

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



Суперкомпютър

Система за големи данни

София
17.11.2022



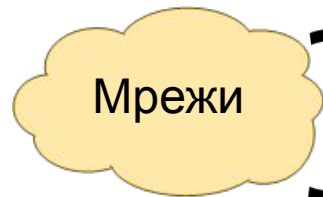
**УНИВЕРСИТЕТ ЗА НАЦИОНАЛНО
И СВЕТОВНО СТОПАНСТВО**



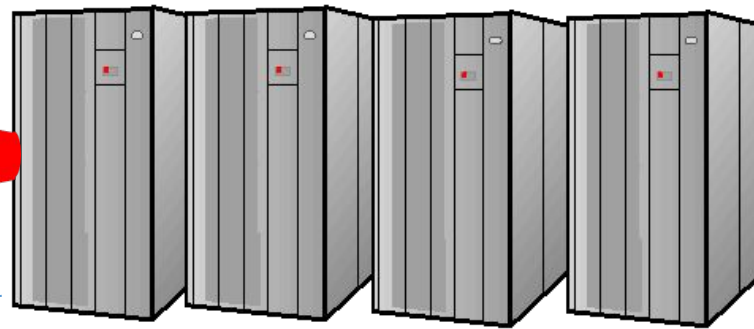
Кибер сигурност на Системата за големи данни и роля при интеграцията ѝ със Суперкомпютър

2xСуперкомпютри
(СК)

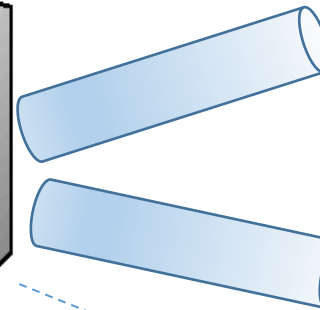
СИСТЕМА ЗА ГОЛЕМИ ДАННИ
(СГД)



Мрежи



интегриране



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

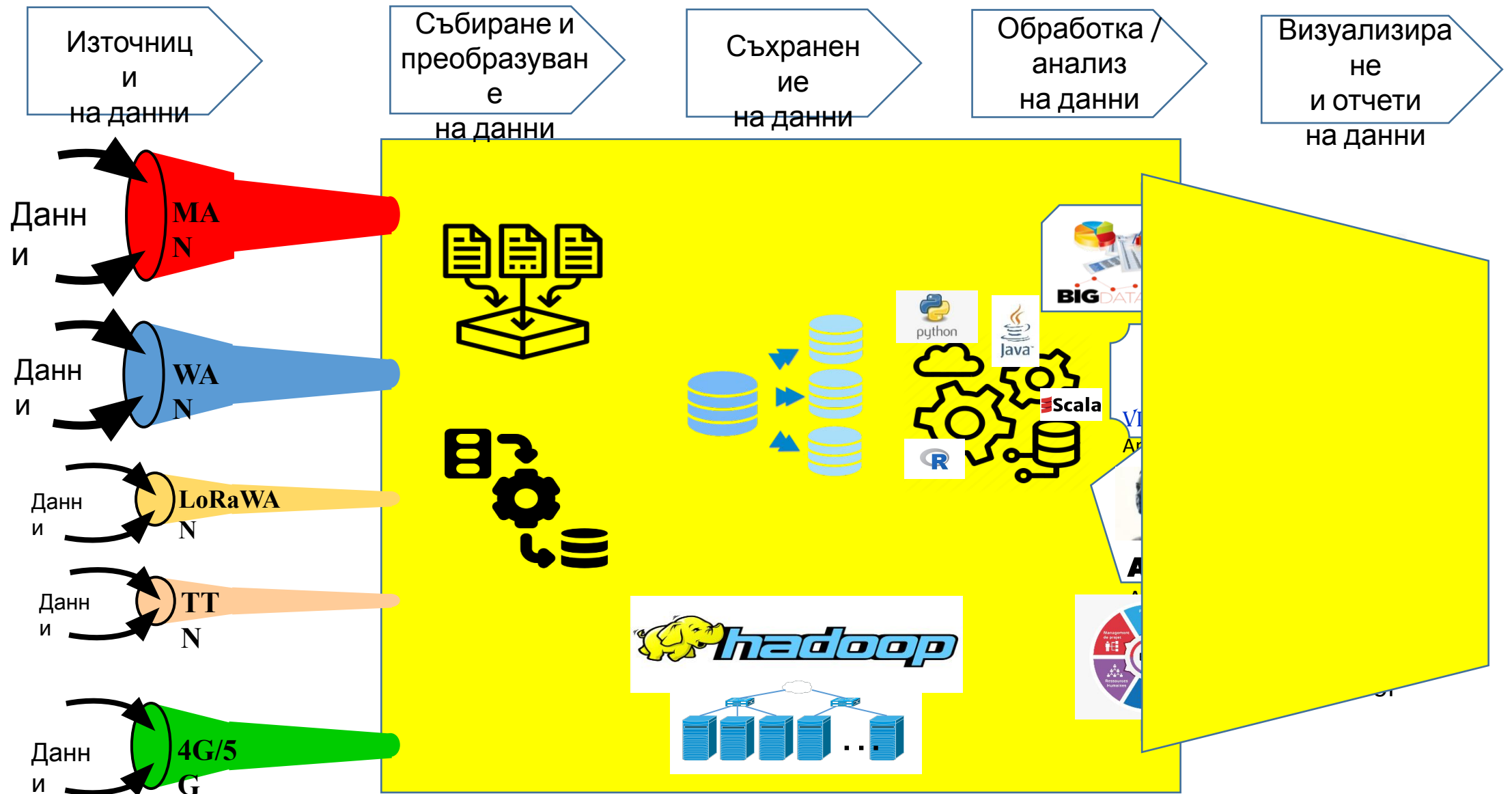
Система за Големи данни като

ИНСТРУМЕНТ

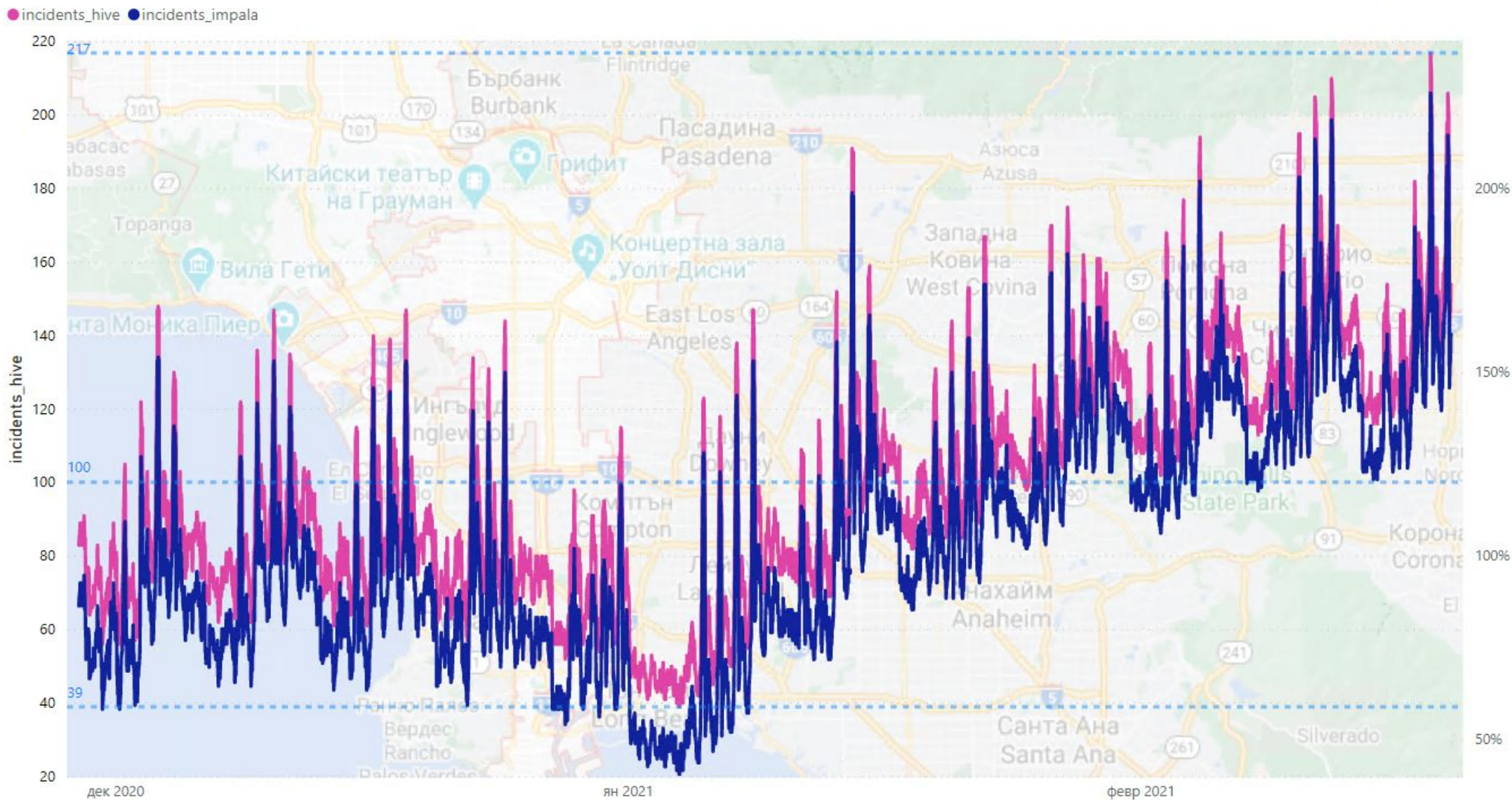
за Кибер сигурността

- 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



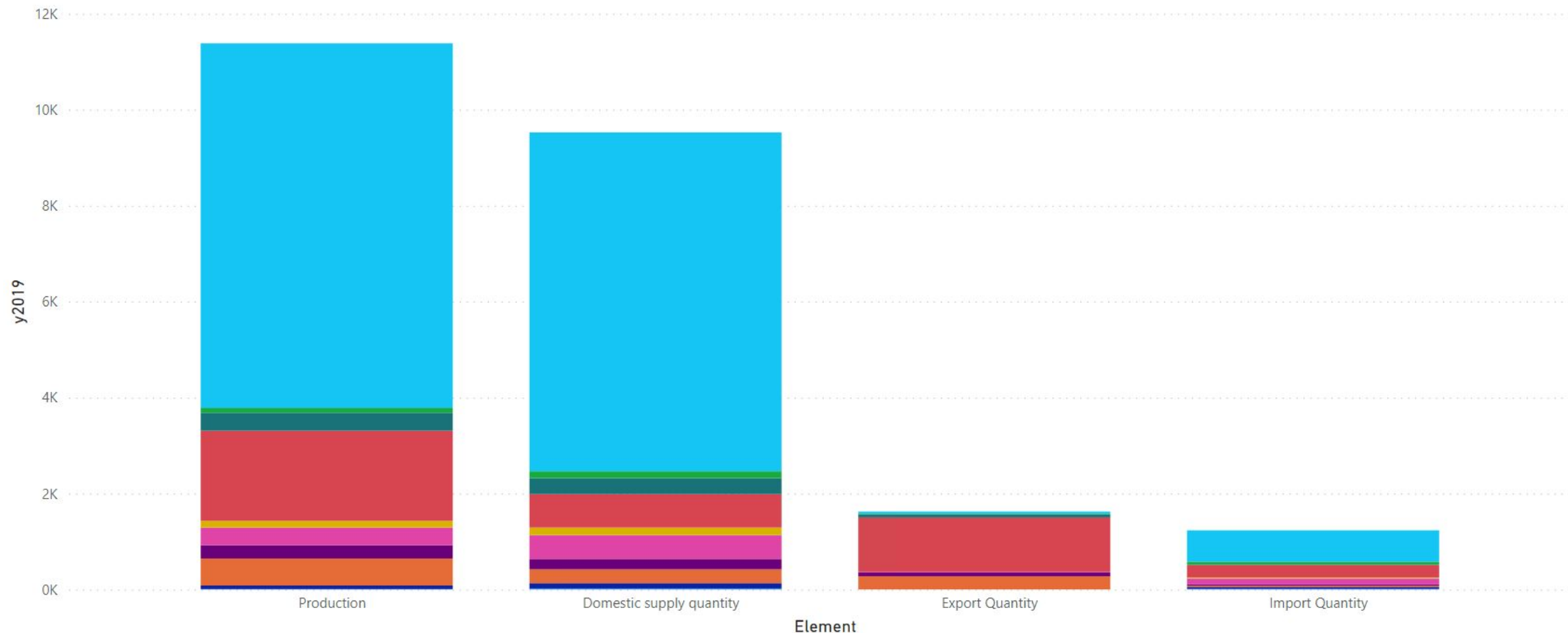
Пример – транспортни инциденти в LA областта обработени, чрез Софтуерна/AI Nadoor бизнес сигурност (с участие на NiFi и Impala) и визуализирани чрез HIVE



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



Country ● Albania ● Bosnia and Herzegovina ● Bulgaria ● Croatia ● Greece ● Montenegro ● North Macedonia ● Romania ● Serbia ● Slovenia ● Turkey



Пример за разпознаване на малки промени в снимки, чрез Софтуерна /AI Надзор 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:

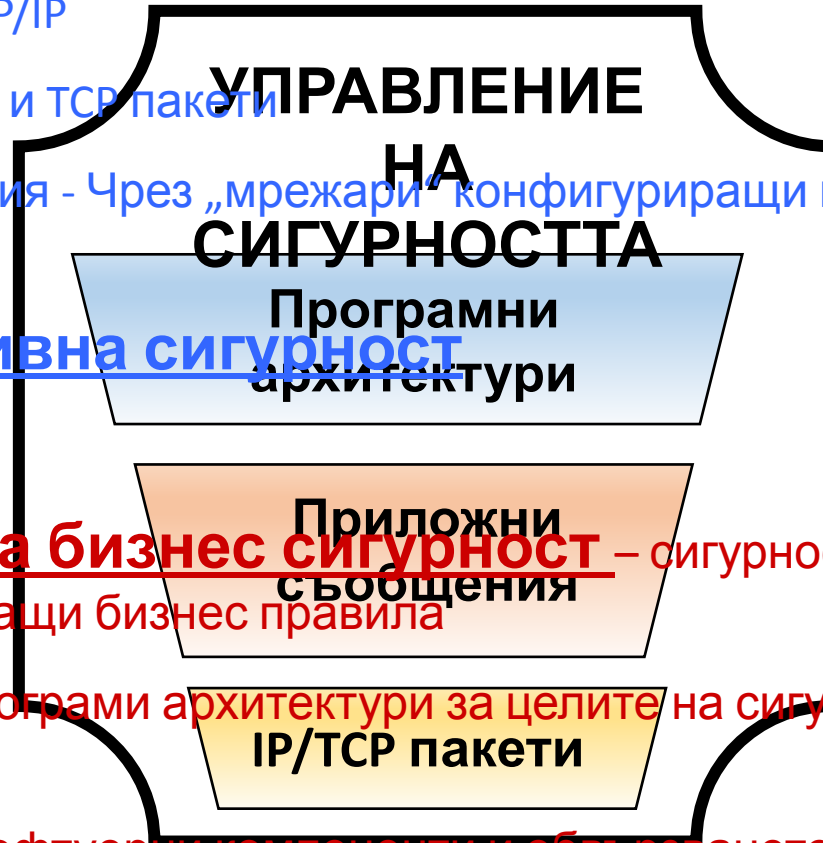
- балансирана защита на поверителност, интегрираност и наличност на данни и процеси
- фокус - върху ефективното прилагане на бизнес политики
- управление - на базата на Управление на риска и стандарти

□ Кибер сигурността е част от Информационната сигурност

Развиваме нивата на управление на Кибер сигурността

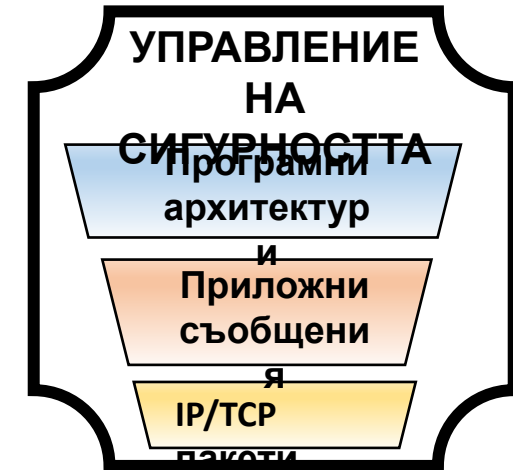
1. **Инфраструктурна сигурност** – сигурност, чрез инфраструктурни (включително облачни) средства

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



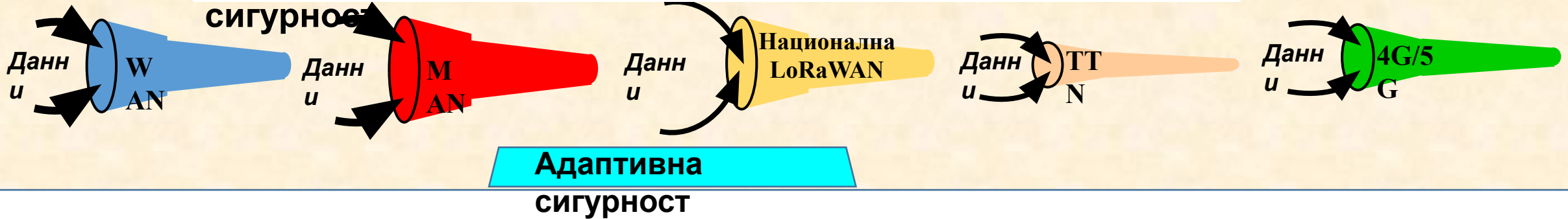
2. **Софтуерна бизнес сигурност** – сигурност, чрез софтуерни средства прилагачи бизнес правила

- ❖ 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



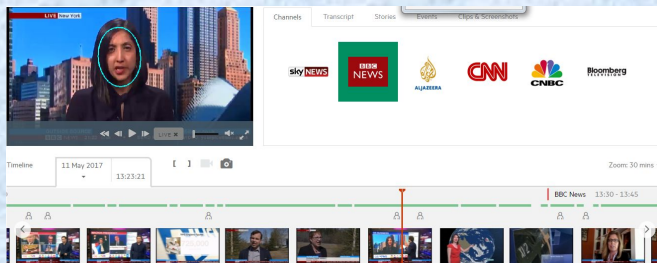
Работим с различни източници на данни при Системата за големи данни, изискващи сигурност

ДАНИИ ОТ МРЕЖИ – прилагане на Инфраструктурна сигурност



СПЕЦИФИЧНИ ДАНИИ – прилагане на Софтуерна бизнес

Видео/аудио сигурност

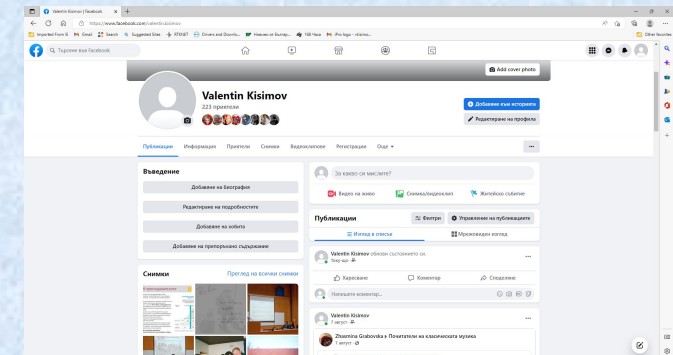


- Разпознаване на лица
- Разчитане на текст от екран
- Съхранение на видео, аудио и техни потоци

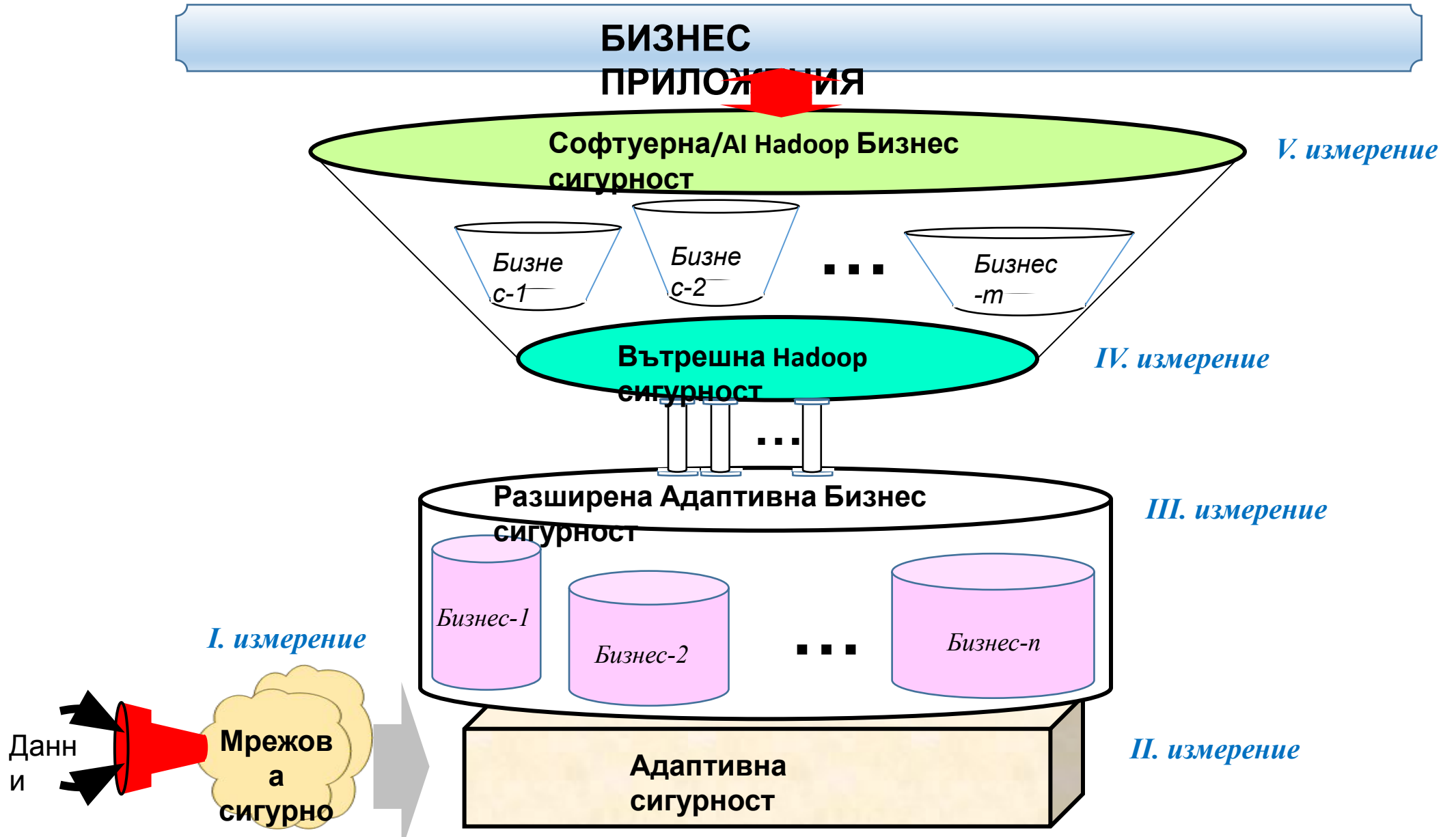
Уеб сайтове / Dark



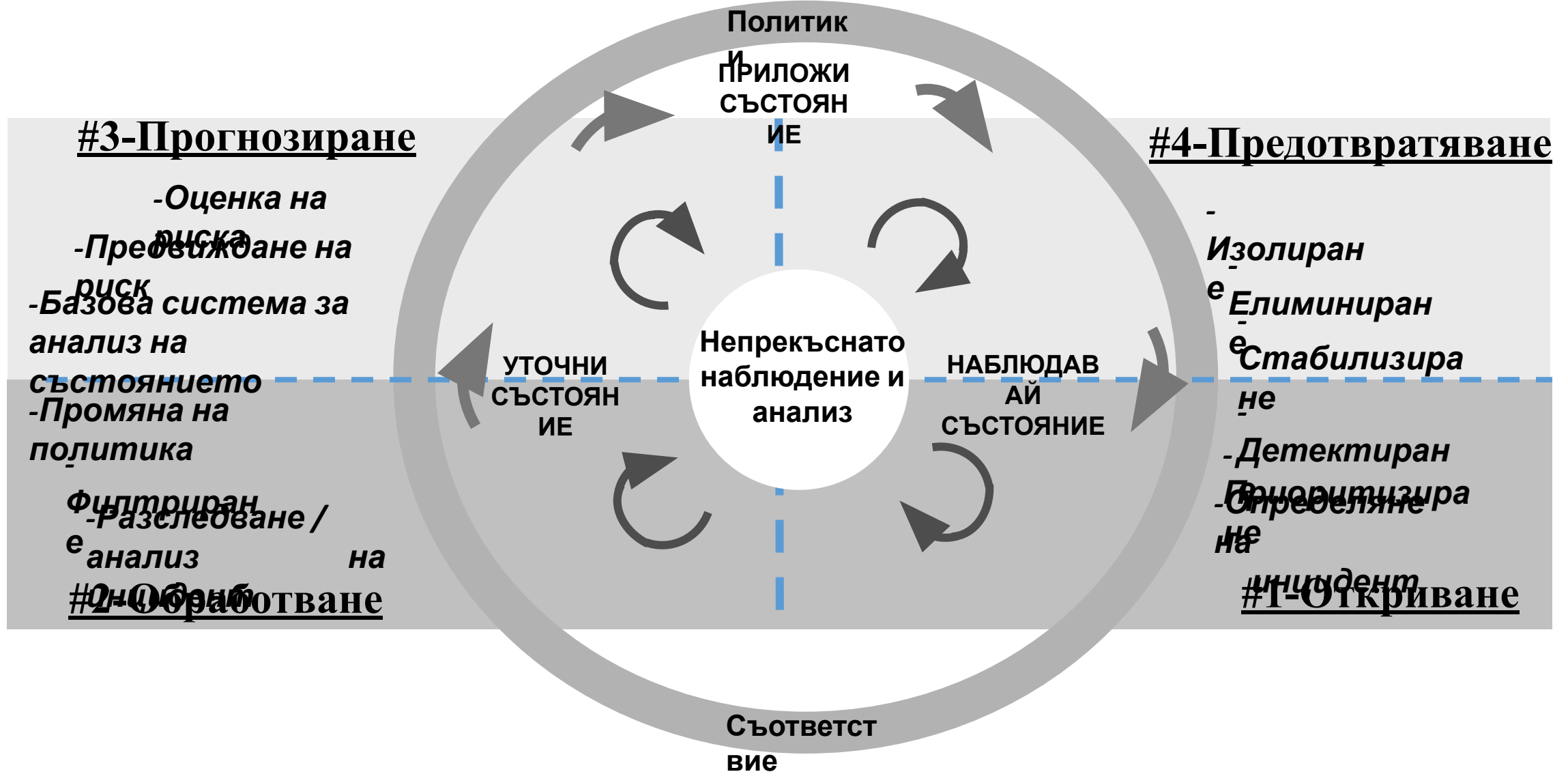
Социални



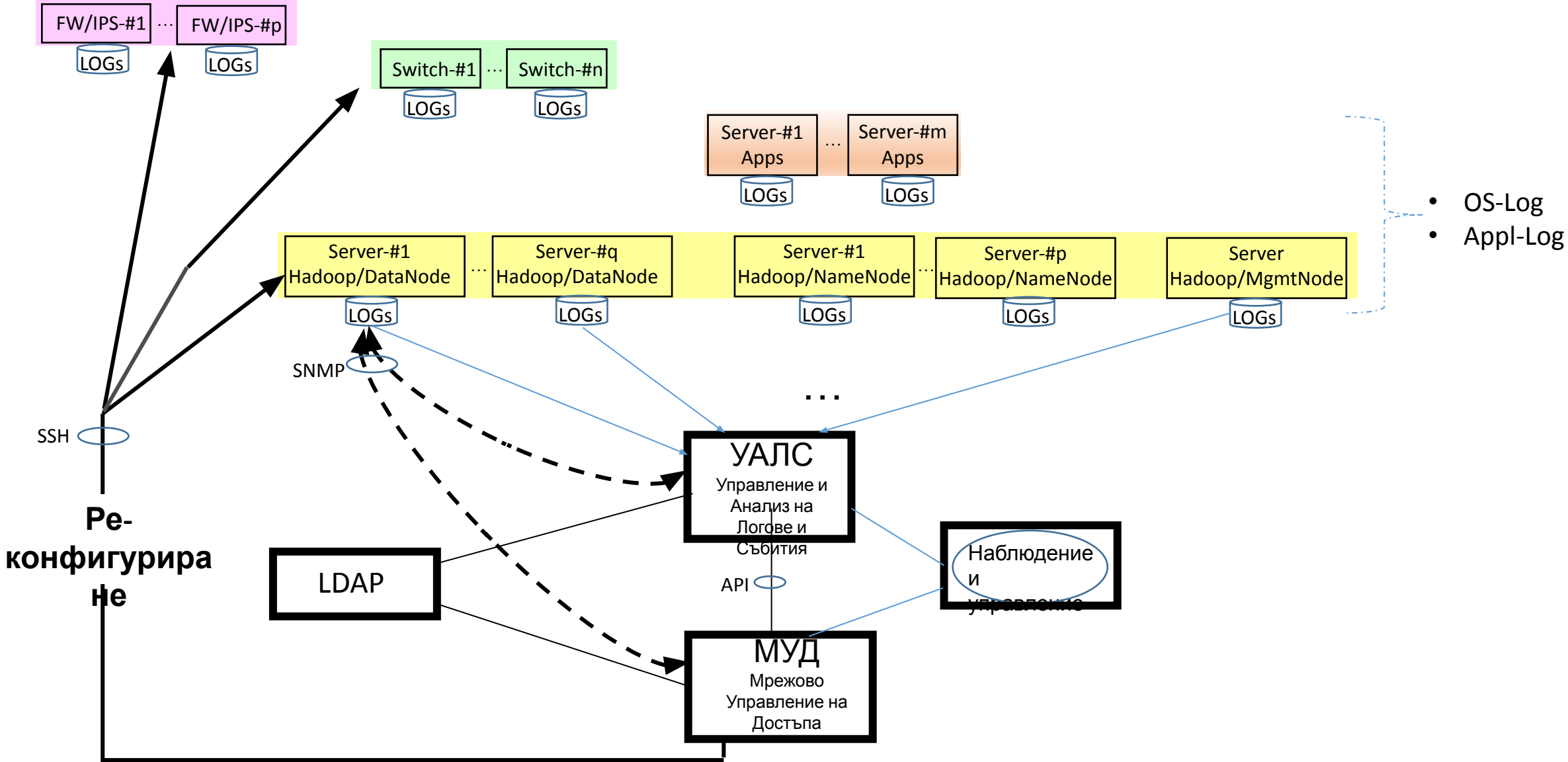
На тази база разработихме Кибер секюрити Архитектура в 5 измерения



В Инфраструктурната сигурност използваме концепцията за Адаптивна сигурност разработена от Gartner



Разработихме Адаптивна секюрити архитектура за Система за големи данни

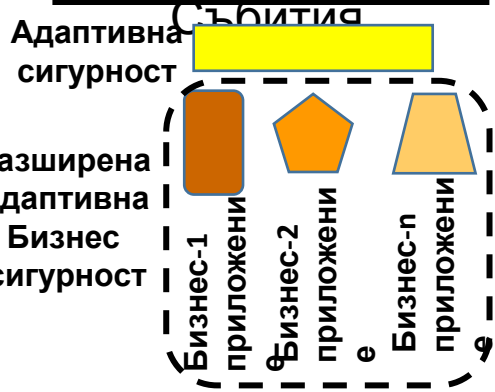


Създадохме Разширената Адаптивна Бизнес сигурност (1 от 2) - чрез УАЛС

УАЛС
Управление и
Анализ на
Логове и



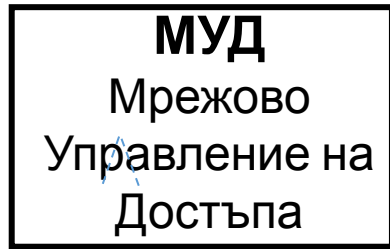
- Анализ на логове, събития и аномалии наречени „**одитни данни**“



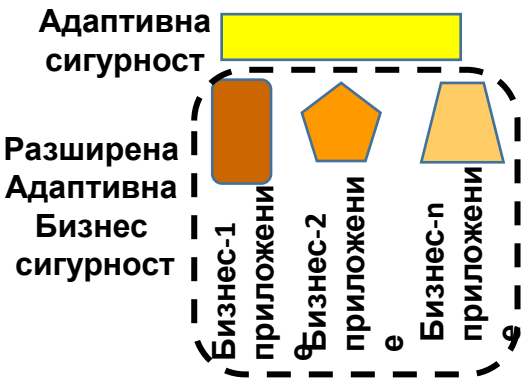
**Разширена
Адаптивна
сигурност за
конкретен бизнес**

- 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

Създаване на корелация

Rule Test Results

Status: **Stopped** (Correlation rule test was aborted: event search limit was reached.)

Executed test of rule on 100,000 events over the time range 2022 Sep 26 09:42:28 - 2022 Sep 27 09:42:28 matching 12 times in 107 ms

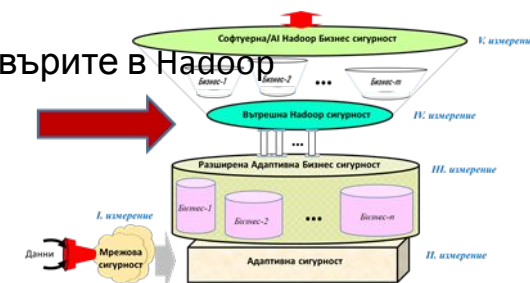
Matches (12)	Details
A member was added to a security-enabled global group. 15:33:52 (1 event)	09:39:56 A member was added to a security-enabled global group. (Operating System : Microsoft Active Directory and Windows) 2022-09-27 Trust Management > Associate > Success admin (S-1-5-21-464046617-3727334649-2038843023-1112) 192.168.150.249 user 3 (S-1-5-21-464046617-3727334649-2038843023-1108) Message: A member was added to a security-enabled global group. Subject: Security ID: S-1-5-21-464046617-3727334649-2038843023-1112 Account Name: admin Account Domain: TEST Logon ID: 0x ...
A local group has had a new member added 15:33:52 (1 event)	
A member was added to a security-enabled global group. 15:33:52 (1 event)	
A member was added to a security-enabled global group. 15:33:52 (1 event)	
A member was added to a security-enabled global group. 15:33:53 (1 event)	
A member was added to a security-enabled universal group. 15:35:52 (1 event)	
A member was added to a security-enabled universal group. 15:35:52 (1 event)	
A member was added to a security-enabled universal group. 15:35:52 (1 event)	
A member was added to a security-enabled universal group. 15:35:53 (1 event)	
A member was added to a security-enabled global group. 09:39:56 (1 event)	

Добавен е 10-ти нов член в групата, идентифицира се за потенциално блокиране

Activate Windows
Go to Settings to activate Windows.

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 Linux
- 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)

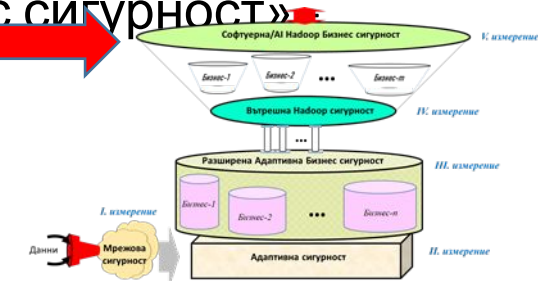


=>БИЗНЕС ОРИЕНТИРАНИ ФУНКЦИИ ЗА СИГУРНОСТ

(ЗА КЛИЕНТ ПРОЦЕС И ДАННИ)

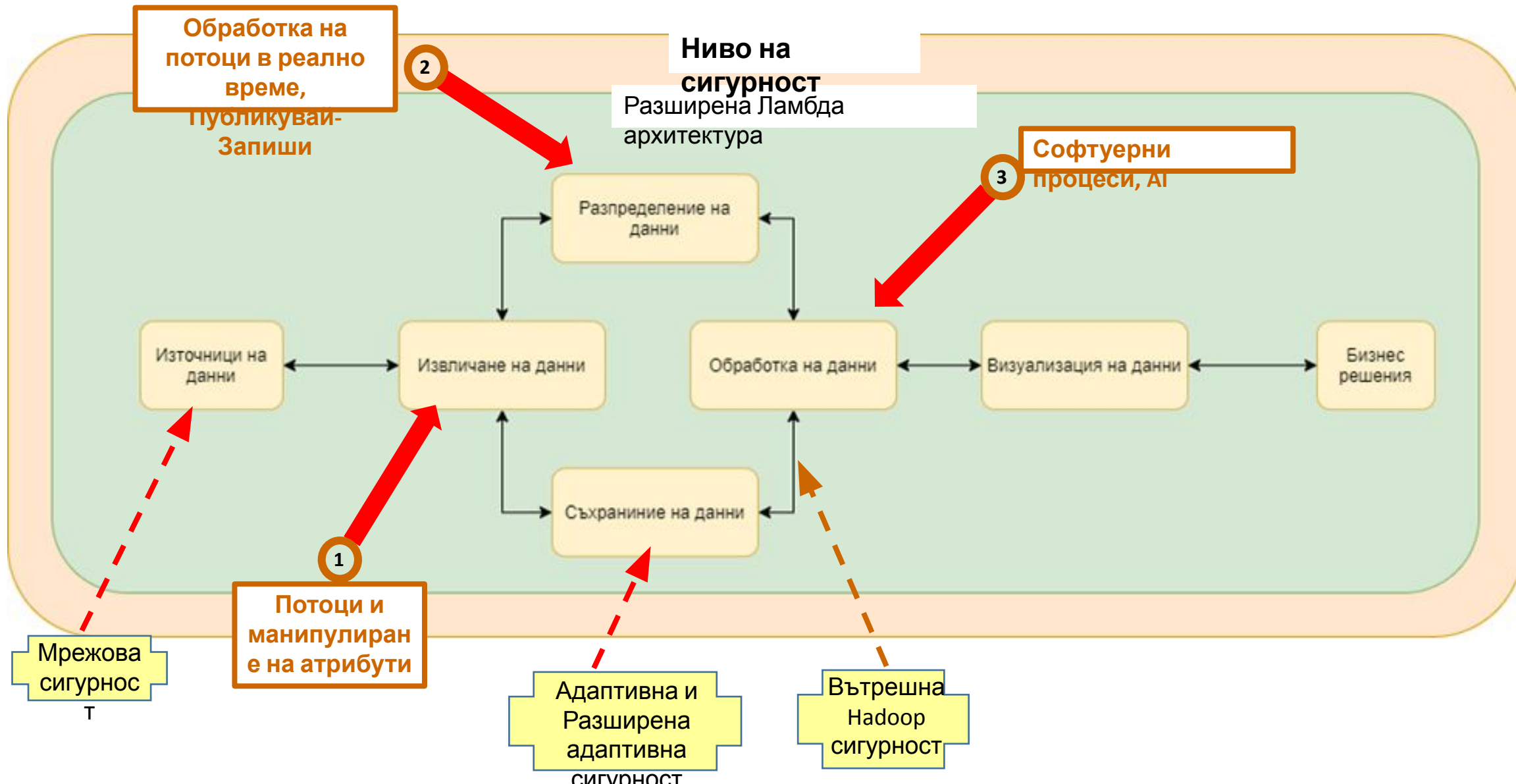
Развихме понятието „Софтуерната бизнес сигурност“ до „Софтуерна/AI Hadoop бизнес сигурност“ – най-високо ниво на кибер сигурост

- 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).

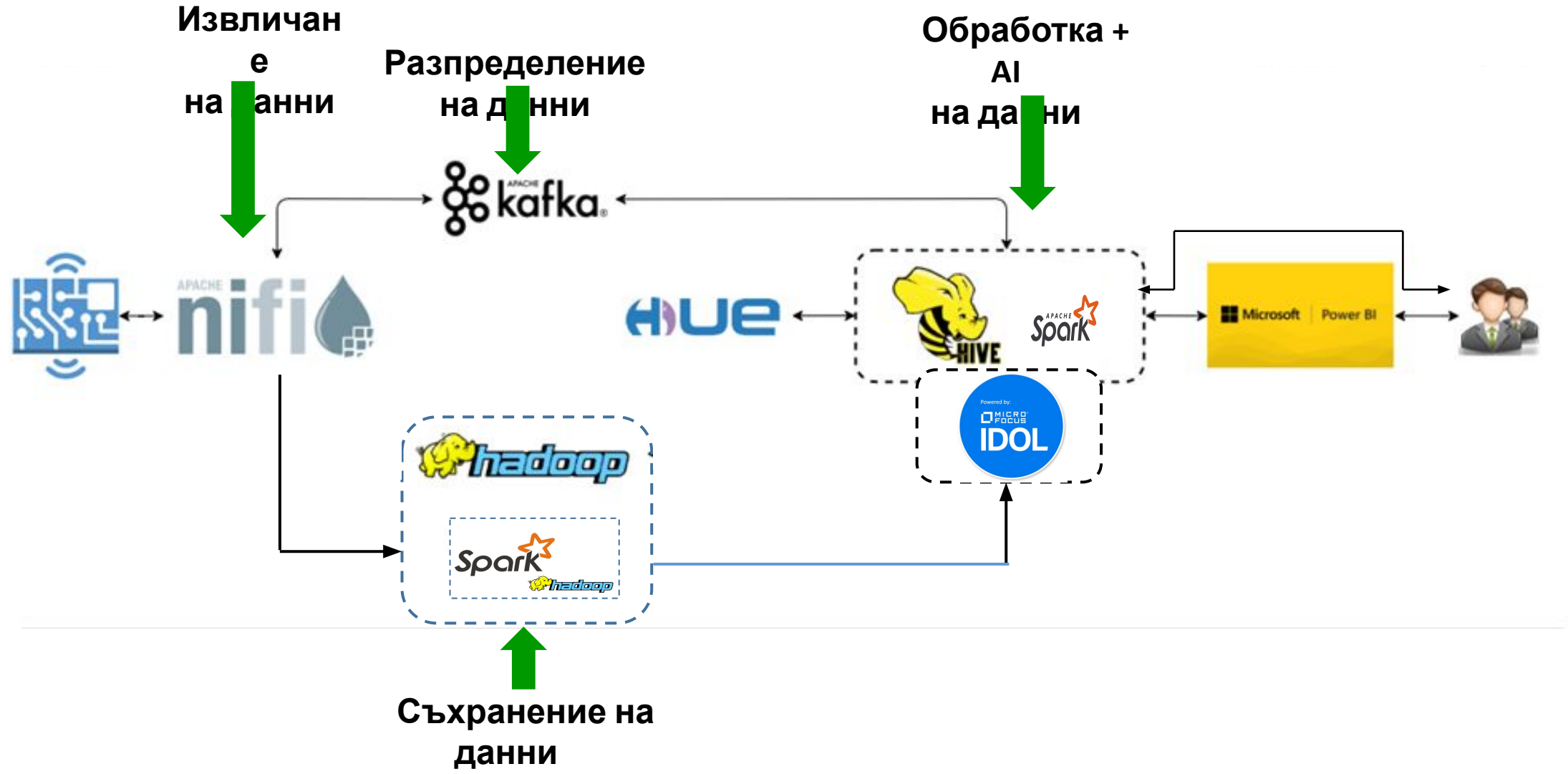


=>Обработка заплахи и събития като размито множество на стриктни бизнес правила

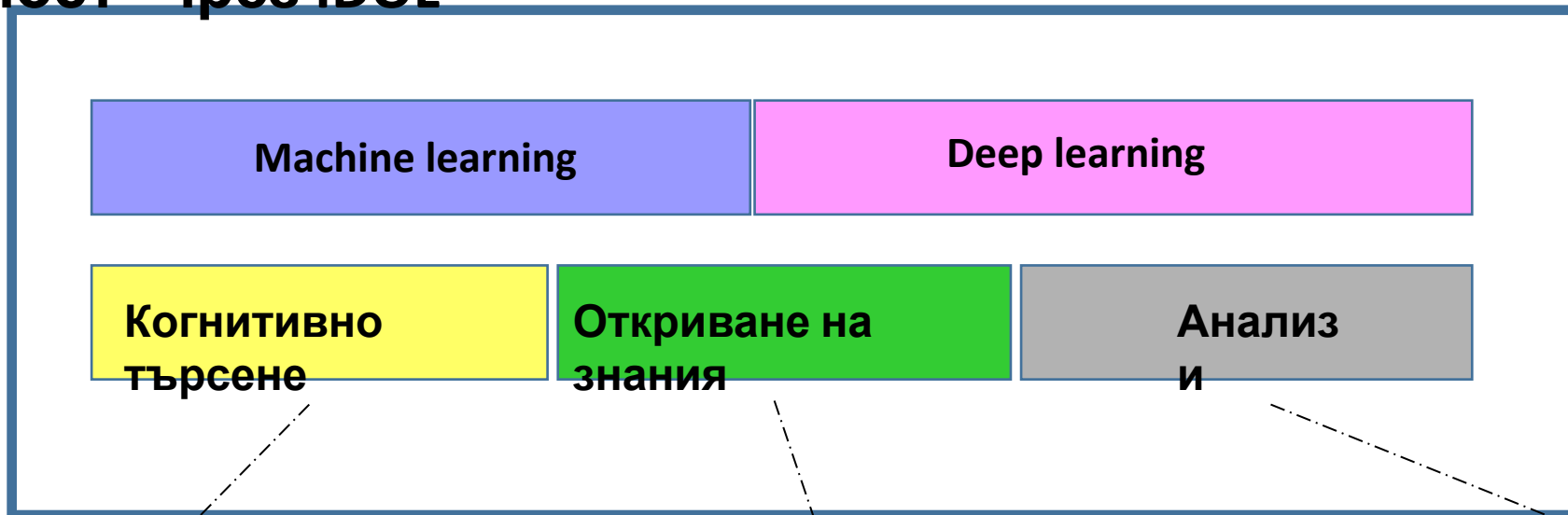
„Софтуерната/AI Надзор бизнес сигурност“ използва Разширена Ламбда архитектурата



Софтуерна архитектура на „Софтуер /AI Hadoop бизнес системността“



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

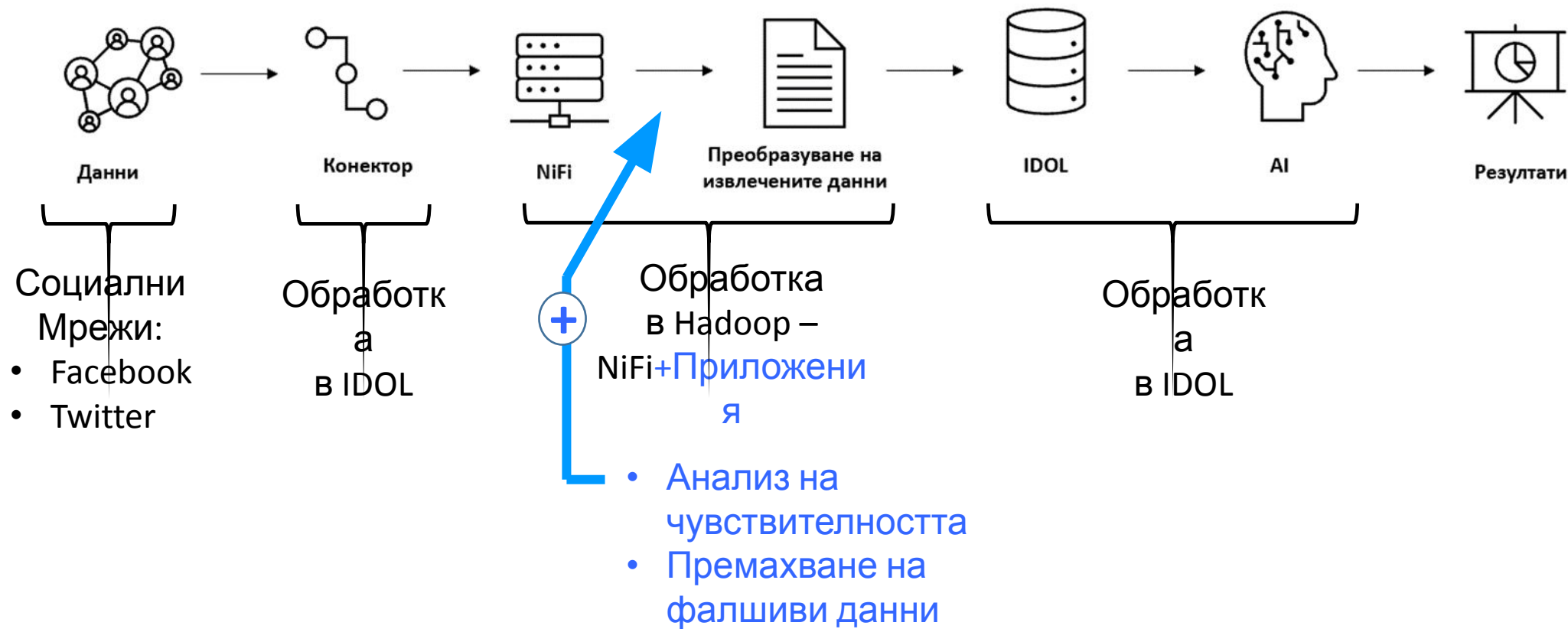


Търсене с използване на AI, търсене с различни видове данни

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

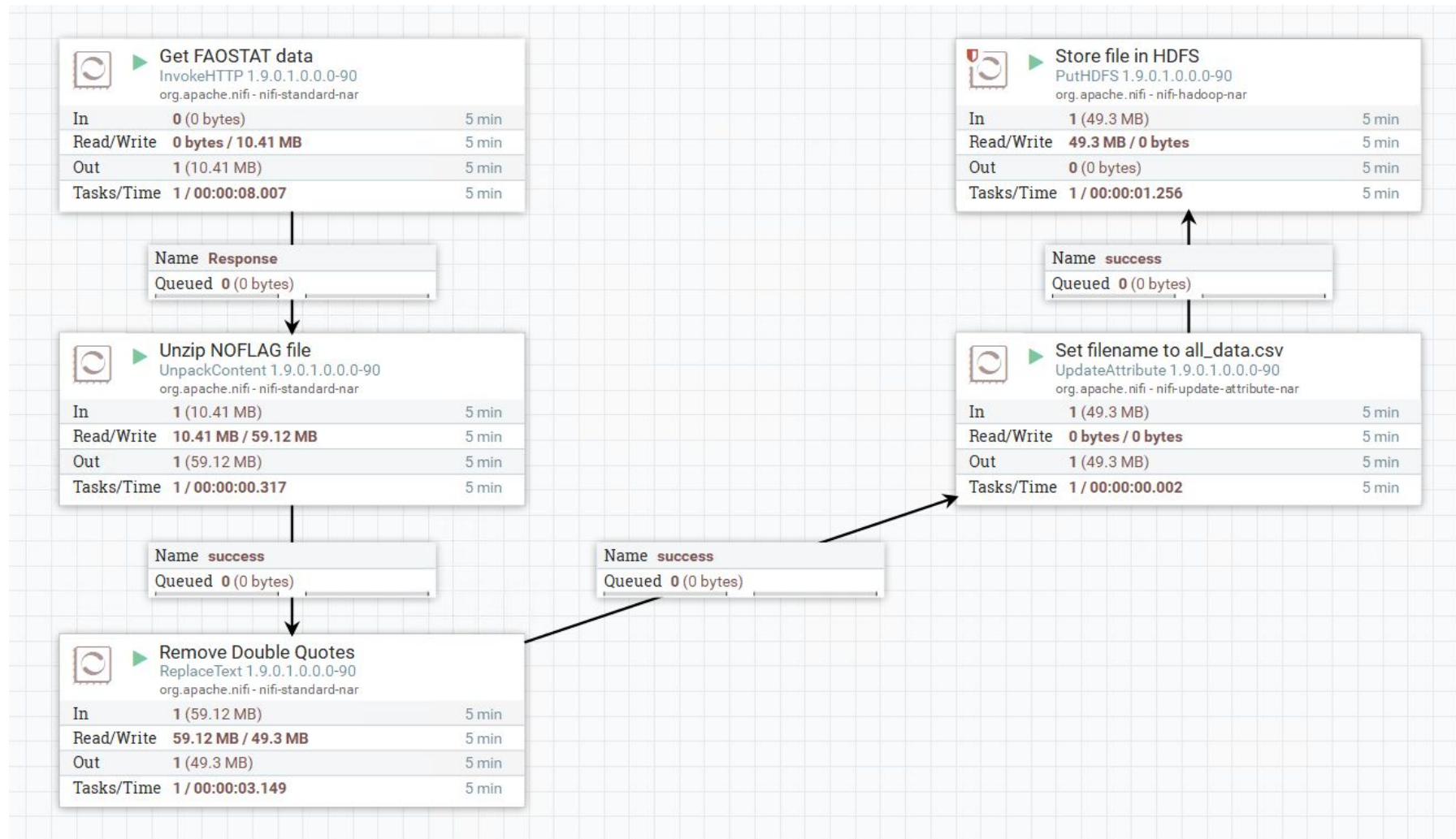
Софтуерна архитектура на „Софтуер /AI Hadoop бизнес сигурност“ се поддържа и чрез IDOL система, интегрирана с Hadoop



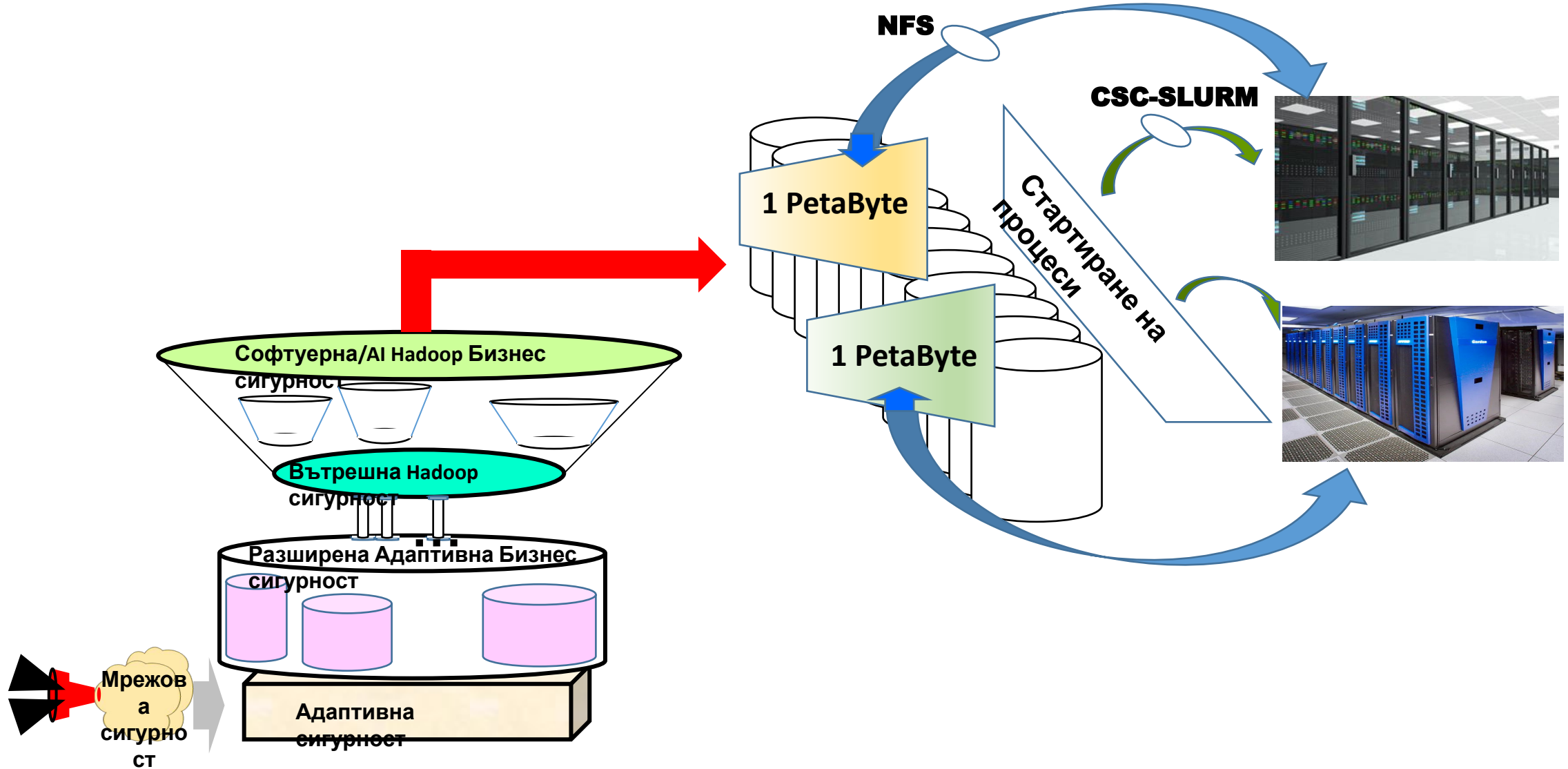
Пример – част от „Софтуер/AI Nadoop бизнес сигурност“ за работа с данни от Twitter - за сигурност на данни – *наличност (availability) на данни* – чрез IDOL

The screenshot displays the Micro Focus IDOL interface. At the top, there is a navigation bar with 'Processor Details' and a search bar containing 'Пример – Конфигуриране връзка с'. Below this, a secondary navigation bar includes 'MICRO FOCUS', 'GUIDED SETUP', 'OAUTH SETUP', 'SCHEDULING', 'LOG MESSAGES', 'STATISTICS', and a search bar with 'Пример – Търсене в Twitter'. On the right side of this bar are buttons for 'PURGE DATASTORE', 'PROPERTY DETAILS', and 'VIEW USAGE'. The main content area shows search results for 'Premium Food'. A dropdown menu is open, showing 'Sort by relevance' and a list of 'RELATED CONCEPTS': 'PREMIUM FOOD', 'bio', 'healthy', and 'premium'. A red arrow points to the 'premium' concept with the text 'Може да добавим ръчно "Kosher"'. The interface also shows a 'Similar documents' section at the bottom.

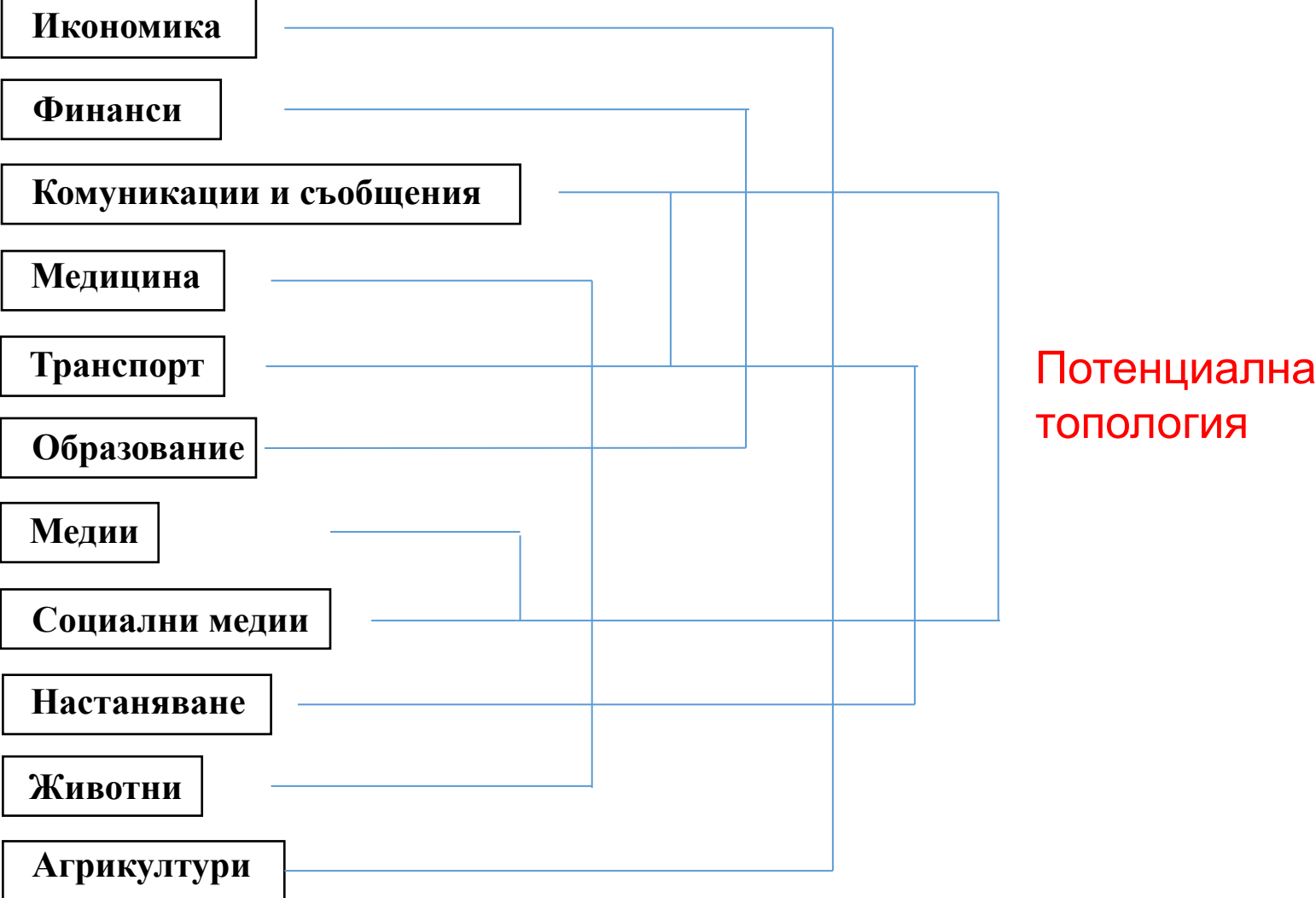
Пример – част от „Софтуер/AI Hadoop бизнес сигурност“ на данни за ечемик – *наличност (availability)* на данни чрез NiFi



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



**БЛАГОДАР
Я!**

***Въпрос
и ?***

