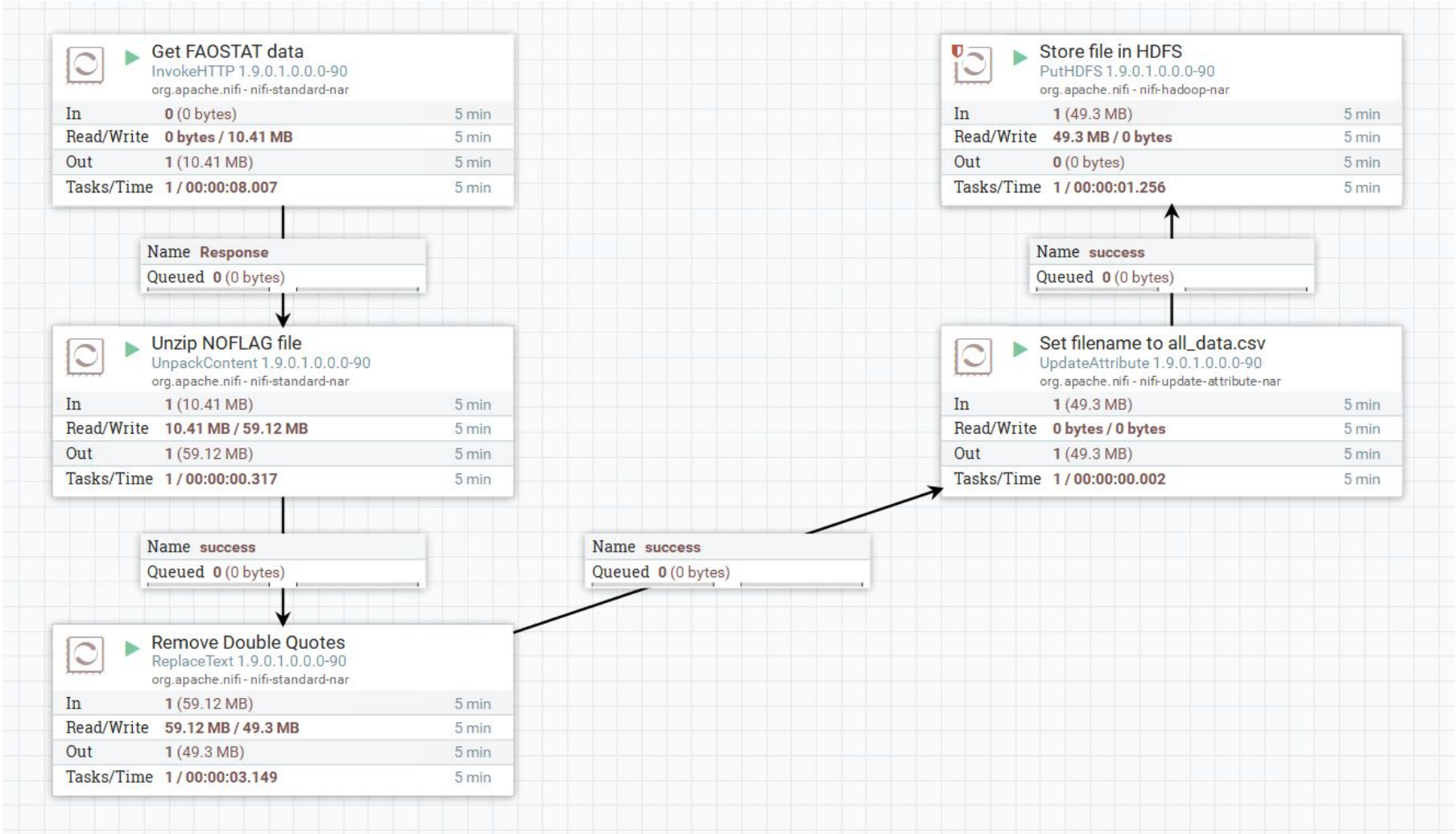
Софтуерна архитектура на „Софтуер /AI Hadoop бизнес сигурност“ се поддържа и чрез IDOL система, интегрирана с Hadoop



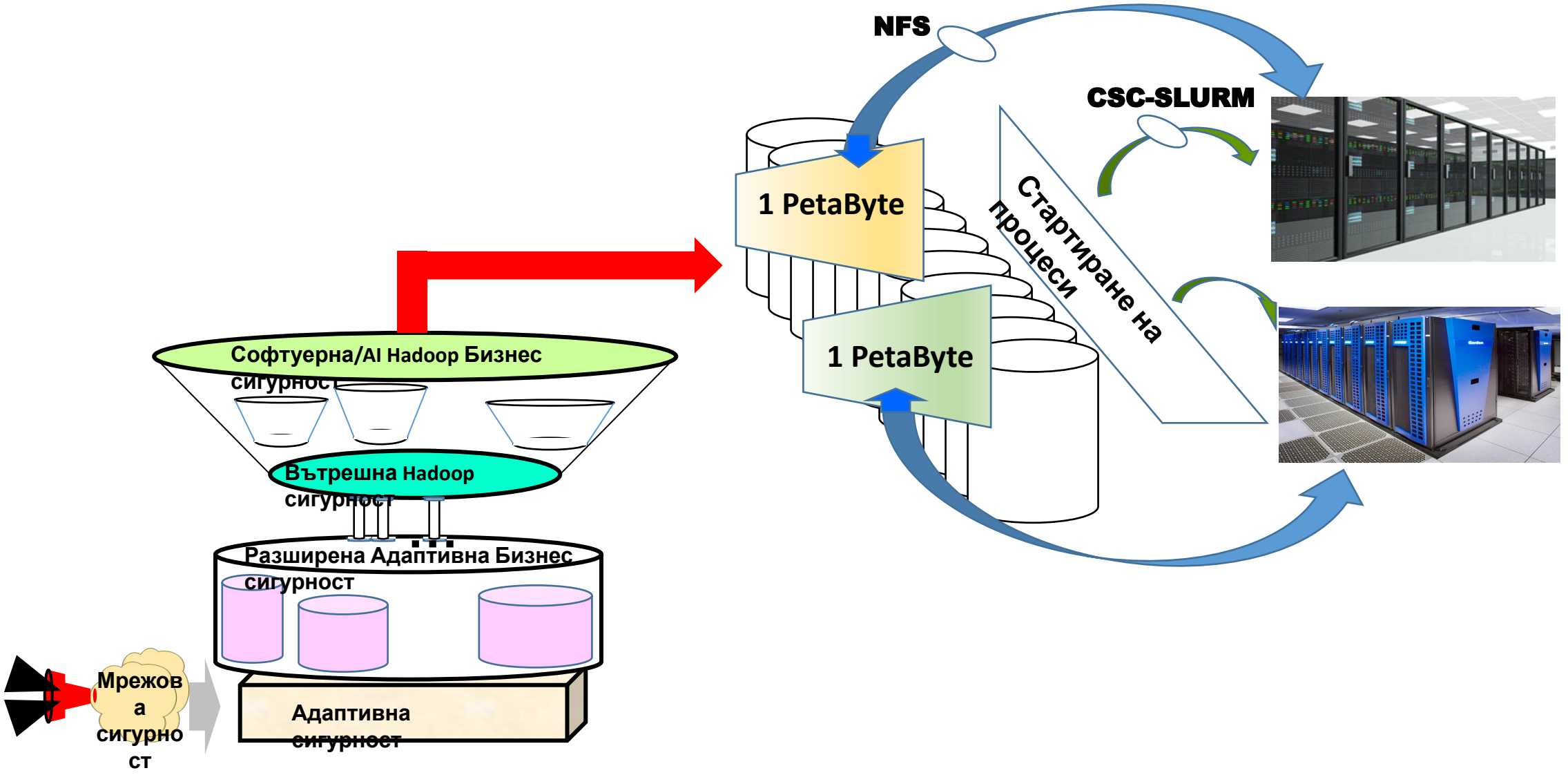
Пример – част от „Софтуер/AI Hadoop бизнес сигурност“ за работа с данни от Twitter - за сигурност на данни – *наличност (availability) на данни* – чрез IDOL



Пример – част от „Софтуер/AI Hadoop бизнес сигурност“ на данни за ечемик – *наличност (availability) на данни* чрез NiFi



Системата за големи данни осигурява сигурни данни за работа на Суперкомпютрите и стартира сигурни процеси в тях



Създадена е Съвкупност от Големи данни за изследване

БЛАГОДАРЯ !

Въпроси ?