Разведка угроз

Денис Симонов // 2024 г.

Обо мне

Денис Симонов

10 лет в ИБ

Менеджер проектов в #T.Hunter

Пишу код на Python

Автор в журнале xakep.ru

Давал интервью **TechCrunch.com**

Веду блог **https://n0a.pw**

DRP и Threat Intelligence

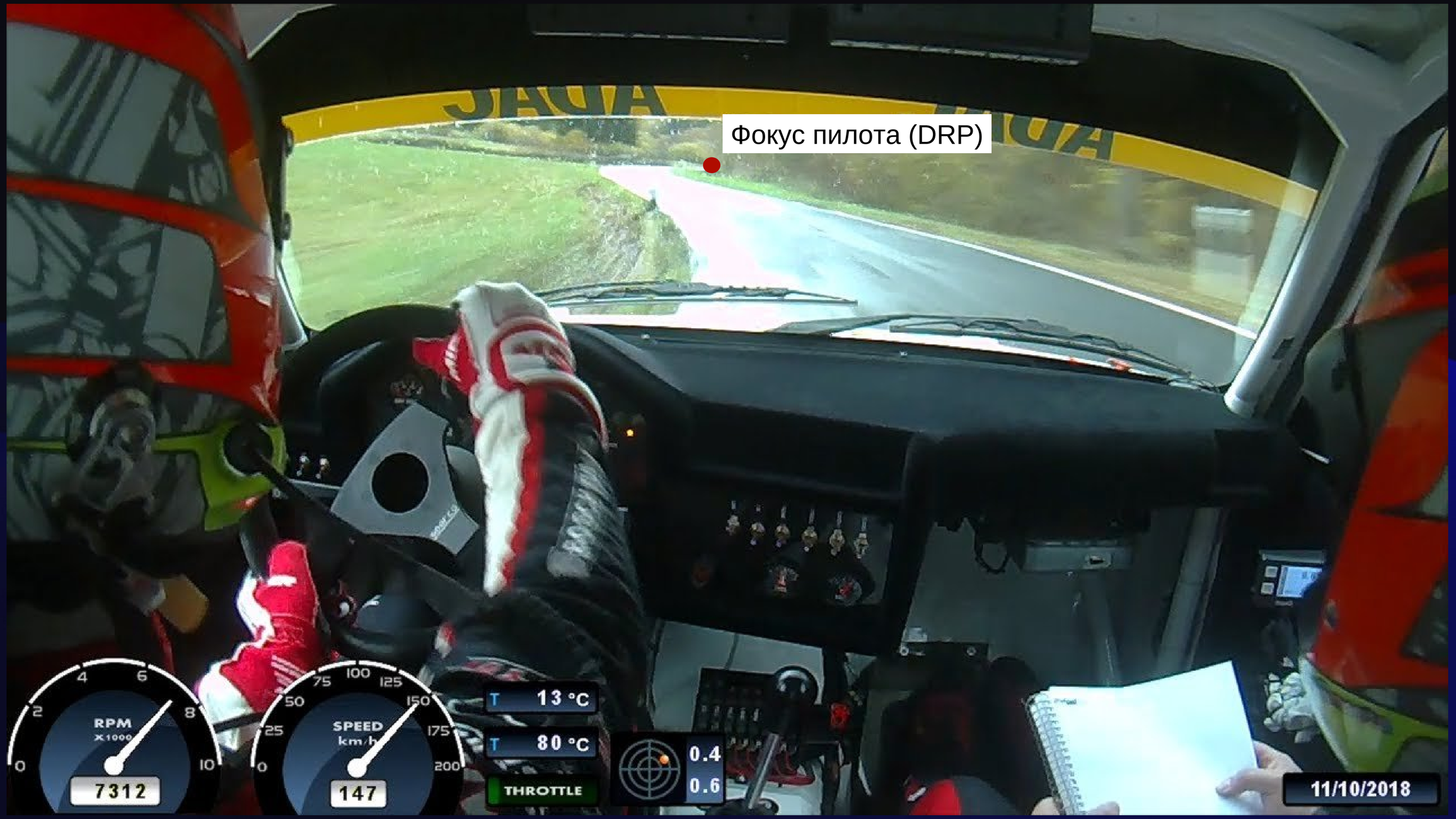
В чем отличие?

Threat Intelligence фокусируется на анализе и понимании киберугроз, в то время как ***Digital Risk Protection*** активно защищает цифровые активы и онлайн-присутствие организации от этих угроз.


TI
DRP

Threat Intel Feed

Это потоки данных, обычно предоставляемые в режиме реального времени, которые включают информацию об известных угрозах, таких как вредоносные IP-адреса, домены, URL-адреса и хэши файлов. Эти данные помогают компаниям своевременно обновлять свои защитные меры. Примеры: CrowdStrike Falcon X, Cisco Talos, FireEye iSIGHT.


Фокус пилота (DRP)
RPM
x1000
7312
SPEED
km/h
147
T 13 °C
T 80 °C
THROTTLE
0.4
0.6
11/10/2018


Модули DRP
SUBARU
YOKOHAMA
YOKOHAMA
VermontSportsCar

Утечки данных

Защита конфиденциальной информации

- **Мониторинг утечек данных**
  Автоматическое отслеживание и обнаружение утечек конфиденциальных данных в открытом доступе, на форумах, в даркнете.
- **Анализ компрометации**
  Оценка и классификация утечек по уровню риска и потенциальному воздействию на организацию.
- **Уведомления о нарушениях**
  Мгновенное информирование о потенциальных утечках для быстрого реагирования и смягчения последствий.

Поддельные корпоративные домены

Защита от фишинга и мошенничества

- **Отслеживание поддельных доменов**
  Идентификация и мониторинг доменов, имитирующих бренд компании.
- **Анализ фишинговых угроз**
  Оценка содержания подозрительных сайтов и их потенциальной угрозы для пользователей и организации.
- **Сотрудничество с регистраторами**
  Взаимодействие с регистраторами доменов для блокирования или удаления мошеннических сайтов.
- **Обучение сотрудников**
  Разработка программ повышения осведомленности сотрудников о фишинге и методах мошенничества.

Безопасность контрагентов

Минимизация рисков при работе с третьими сторонами

- **Оценка контрагентов**
  Анализ кибербезопасности и рисков, связанных с текущими и потенциальными партнерами.
- **Мониторинг третьих сторон**
  Непрерывный аудит безопасности используемых сервисов и поставщиков.
- **Контрактное регулирование**
  Включение требований к кибербезопасности в договоры с партнерами.
- **Управление инцидентами**
  Разработка процедур быстрого реагирования на инциденты безопасности, затрагивающие третьи стороны.

	8 янв. 2023 г., 23:34	--	Папка
ал 2022_v1.docx	31 дек. 2022 г., 18:19	24 КБ	Документ Word
ение к акту (по т...са)_декабрь_2022 v2.xlsx	31 дек. 2022 г., 18:18	11 КБ	Micros...k (.xlsx)

gazprom_L_1.png

Открыть в приложении «Просмотр»

[redacted] bank.ru>

Ответить всем

Чт 17.11.2022 12:38

Кому:

Копия: [redacted] bank.ru>

> Это сообщение отправлено с высокой важностью.

Напомню, что в файлах – ПРЕДЕЛЬНО КРИТИЧНАЯ ИНФОРМАЦИЯ , подпадающая под все мыслимые Законы, Внутренние Положения Банка, Указания ЦБ и NDA и составляющая в т.ч. Коммерческую и Банковскую Тайны.

Отнеситесь к сведениям ПРЕДЕЛЬНО-ПРЕДЕЛЬНО ВНИМАТЕЛЬНО с обеспечением всех норм безопасности.

Я ОБЯЗАН вас еще раз предупредить.
Цена слишком высокая, чтобы относиться легкомысленно.

Проверьте еще раз, что утечки (выноса за контуры Банка или ОГРАНИЧЕННОГО круга лиц) с вашей стороны ИСКЛЮЧЕНЫ.

Обязательно убедитесь, что по завершении работ данные будут НАДЕЖНО УДАЛЕНЫ с ресурсов, не являющихся авторизованными ресурсами контура Банка.

Спасибо!

From: [redacted]
Sent: Thursday, November 17, 2022 12:29 PM
To: [redacted]
Cc: [redacted]
Subject: RE: [External Email] Re: IRPLN-270 Канал Pub/Sub (topic) для ИО Customer на базе Kafka-кластера в СУВ

Добрый день!

Архив выложен на сетевой ресурс в полном объеме. Информацию по пути размещения и пароль к архиву сообщу отдельно.
Разницы между файлами нет (насколько я знаю из беседы с админом ЕСК), разделение на тома архива выполнено случайным образом.

Мониторинг инфополя в Telegram

Идентификация и превентивная защита от киберугроз через социальные медиа

- **Отслеживание активности в группах и каналах**
  Мониторинг публичных и закрытых групп Telegram на предмет обсуждения и планирования кибератак, слива данных и других угроз.

- **Анализ контента и контекста**
  Применение технологий машинного обучения и NLP для анализа текстов и выявления потенциальных угроз или нежелательной активности.

- **Расследование инцидента до его совершения**
  Использование методов цифровой атрибуции для идентификации пользователей Telegram, потенциально участвующих в подготовке к атакам или в утечках информации.

[redacted]
1 584 подписчика

CloudFire.z73
3.8GB - Загрузить

CloudFire.z74
3.8GB - Загрузить

CloudFire.z75
3.8GB - Загрузить

409 22:12

CloudFire.z76
3.8GB - Загрузить

CloudFire.z77
3.8GB - Загрузить

CloudFire.z78
3.8GB - Загрузить

CloudFire.z79
3.8GB - Загрузить

CloudFire.z80
3.8GB - Загрузить

CloudFire.z81
3.8GB - Загрузить

CloudFire.z82
3.8GB - Загрузить

CloudFire.z83
3.8GB - Загрузить

CloudFire.z84
3.8GB - Загрузить

[redacted]
9 851 подписчик

Закреплённое сообщение
If you need easy and quickly search by phone, email, account, passwo

Email
Phone
First Name
Middle Name
Last Name
Date of birth
Address
Passport

[redacted]

1,6K 01:21

Переслано от: DataBaseCollection

kora_@DBC_links.zip
200.3MB - Показать в Finder

kora.ru (08.03.2024) (sql)
(More info)

Email
Phone
First Name
Middle Name
Last Name
Address
Password
Date of birth

[redacted]

1,8K 01:21

Переслано от: DataBaseCollection

iw-shop.ru_@DBC_links.zip
1.7MB - Загрузить

iw-shop.ru

12к +18к (user + order)

[redacted]

1,9K 01:21

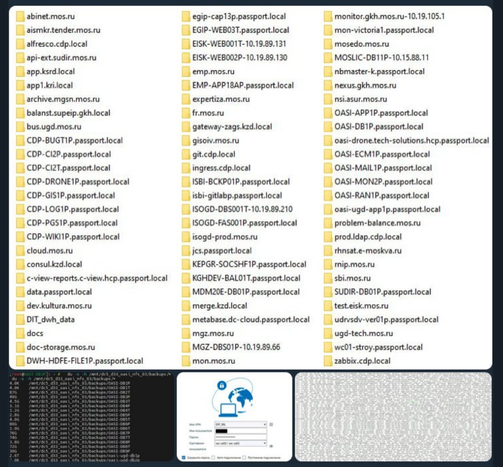
Переслано от: DataBaseCollection

almet.ru_@DBC_links.zip

Cyber Legions 🇺🇦
4 313 подписчиков

Закреплённое сообщение
Надо брать яйца в кулак и сказать "Это мы ёбнули volgofarm.ru и остановили р

Переслано от: DumpForums



Прошел уже год как мы взломали **Департамент информационных технологий города Москвы** (ДИТ).

Большую часть времени мы выгружали информацию, продвигались в инфраструктуре и получали доступ к тому, что нам было нужно. И вот - результат. Результат долгой и сложной работы. Неисчисляемое количество попыток выгнать нас из сети, увы, были тщетны.

За время пребывания нам удалось взломать все технические ресурсы ДИТ, выгрузить **40ТБ** баз данных различных ресурсов Москвы включая: ЕМИАС, ИС УДРВС, Портал мэра Москвы, СУДИР и другие. Вся полученная информация обрабатывалась, затем извлекалось всё необходимое и уже используется нами в работе над другими целями.

У нас имеются данные на всех госслужащих Москвы за всё время. Персональные данные всех москвичей - паспорта, номера телефонов, почты и многое другое. Мы так-же не оставили без внимания разработки департамента. Внутренний *gitlab*, *nexus*, *jenkins*, архивы работ с ПК сотрудников так-же находятся у нас. Немного позже сольем

Мониторинг хостов и веб-ресурсов

Интеграция Attack Surface Management для усиленной защиты

- **Комплексное сканирование активов**
  Автоматическое обнаружение и сканирование всех цифровых активов, включая неизвестные и забытые ресурсы.

- **Идентификация уязвимостей**
  Использование ASM для выявления уязвимостей на всей атакуемой поверхности.

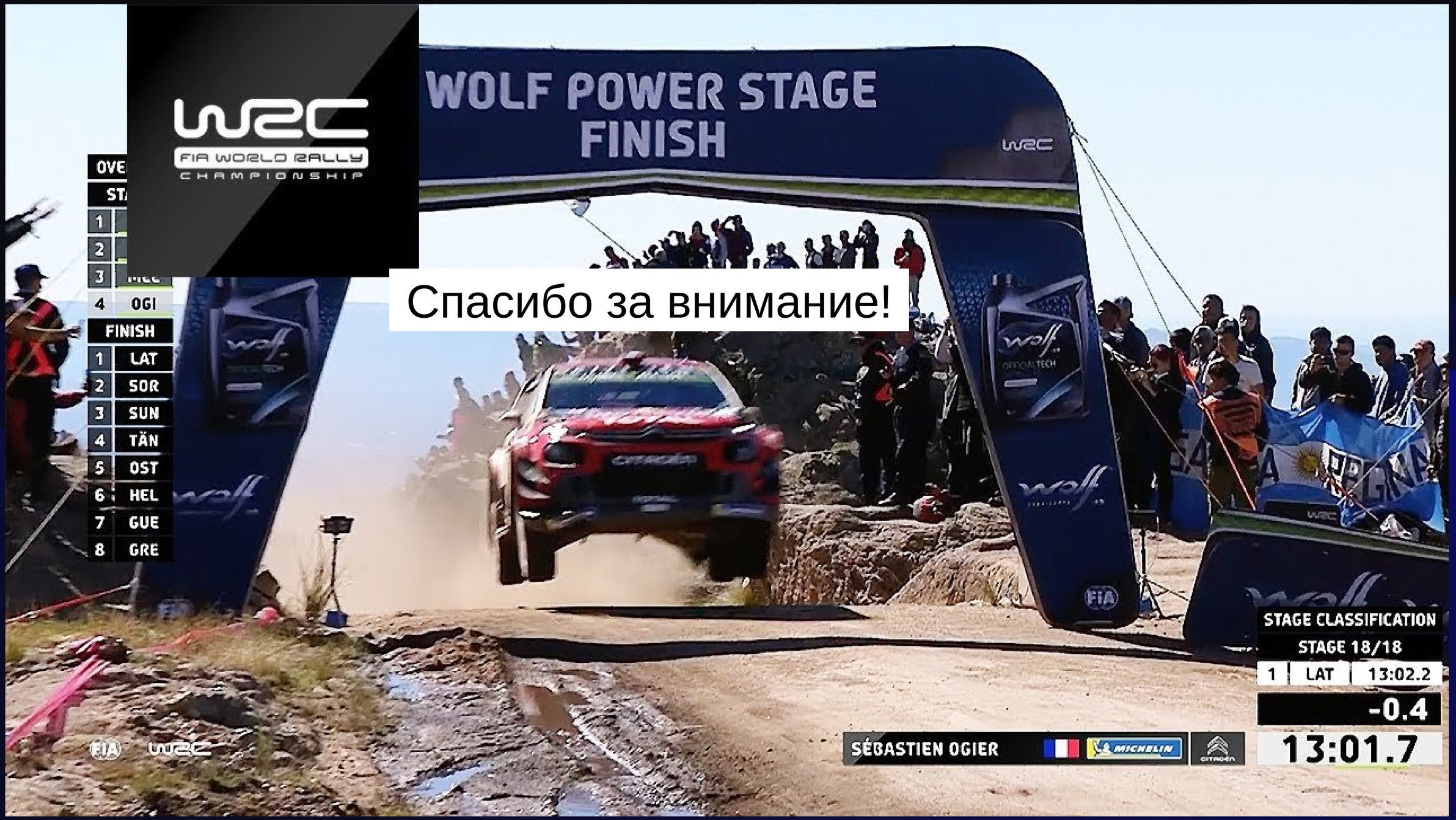
- **Интеграция с Censys, Shodan, etc**
  Использование данных из Censys и Shodan для обнаружения хостов у подрядчика по слепкам сертификатов или hostname, минуя защиту WAF (Web Application Firewall).

- **Моментальное уведомление об изменении ландшафта**
  Автоматическая система уведомлений, которая оповещает об изменениях в сетевом ландшафте, таких как активация нового хоста в сети или открытие нового порта.

Что еще может DRP?

Нет предела совершенству

- Отслеживание утечек кода (Github, pastebin, etc)
- Защита бренда
- Защита интеллектуальной собственности
- Защита VIP-персон
- Кадровый риск
- Комплаенс-риски


WOLF POWER STAGE
FINISH
FIA WORLD RALLY
CHAMPIONSHIP
OVE
ST
1
2
3
4 OGI
FINISH
1 LAT
2 SOR
3 SUN
4 TÄN
5 OST
6 HEL
7 GUE
8 GRE
Спасибо за внимание!
STAGE CLASSIFICATION
STAGE 18/18
1 LAT 13:02.2
-0.4
13:01.7
SÉBASTIEN OGIER