



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Чем мониторинг открытых систем может помочь безопаснику?

Максим Кувшинов
Руководитель обособленного подразделения
Перспективного мониторинга

техно infotecs
2022 Фест

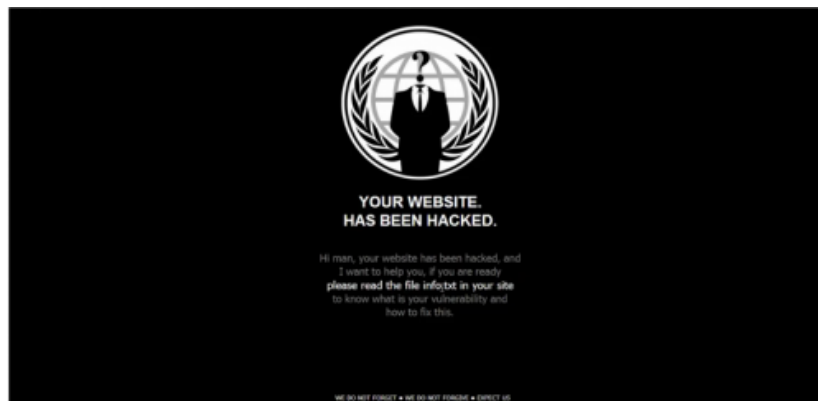
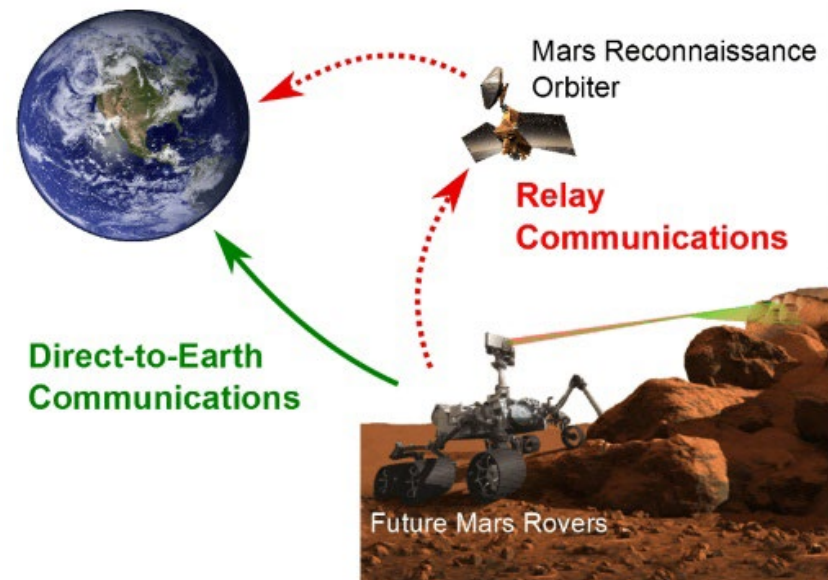
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

О каких системах речь?

- Арендованные VPS/VDS
- Арендованные CMS
- Личный сайт бабушки внука



Что мы хотим от таких систем?



Как защищать такие системы?



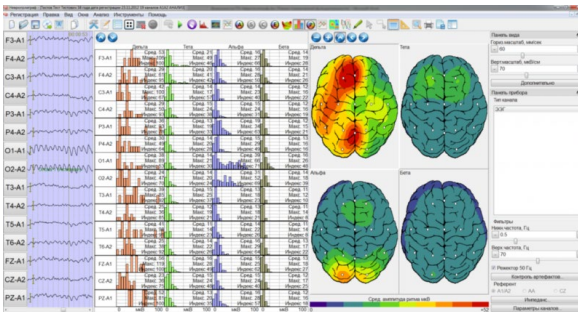
1. Black box

(условия, равные целевому пользователю/внешнему нарушителю)



2. Gray box

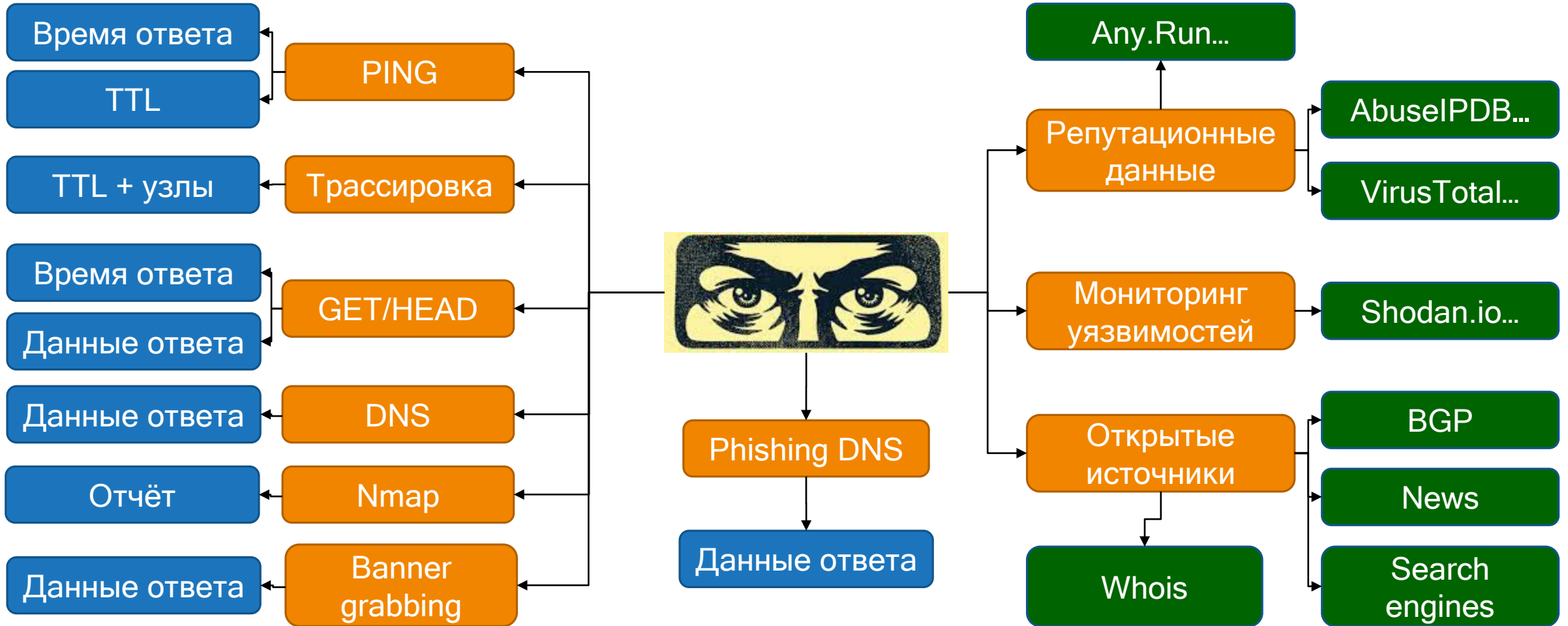
(больше возможностей за счет заранее предусмотренных механизмов)



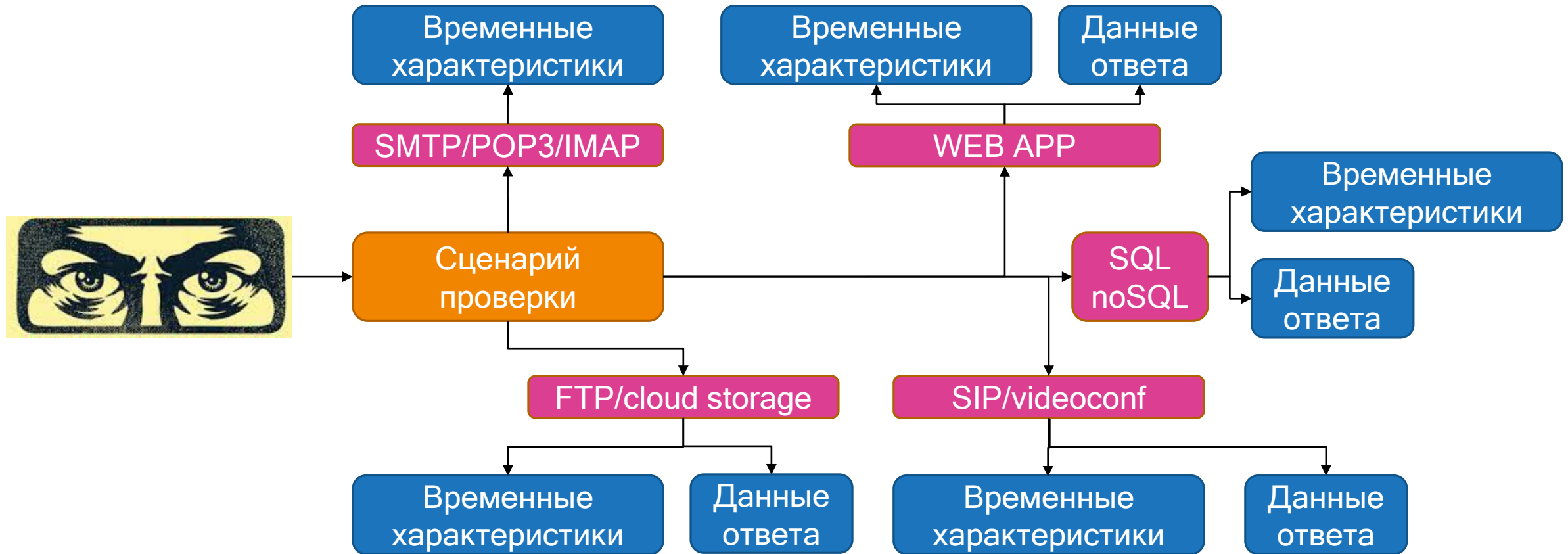
3. White box

(еще больше возможностей при анализе журналов)

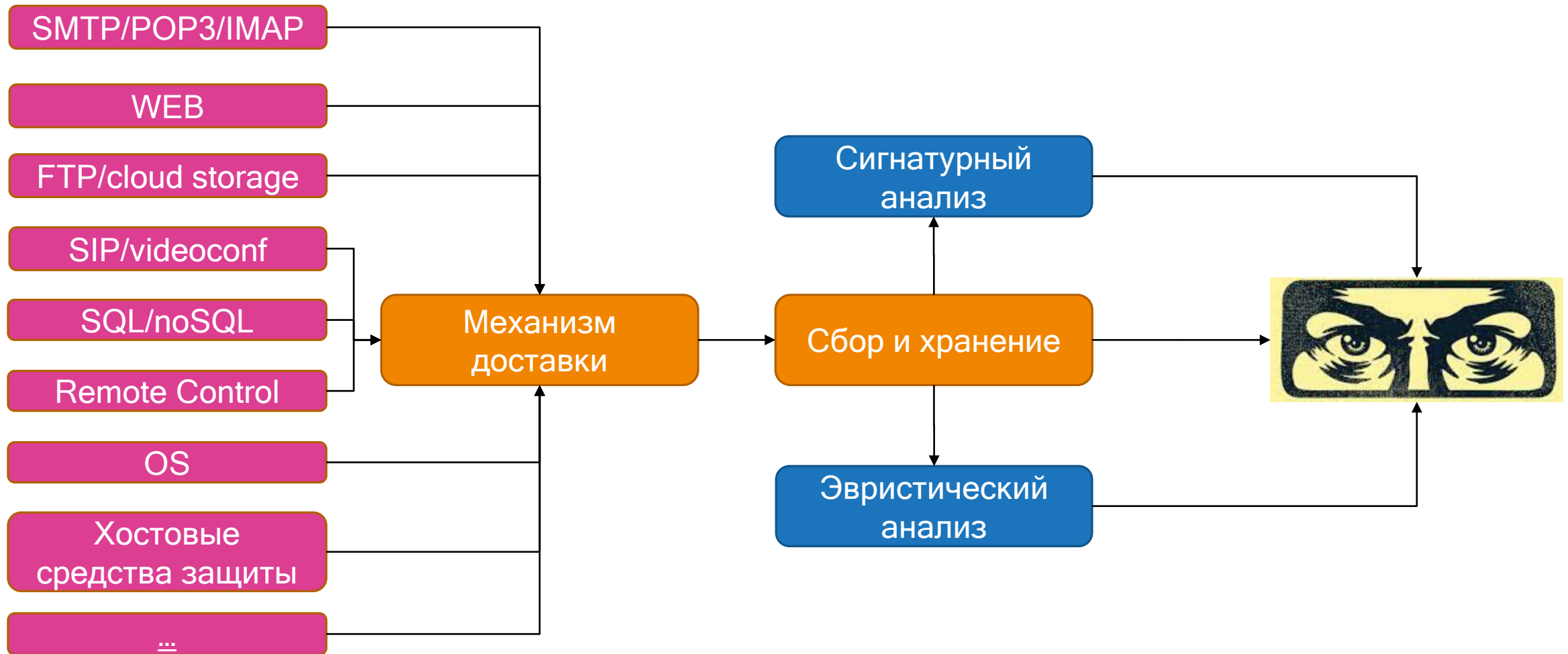
Black box



Gray box



White box (мониторинг логов)



Итоги



Имеется возможность обеспечивать безопасность открытых систем без использования каких-либо средств защиты и изменения конфигурации сервисов

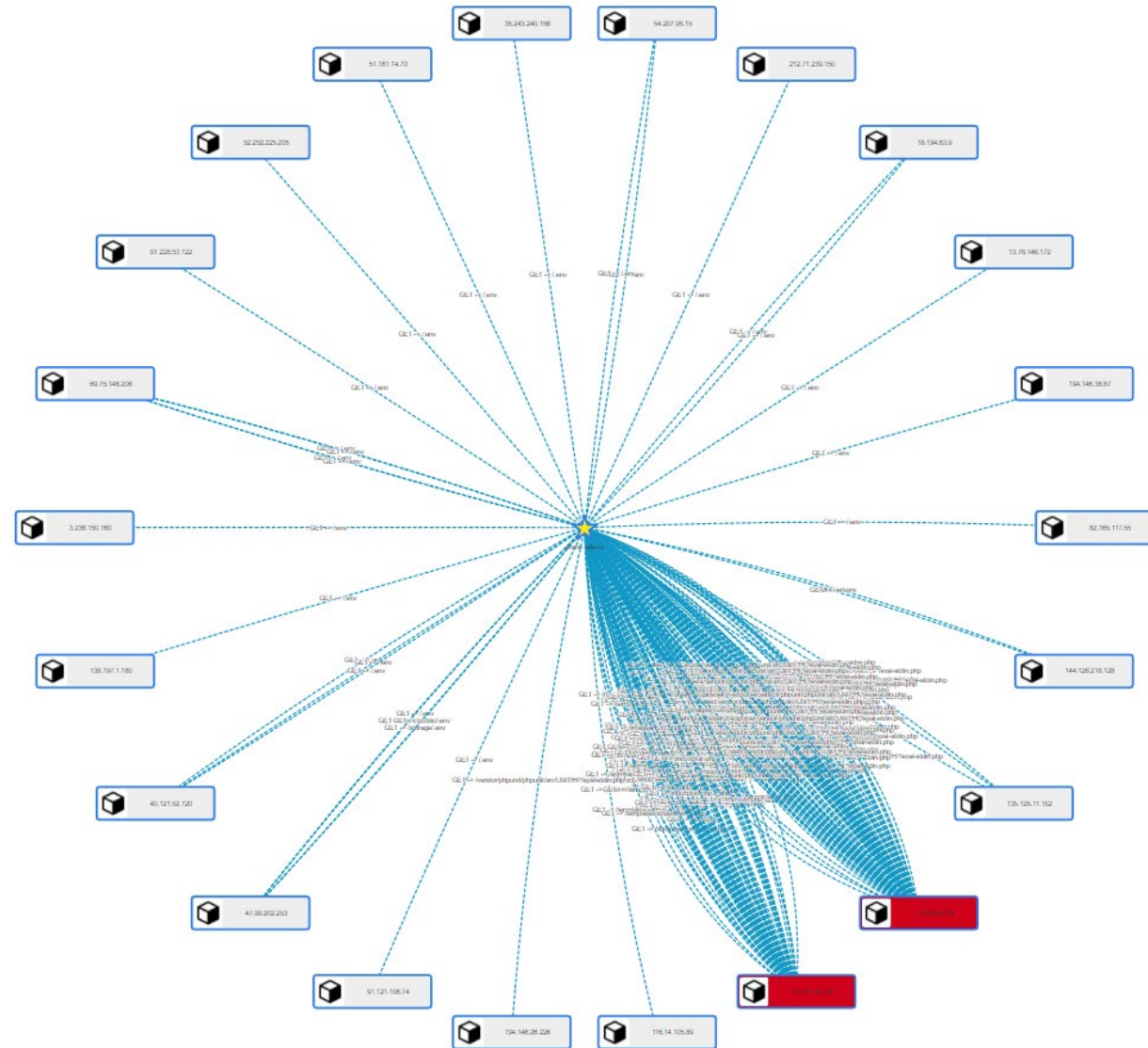
При минимальном изменении конфигурации сервисов возможна расширенная проверка согласно сценариям

При обеспечении непрерывной передачи журналов сервисов имеется возможность обеспечить безопасность открытых сервисов на высоком уровне

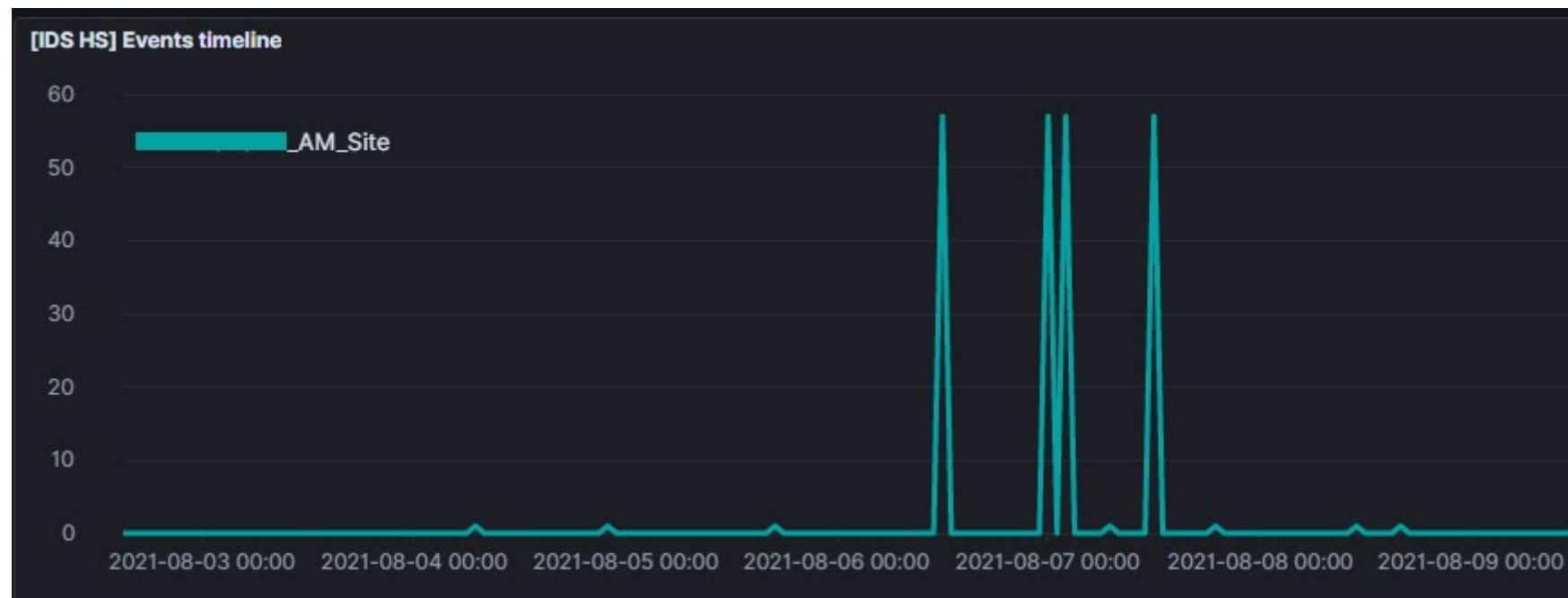
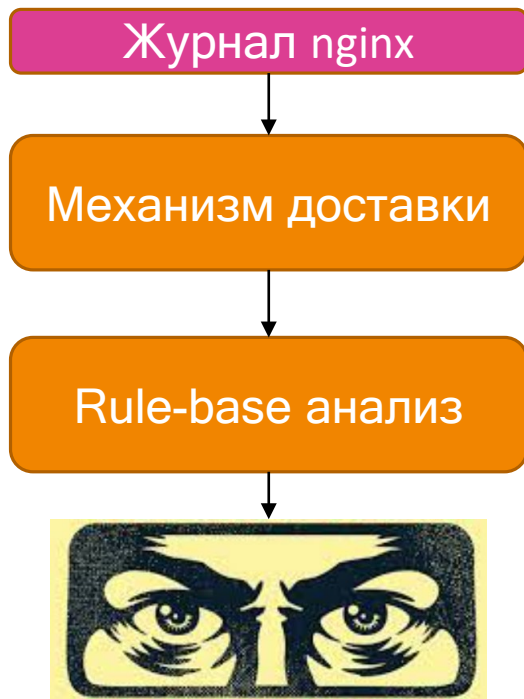
АО «ПМ» уже внедрило в процесс работы SOC данные механизмы мониторинга



Пример №1



Пример №2



```
Aug 7 11:58:08 172.31.0.40 nginx_access_amonitoring_ru: 185.220.102.250 - - [07/Aug/2021:11:58:08 +0300] "GET /wp-content/plugins/db-backup/download.php?file=../../../../wp-config.php HTTP/1.1" 403 118 "http://amonitoring.ru/wp-content/plugins/db-backup/download.php?file=../../../../wp-config.php" "Mozilla/5.0 (Linux; Android 7.0; SM-G892A Bulid/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/60.0.3112.107 Moblie Safari/537.36"
```

AM EXPLOIT Generic Path Traversal in URI

ТЕХНО infotecs 2022 Фест

Спасибо за внимание!
И давайте помониторим!

Максим Кувшинов

Руководитель обособленного подразделения г. Новосибирск
«Перспективный мониторинг»

Maksim.Kuvshinov@amonitoring.ru

Подписывайтесь на наши соцсети



vk.com/infotecs_news



t.me/infotecs_news



rutube.ru/channel/24686363