Użycie narzędzi znanych z pracy w celach innych niż praca

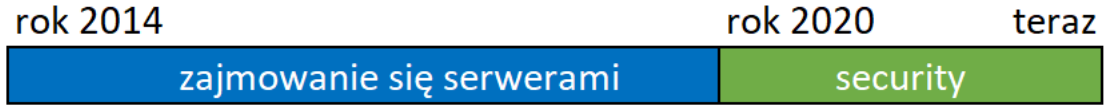
Patryk Stachowiak

Kim jestem

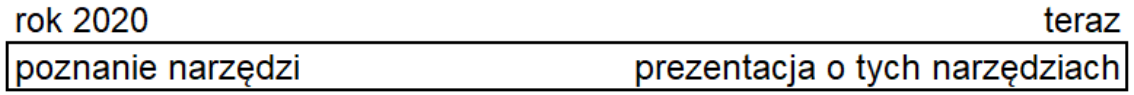
Jak tu wylądowałem

Życie

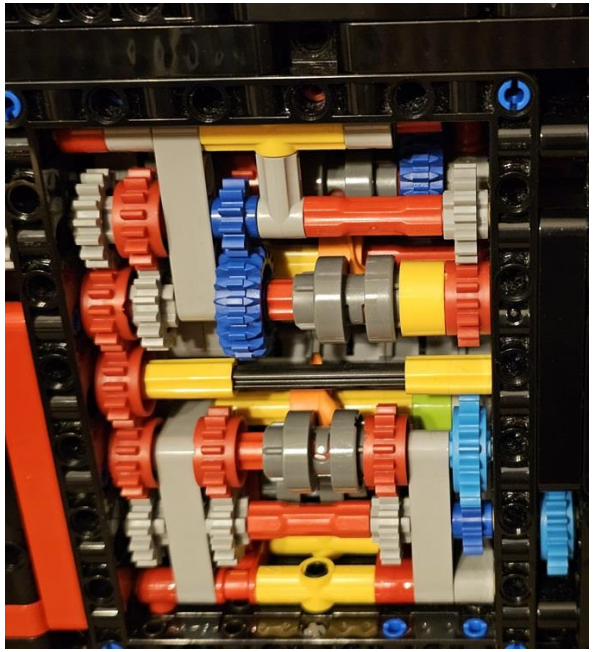
Praca w GSK



Praca w Security Incident Response Team



Moje zainteresowania



Co robi mój zespół

- Wyszukiwanie zagrożeń w danych zebranych z różnych środowisk
- Reagowanie na alerty z oprogramowania antywirusowego
- Analiza maili będących potencjalnym phishingiem
- Zajmowanie się zgłoszeniami użytkowników
- …

Jakich narzędzi używa mój zespół

- SIEM (Security Information and Event Management)
- EDR (Endpoint Detection and Response)
- Reported email analysis (Threat Response Auto Pull)
- Request Management
- …

Skąd pomysł na prezentację

Konferencja Splunk conf23

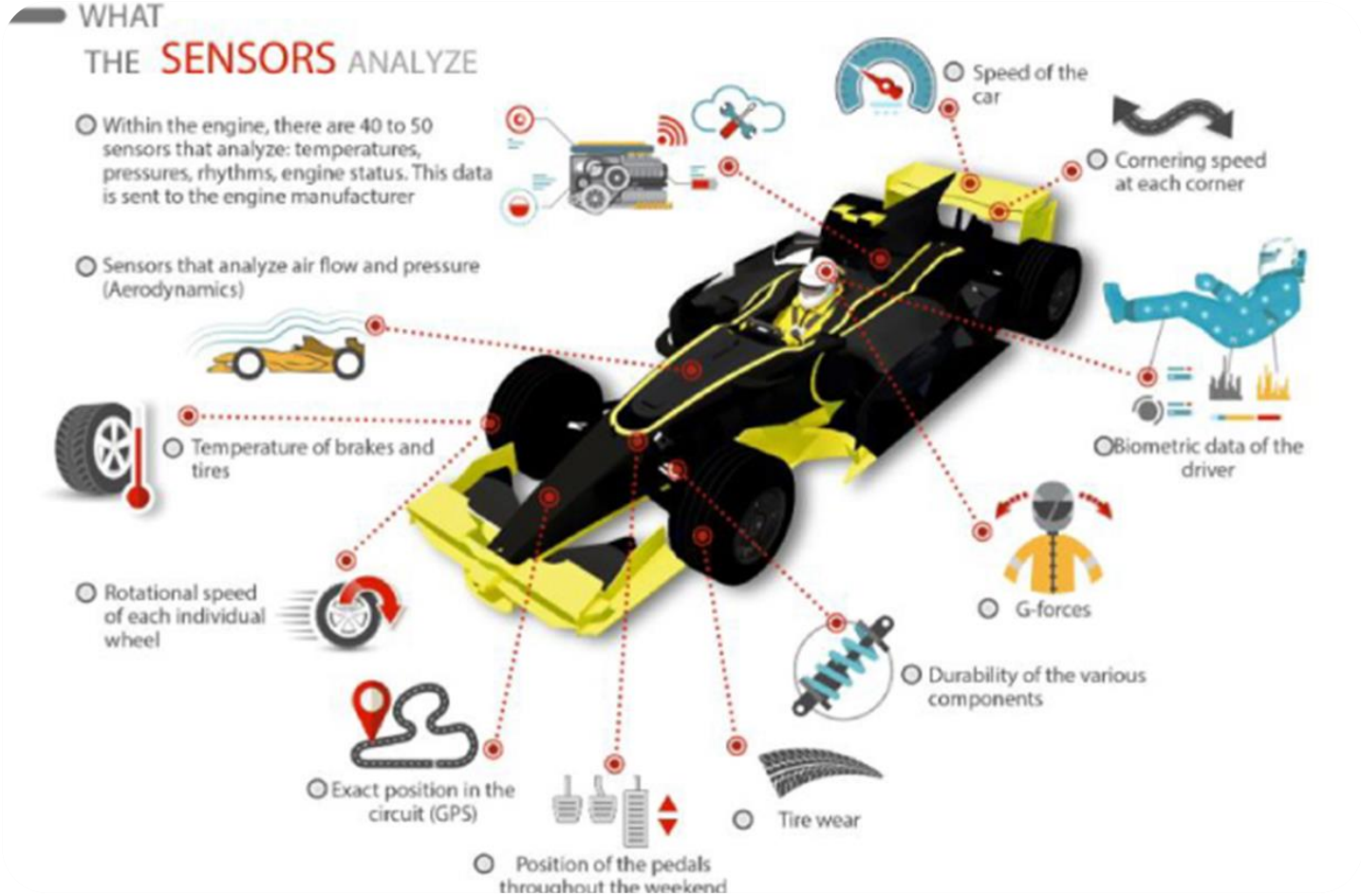
McLaren i Splunk

Zbieranie danych / Telemetria w motorsporcie

- Dane zewnętrzne
  - Czasy okrążeń
  - Czasy sektorów/minisektorów
  - Prędkości w punktach pomiarowych
- Dane wewnętrzne
  - Prędkości na przestrzeni okrążenia
  - Poziom wciśnięcia gazu i hamulca
  - Kąt skrętu kierownicy
  - Obroty i moc silnika, wytwarzany moment obrotowy
  - Ciśnienia w kołach

Telemetria

Przykład w motorsporcie

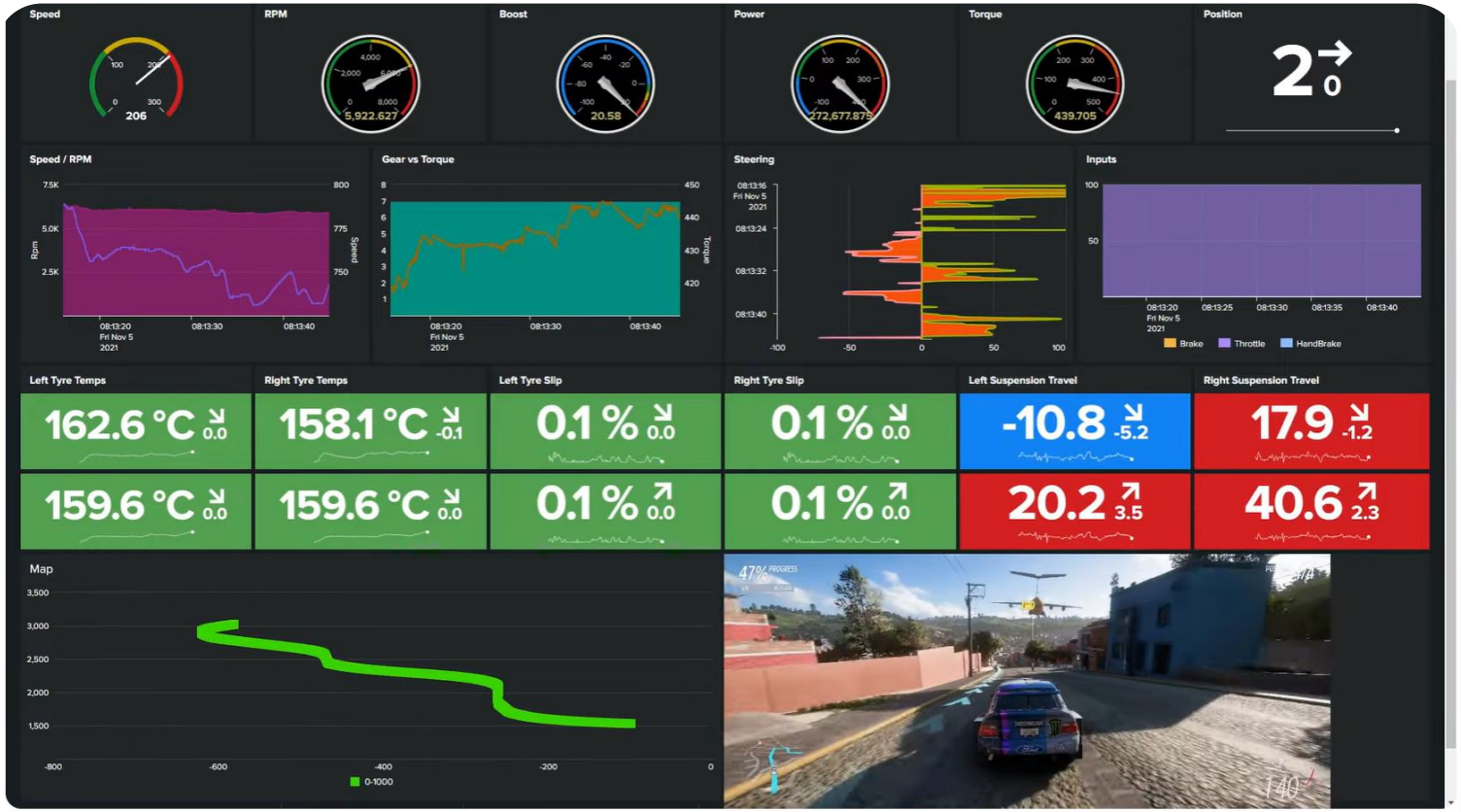


Telemetria

Przykład w grze

Skąd pomysł na prezentację

Film na youtube



Forza Horizon 5 in Splunk

Brett Adams

53 subskrybentów

Subskrybuj

21

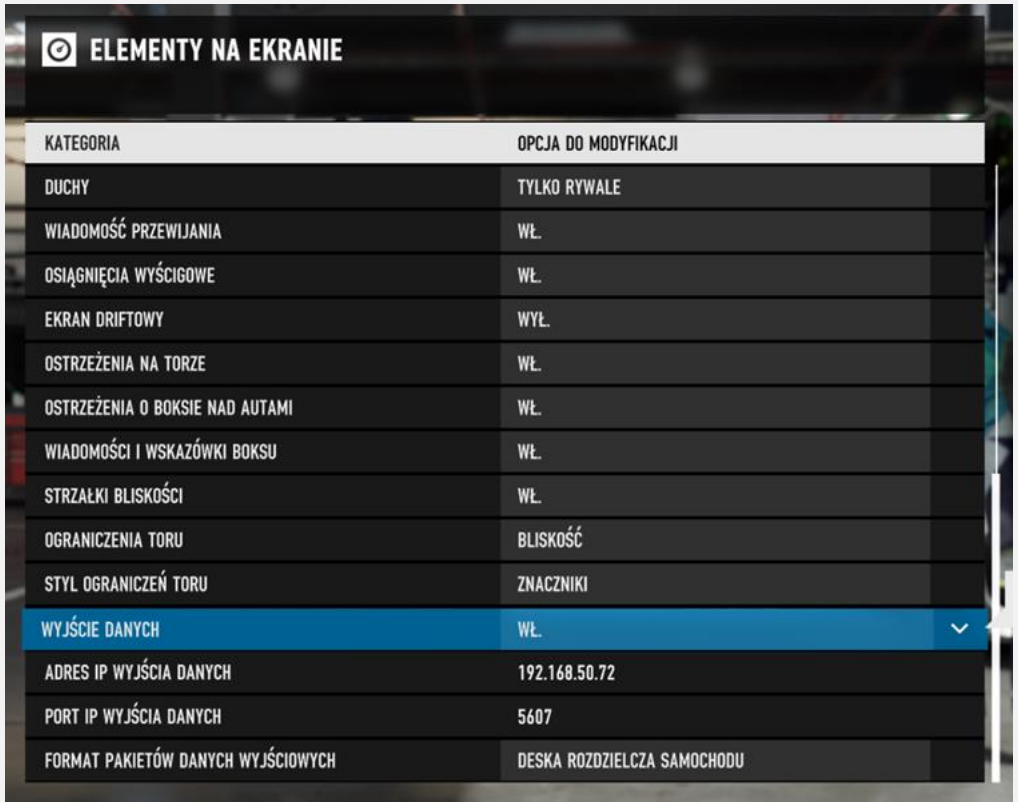
Udostępnij

Zapisz

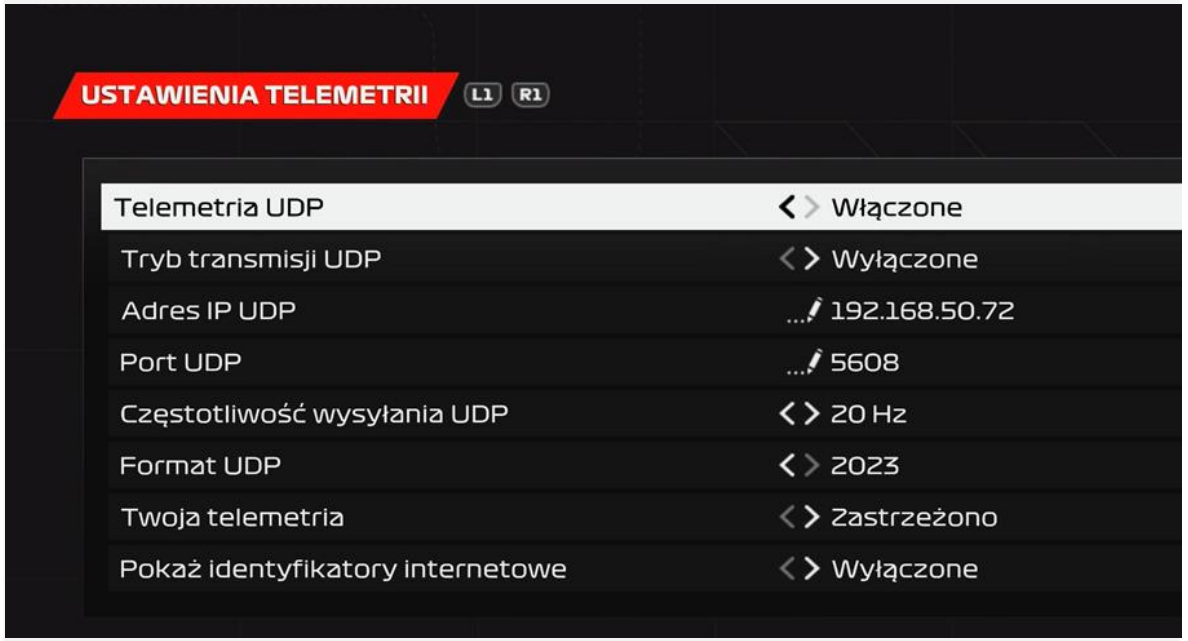
Przykłady gier

Ustawienie wysyłania telemetrii

Forza Motorsport 7

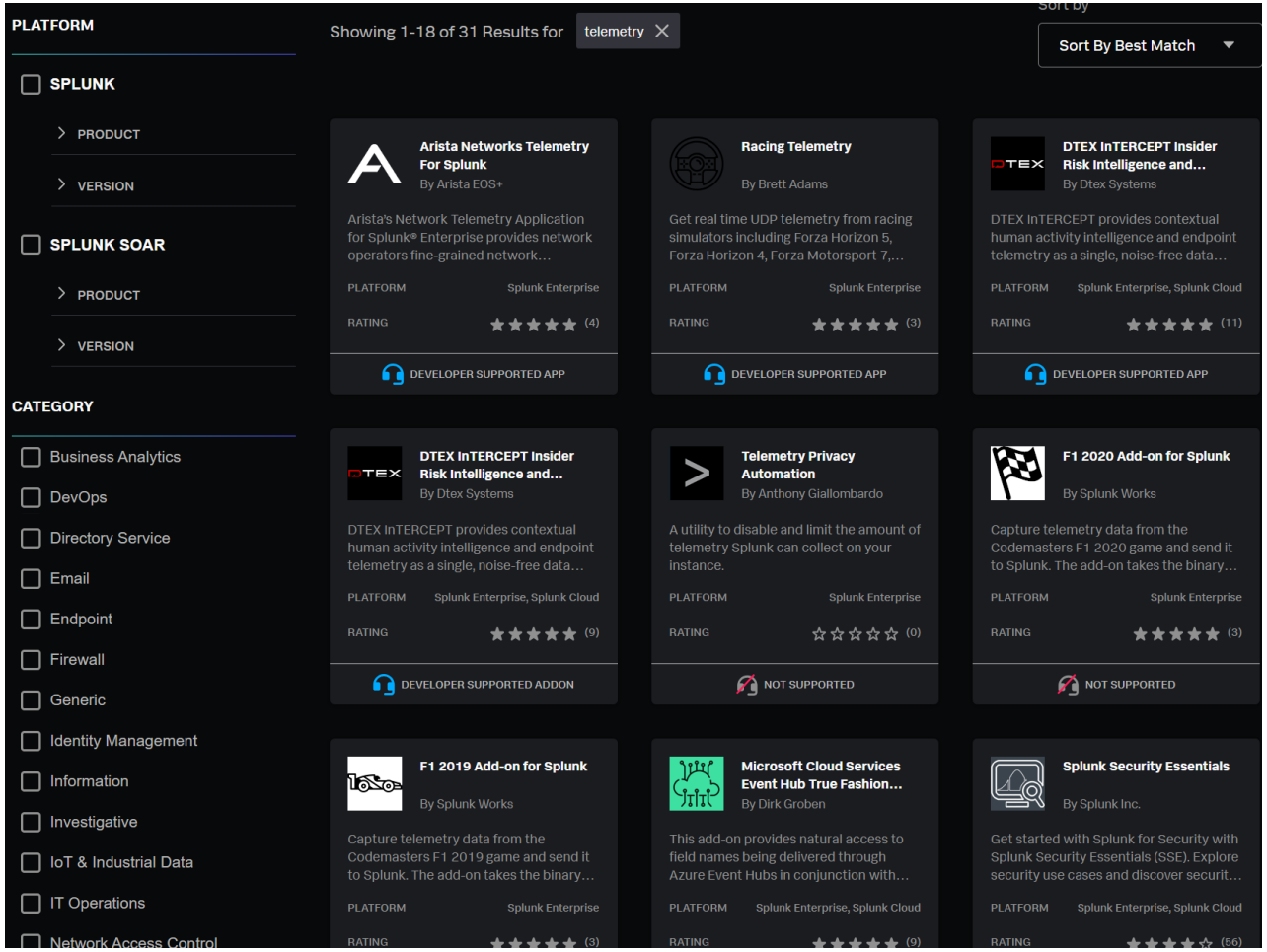


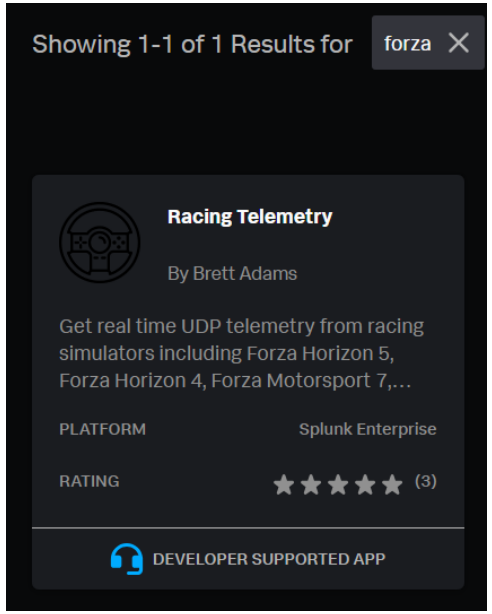
F1 23

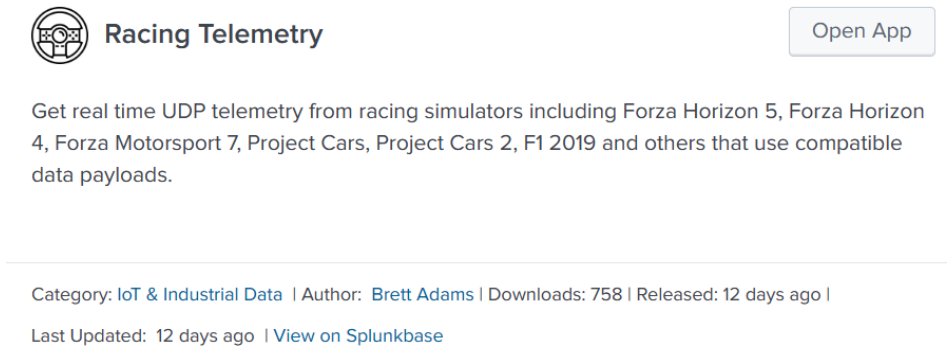


Konfiguracja

Wybór aplikacji i instalacja







Konfiguracja

Zbieranie danych

Name	Actions	Type	App
forza	Edit Delete Disable	Metrics	TA-racing-telemetry

Get metrics from Racing video games over UDP.

Rate Limit
Restrict the frequecy of data by r
100

Port
The UDP port to listen on
5606

Bind IP
The IP address to listen on
0.0.0.0

- [x] Metric Multi-Measurement
- [x] Filter Menu
- [ ] Use Source Timestamp

Telemetry Whitelist
Regex to filter metrics
car\..+

Konfiguracja

Wstępne wyniki

Odebrane dane


```
{ [-]
   CarClass: S2
   CarDriveTrain: AWD
   CarName: Lamborghini Centenario LP 770-4 (2016)
   GameState: Playing
   Lap: 3
   metric_name:car.Acceleration.Local.X: 0.4627000689506531
   metric_name:car.Acceleration.Local.Y: 3.5995571613311768
   metric_name:car.Acceleration.Local.Z: 2.4682834148406982
   metric_name:car.Boost: 0
   metric_name:car.Brake: 0
   metric_name:car.CarPerformanceIndex: 800
   metric_name:car.Clutch: 0
   metric_name:car.CurrentTime: 154.15721130371094
   metric_name:car.Distance: 5826.8359375
   metric_name:car.Fuel.Level: 1
   metric_name:car.Gear: 5
```


index

1 Value, 100% of events

Reports

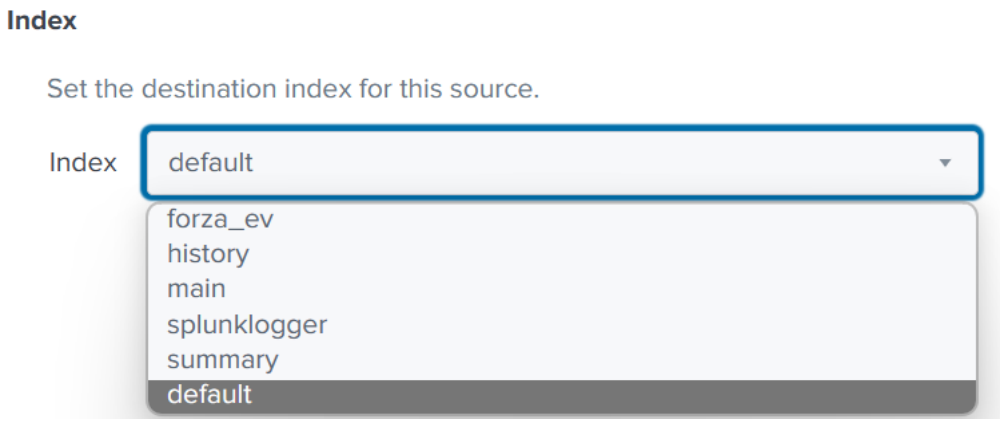
Top values Top values by time

Events with this field

Values	Count
main	1,554

Konfiguracja

Zmiana indexu



./etc/apps/TA-racing-telemetry/local/

- indexes.conf
- inputs.conf

inputs.conf

```
[racing-telemetry://Forza]
bindip = 0.0.0.0
filtermenu = 1
index = forza_ev
interval = -1
multimetric = 1
port = 5606
ratelimit = 100
sourcetype = racing-telemetry
usetimestamp = 0
whitelist = car\..+

[racing-telemetry://forza_metrics]
bindip = 0.0.0.0
filtermenu = 1
index = forza_m
interval = -1
multimetric = 1
port = 5607
ratelimit = 100
sourcetype = racing-telemetry
usetimestamp = 0
whitelist = car\..+
```

Indexy events oraz metrics

Główne zmiany w użyciu indexu metrics

Względem standardowego typu events

- Nieco zmienione funkcje do przetwarzania danych (mstats zamiast stats, mpreview zamiast search)
- Mniej zajętego miejsca

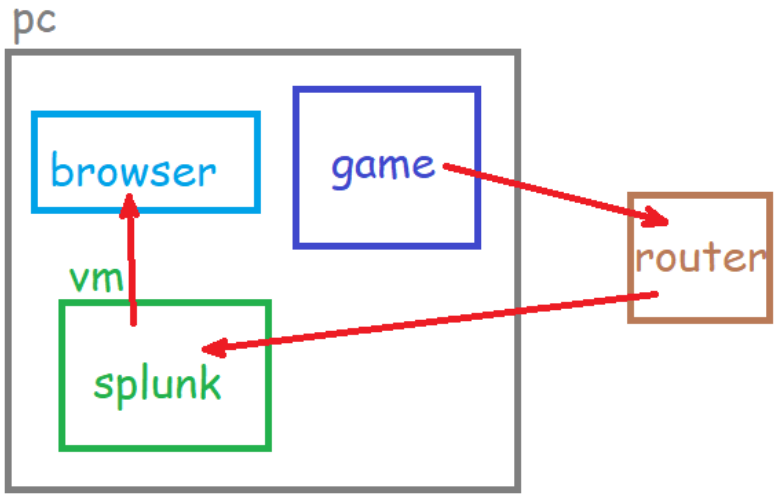
Name ▲	Actions	Type ⇕	App ⇕	Current Size ⇕	Max Size ⇕ ?	Event Count ⇕
forza_ev	Edit Delete Disable	Events	TA-racing-telemetry	112 MB	20 GB	9.56K
forza_m	Edit Delete Disable	Metrics	TA-racing-telemetry	11 MB	20 GB	9.93K

- Wydajność robi brrrrrr (od kilku do kilkudziesięciu razy szybciej niż eventy)

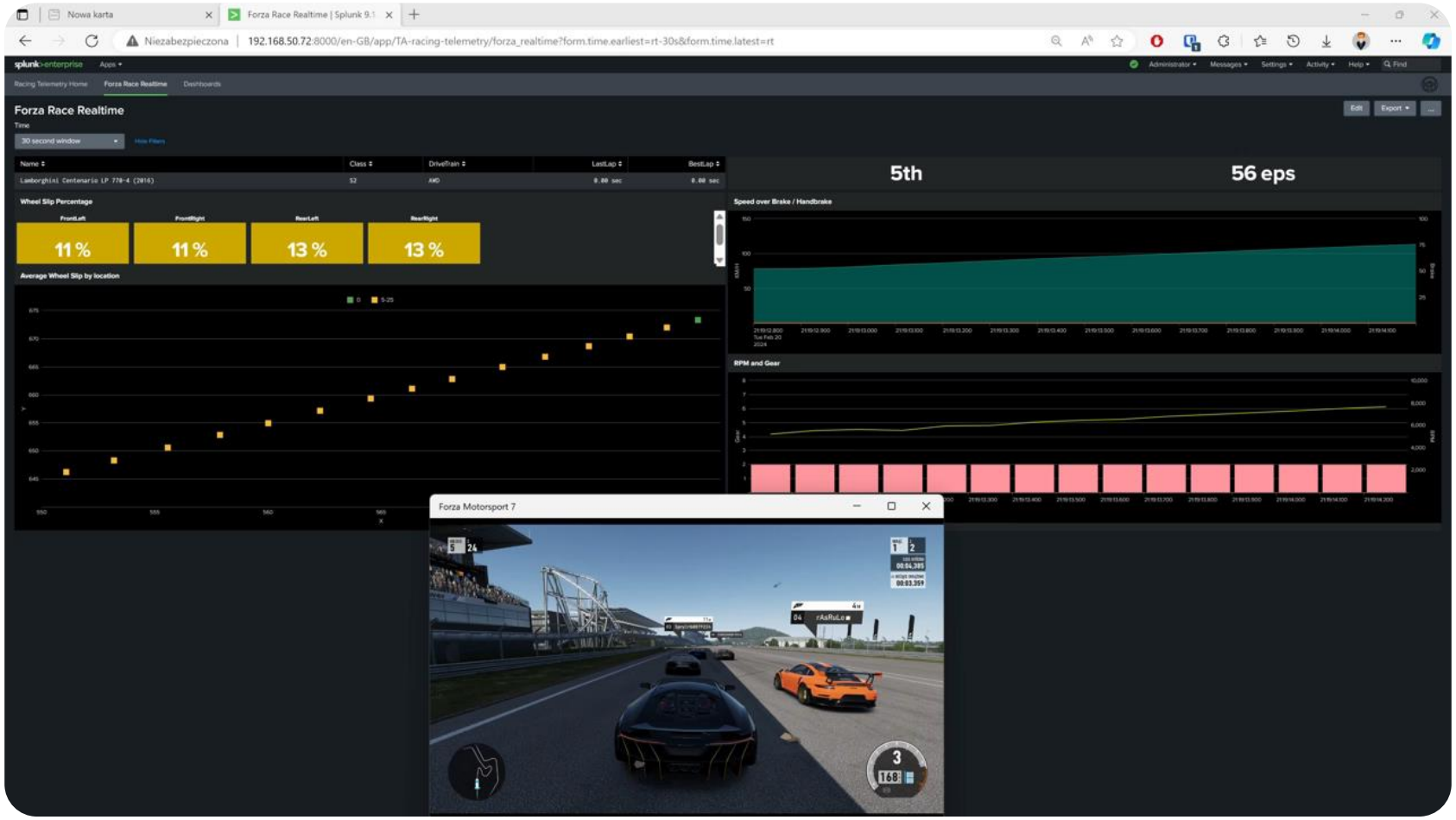
Przykład użycia

Przykład jak ja się za to zabrałem

- Środowisko
  - PC z systemem Windows
  - Maszyna wirtualna z system Windows i instancją Splunka
  - Sieć dostępna zarówno dla PC z grą jak i maszyny wirtualnej
- Oprogramowanie
  - Forza Motorsport 7 – gra służąca jako źródło danych
  - Edge – przeglądarka internetowa dająca dostęp do Splunka



Widok danych w trakcie wyścigu

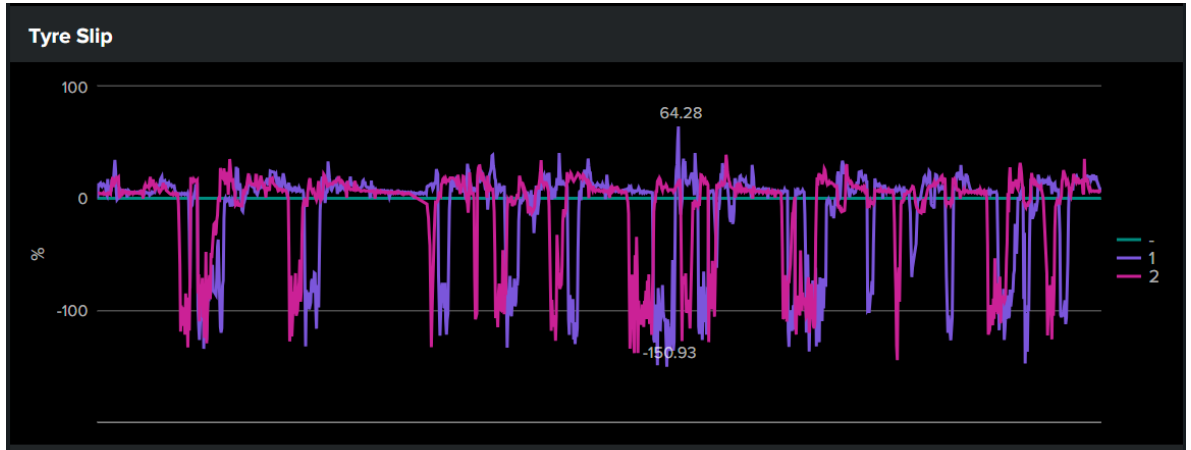


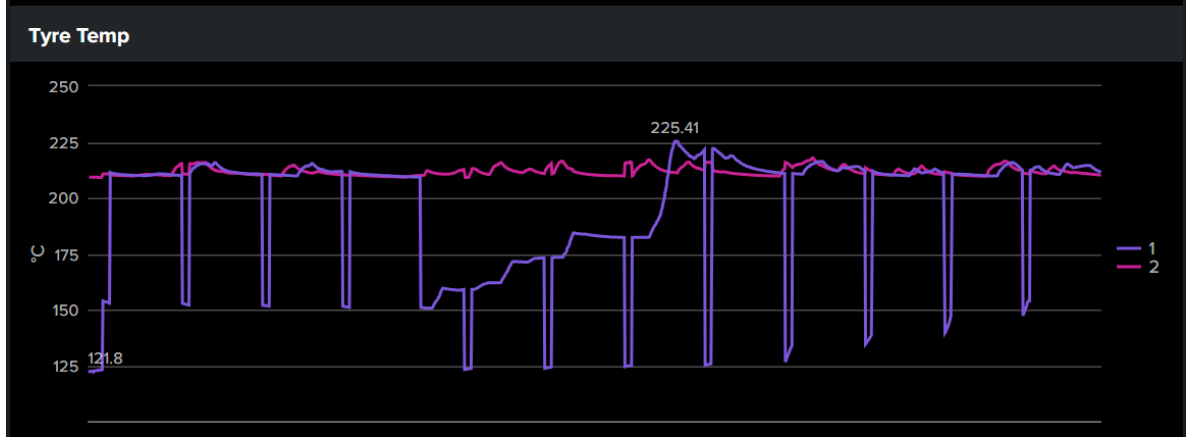
Dane po zakończeniu wyścigu

Ogólny dashboard

Dane po zakończeniu wyścigu

Szczegóły gazu, hamulca i dany dotyczących opon

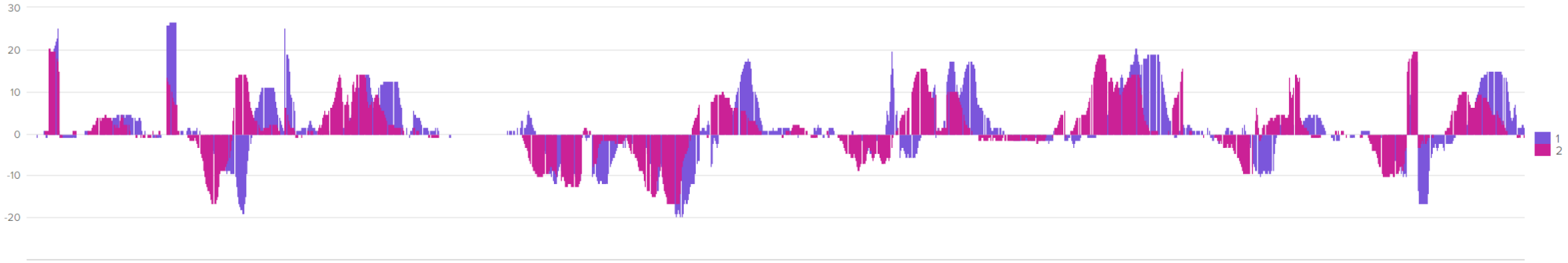




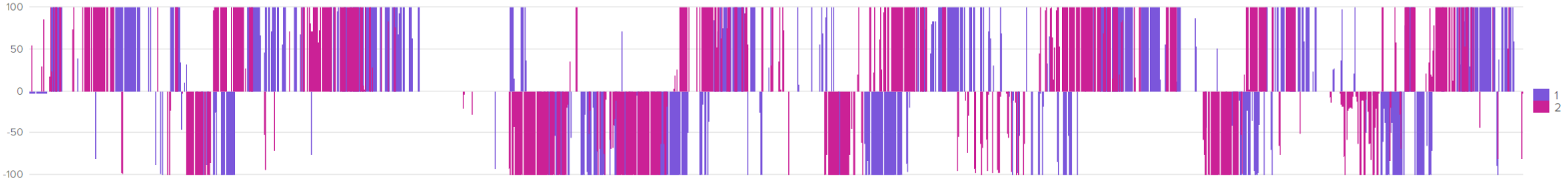
Dane po zakończeniu wyścigu

Porównaniu danych wejściowych kąta skrętu kół

Kierownica



Gamepad



Po co to wszystko?

Po co to wszystko?

Po co to wszystko?

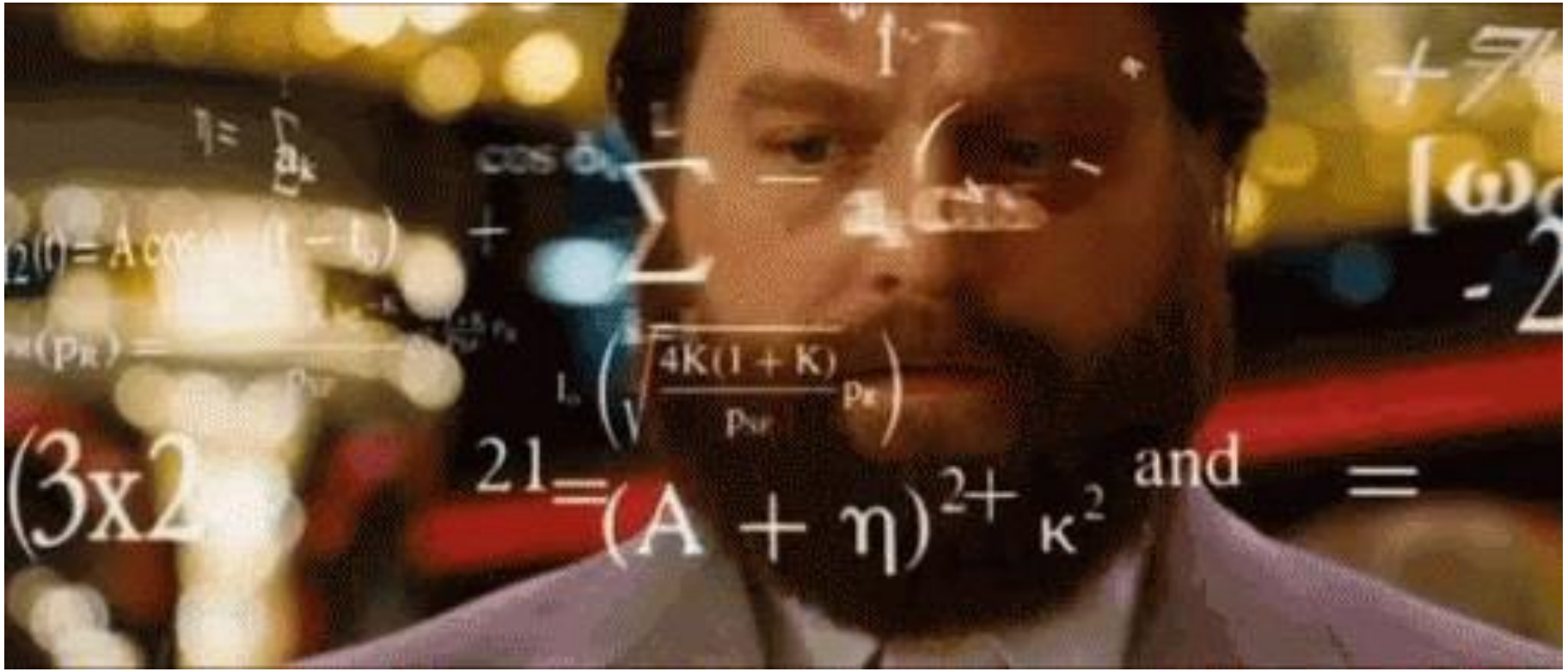
Analiza danych i wykonanie dashboardów w pracy

Po co to wszystko?

Analiza danych i wykonanie dashboardów w pracy

Po co to wszystko?

Chęć poprawy w wyścigach



Po co to wszystko?

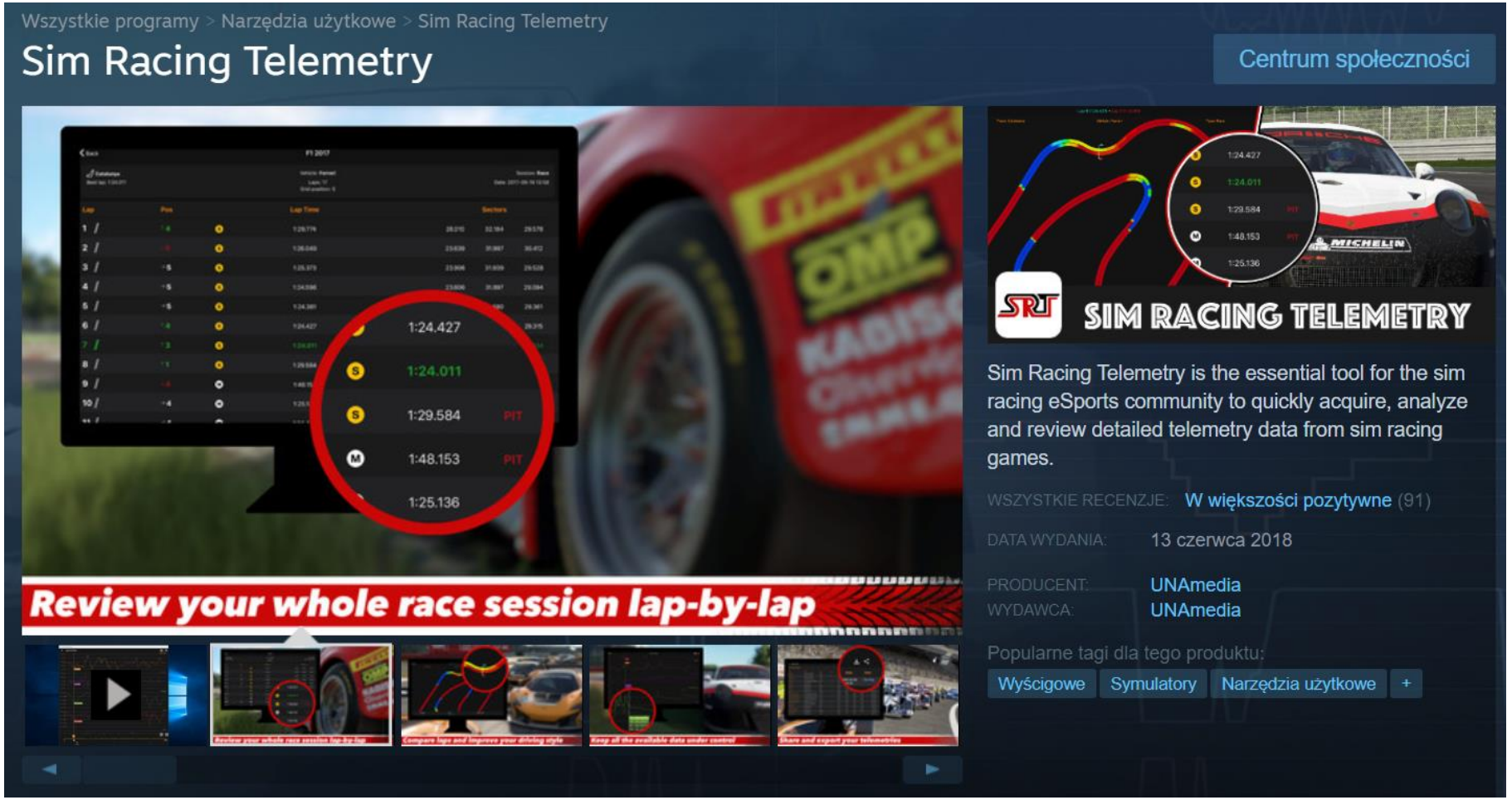
Chęć poprawy w wyścigach

Alternatywy do Splunka

Elasticsearch

Alternatywy dla Splunka

Sim Racing Telemetry - Steam



Warto się zapoznać

Materiały z których korzystałem

- https://docs.splunk.com/
- https://www.youtube.com/@BrettAdams
- https://splunkbase.splunk.com/app/4884
- https://kinneygroup.com/blog/working-with-splunk-metrics-indexes/
- https://www.puurdata.nl/us/f1-racen-voor-gevorderden-met-elastic-part-2/

Może Ty używasz narzędzia, które można użyć inaczej?