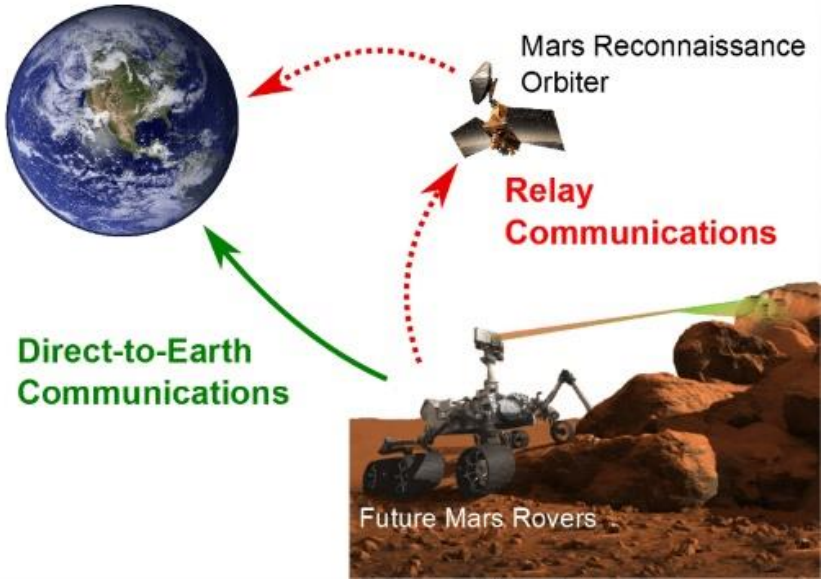
Чем мониторинг открытых систем может помочь безопаснику?

Сергей Нейгер
«Перспективный мониторинг»

О каких системах речь?

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

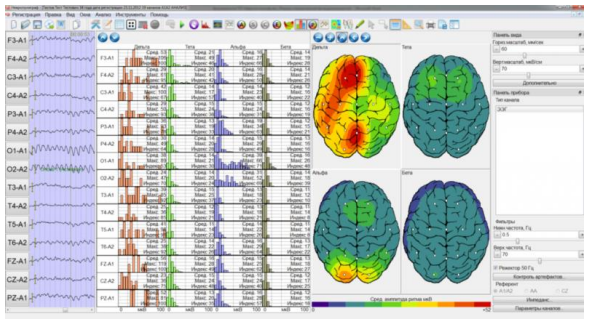
Что мы хотим от таких систем?



Как защищать такие системы?

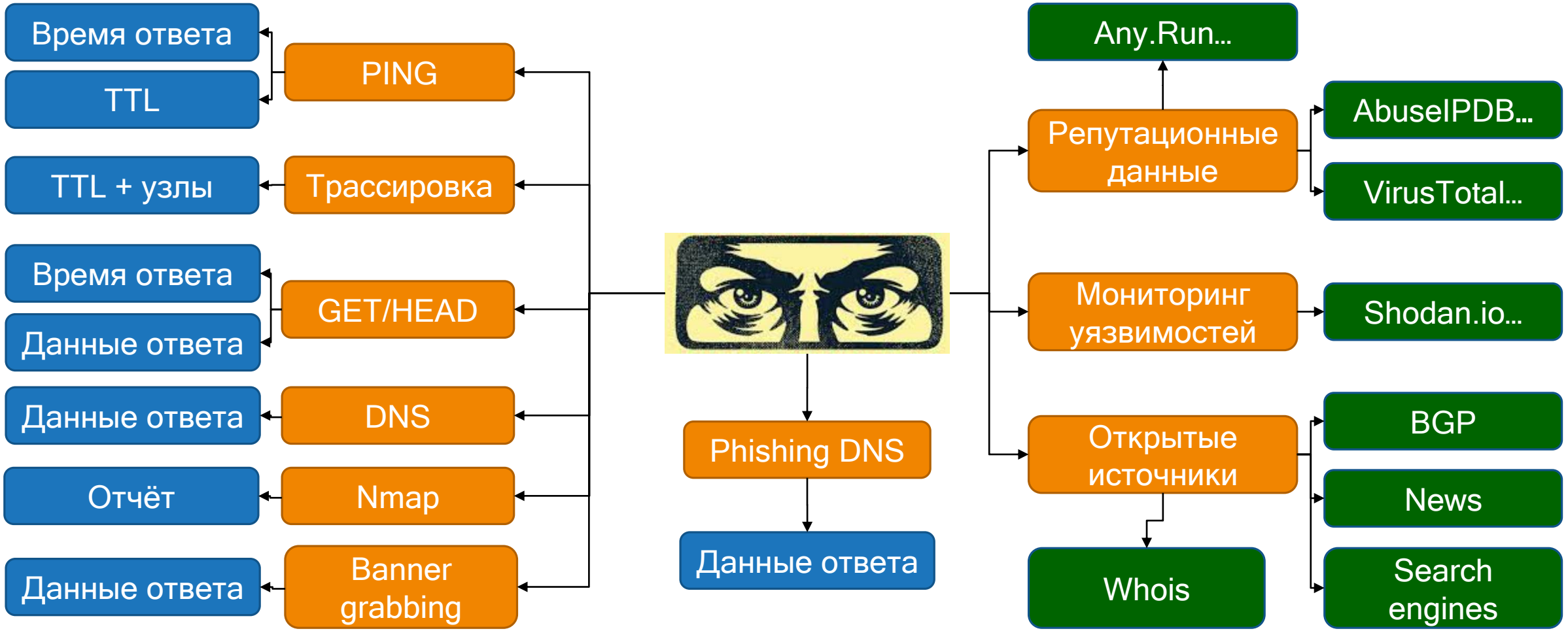
1. Black box
   (условия, равные целевому пользователю/внешнему нарушителю)

2. Gray box
   (больше возможностей за счет заранее предусмотренных механизмов)

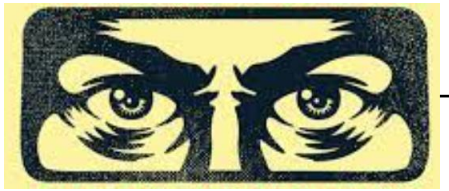


3. White box
   (еще больше возможностей при анализе журналов)

Black box


Время ответа
TTL
PING
TTL + узлы
Трассировка
Время ответа
Данные ответа
GET/HEAD
Данные ответа
DNS
Отчёт
Nmap
Данные ответа
Banner grabbing
Phishing DNS
Данные ответа
Any.Run...
Репутационные данные
AbuseIPDB...
VirusTotal...
Мониторинг уязвимостей
Shodan.io...
Открытые источники
BGP
News
Search engines
Whois

Gray box



Временные характеристики

Временные характеристики

Данные ответа

SMTP/POP3/IMAP

WEB APP

Временные характеристики

Сценарий проверки

SQL noSQL

Данные ответа

FTP/cloud storage

SIP/videoconf

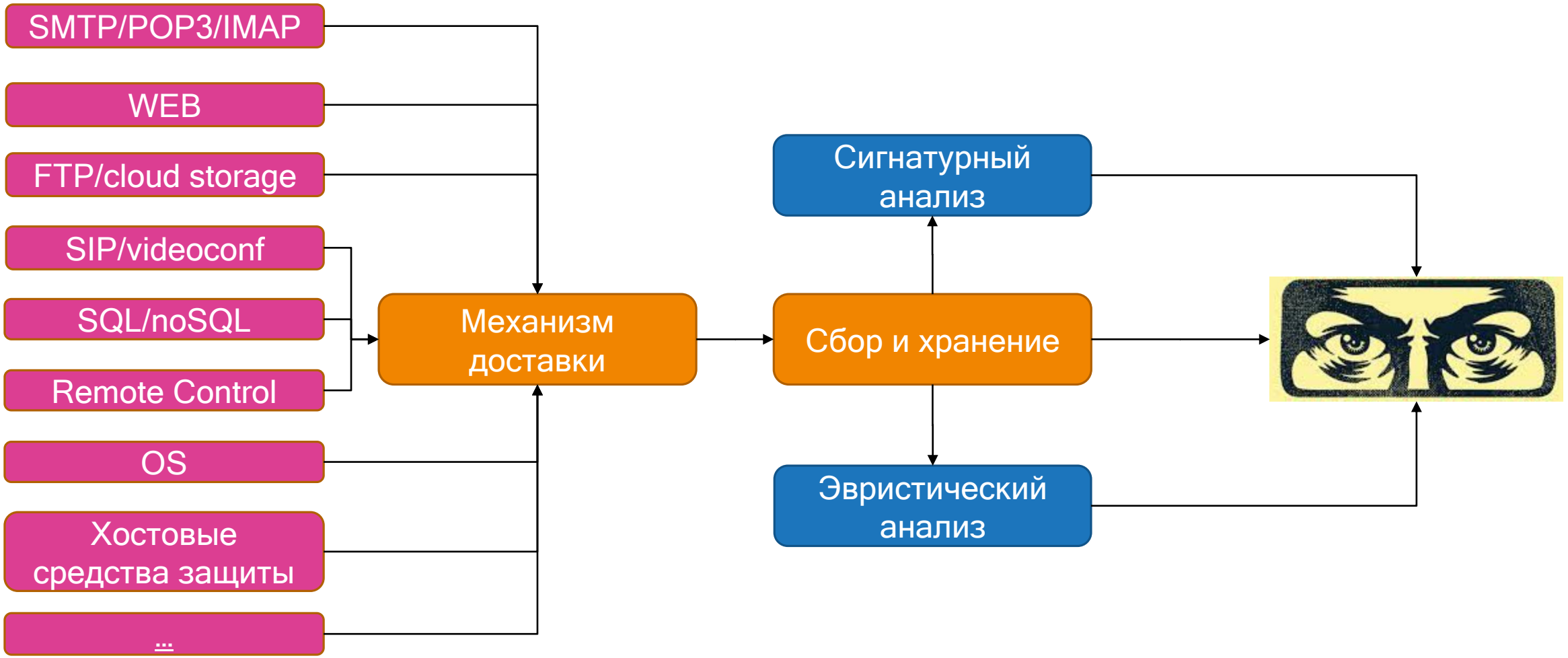
Временные характеристики

Данные ответа

Временные характеристики

Данные ответа

White box (мониторинг логов)



Итоги

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

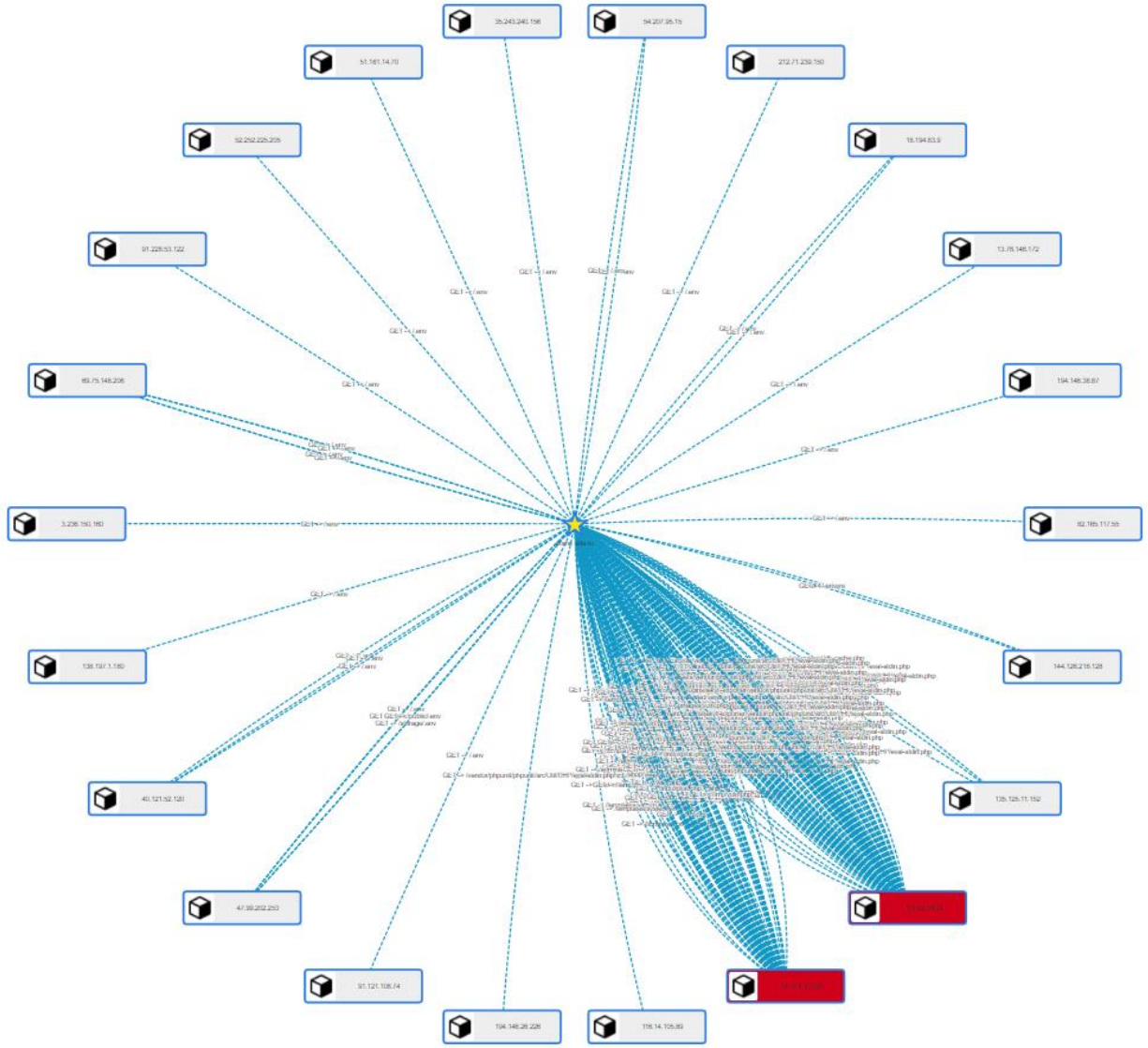
При минимальном изменении конфигурации сервисов возможна расширенная проверка согласно сценариям

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

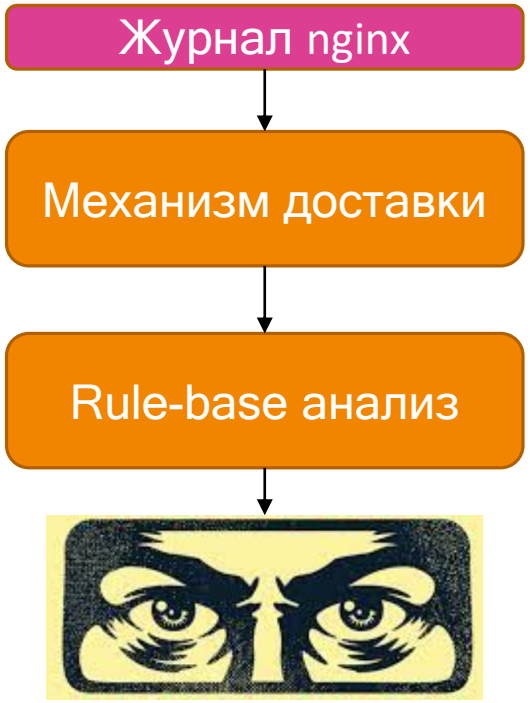
АО «ПМ» уже внедрило в процесс работы SOC данные механизмы мониторинга

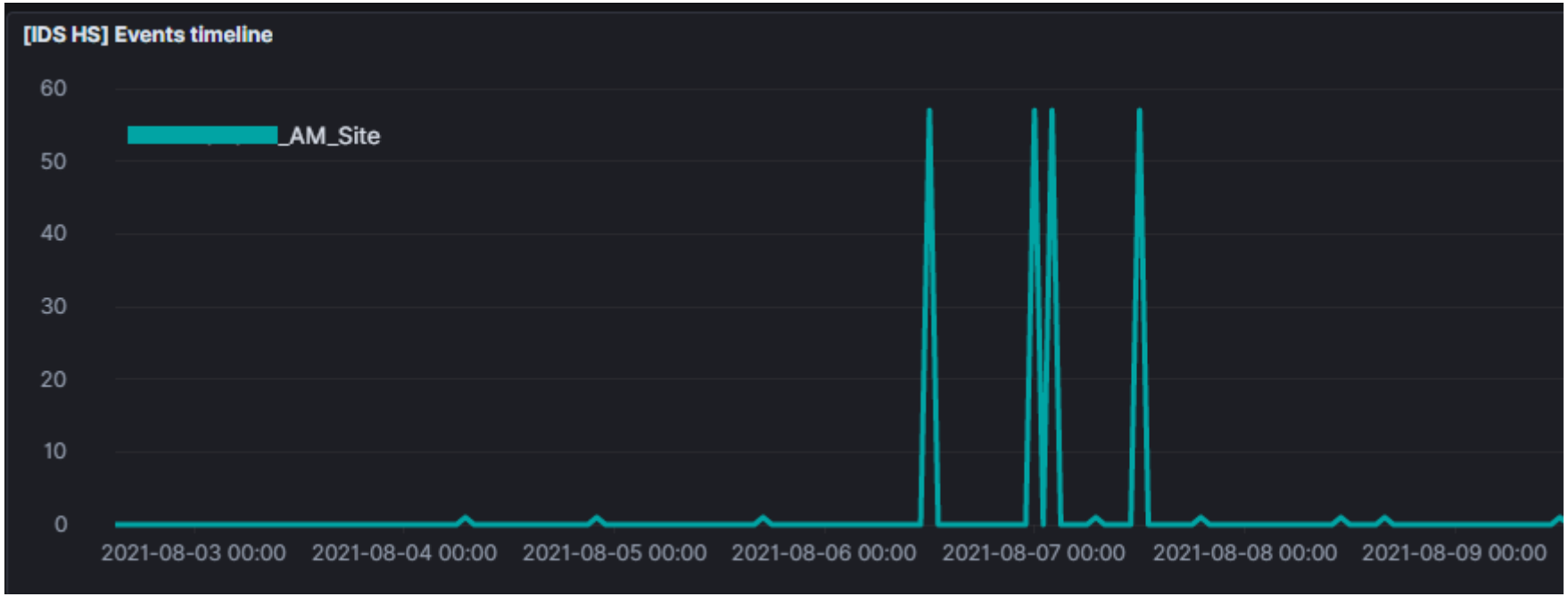
Пример №1


Журнал nginx
Механизм доставки
Статистический анализ
Построение красивого графа (колесо обозрения)



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" "Mozlila/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
```

Спасибо за внимание!

Сергей Нейгер

Директор по развитию бизнеса компании «Перспективный мониторинг»

Sergey.Neyger@amonitoring.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363