



Użycie narzędzi znanych z pracy w celach innych niż praca

Patryk Stachowiak

Kim jestem

Jak tu wylądowałem

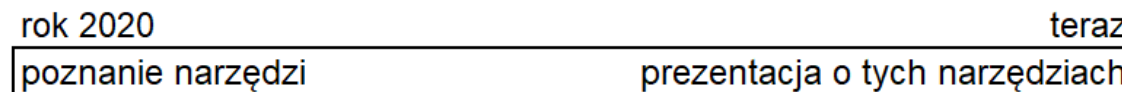
Życie



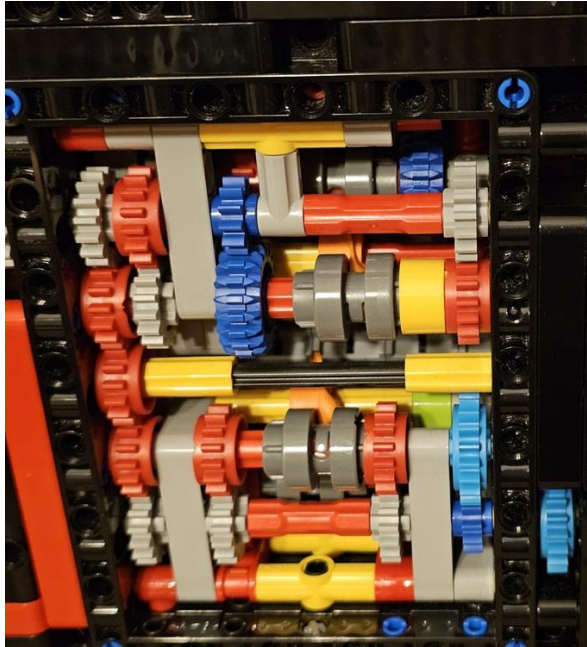
Praca w GSK



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

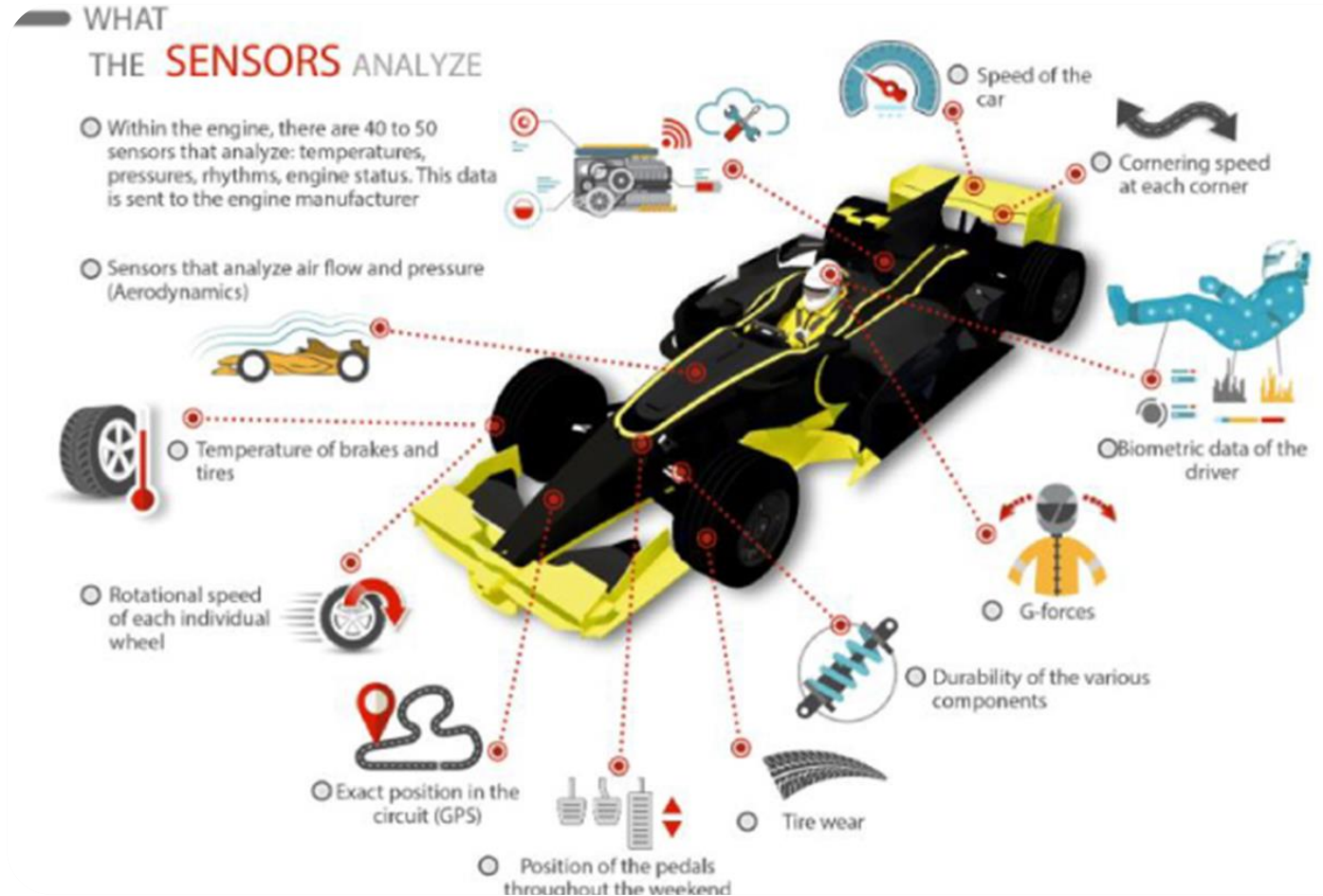


Zbieranie danych / Telemetria w motorsporcie

- 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



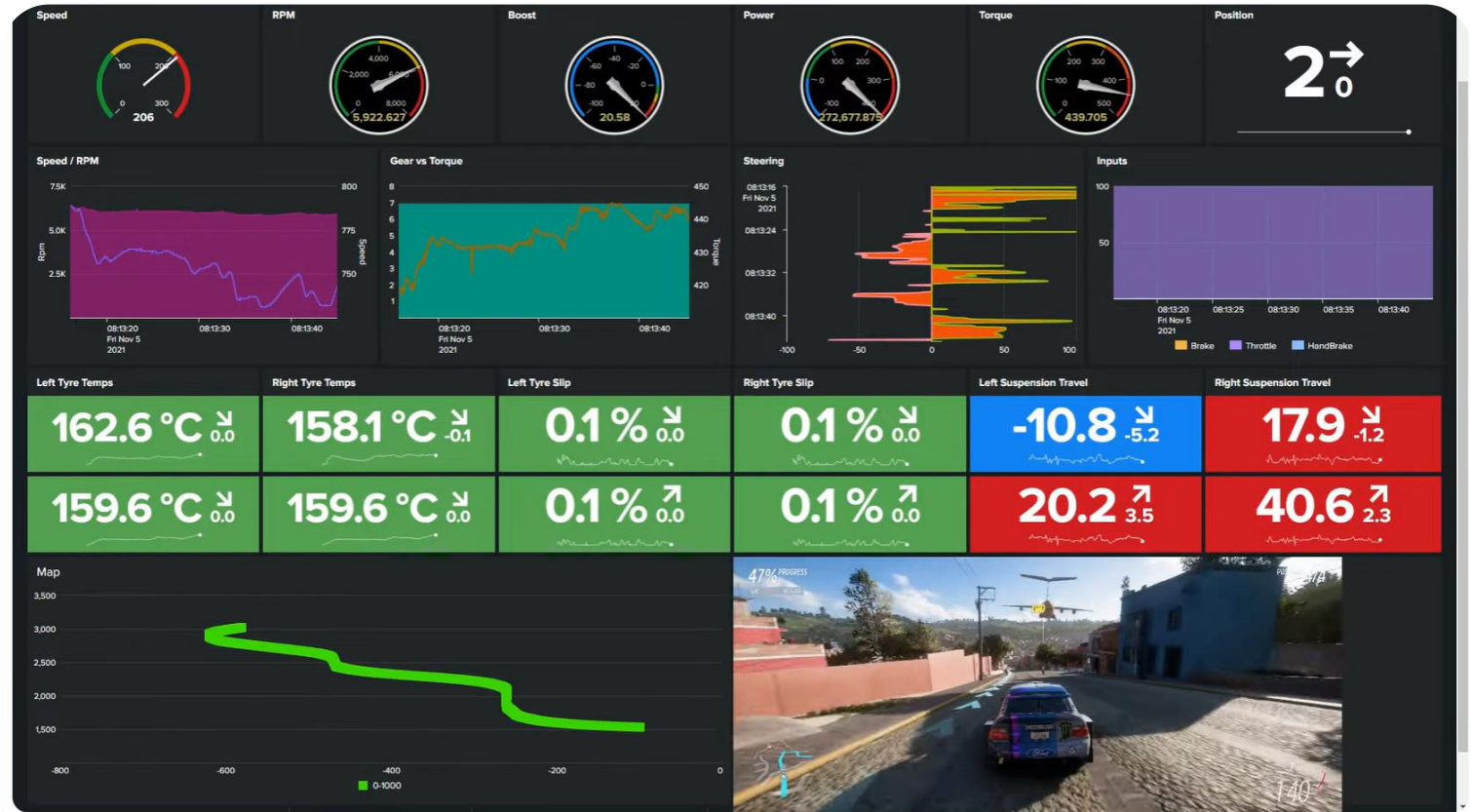
Telemetria

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

ELEMENTY NA EKRANIE	
KATEGORIA	OPCJA DO MODYFIKACJI
DUCHY	TYLKO RYWALE
WIADOMOŚĆ PRZEWIJANIA	WŁ.
OSIĄGNIĘCIA WYŚCIGOWE	WŁ.
EKRAN DRIFTOWY	WYL.
OSTRZEŻENIA NA TORZE	WŁ.
OSTRZEŻENIA O BOKSIE NAD AUTAMI	WŁ.
WIADOMOŚCI I WSKAZÓWKI BOKSU	WŁ.
STRZAŁKI BLISKOŚCI	WŁ.
OGRANICZENIA TORU	BLISKOŚĆ
STYL OGRANICZEŃ TORU	ZNACZNIKI
WYJŚCIE DANYCH	WŁ. 
ADRES IP WYJŚCIA DANYCH	192.168.50.72
PORT IP WYJŚCIA DANYCH	5607
FORMAT PAKIETÓW DANYCH WYJŚCIOWYCH	DESKA ROZDZIELCZA SAMOCHODU

F1 23

USTAWIENIA TELEMETRII  	
Telemetria UDP	 Włączone
Tryb transmisji UDP	 Wyłączone
Adres IP UDP	...  192.168.50.72
Port UDP	...  5608
Częstotliwość wysyłania UDP	 20 Hz
Format UDP	 2023
Twoja telemetria	 Zastrzeżono
Pokaż identyfikatory internetowe	 Wyłączone

Konfiguracja

Wybór aplikacji i instalacja

The screenshot shows the Splunk App Store search results for the keyword 'telemetry'. The interface includes a search bar at the top with 'Showing 1-18 of 31 Results for telemetry' and a 'Sort By Best Match' dropdown. On the left, there are filters for 'PLATFORM' (SPLUNK, SPLUNK SOAR) and 'CATEGORY' (Business Analytics, DevOps, Directory Service, Email, Endpoint, Firewall, Generic, Identity Management, Information, Investigative, IoT & Industrial Data, IT Operations, Network Access Control). The main area displays a grid of app cards. The 'Racing Telemetry' app by Brett Adams is highlighted, showing a 5-star rating and 'DEVELOPER SUPPORTED APP' status. Other visible apps include 'Arista Networks Telemetry For Splunk', 'DTEX InTERCEPT Insider Risk Intelligence and...', 'Telemetry Privacy Automation', 'F1 2020 Add-on for Splunk', 'F1 2019 Add-on for Splunk', 'Microsoft Cloud Services Event Hub True Fashion...', and 'Splunk Security Essentials'.

This is a detailed view of the 'Racing Telemetry' app. At the top, it says 'Showing 1-1 of 1 Results for forza'. The app card features the 'Racing Telemetry' icon, the title 'Racing Telemetry' by Brett Adams, and a description: 'Get real time UDP telemetry from racing simulators including Forza Horizon 5, Forza Horizon 4, Forza Motorsport 7, ...'. It lists the platform as 'Splunk Enterprise' and has a 5-star rating with 3 reviews. A 'DEVELOPER SUPPORTED APP' badge is visible at the bottom.



Racing Telemetry

Open App

Get real time UDP telemetry from racing simulators including Forza Horizon 5, Forza Horizon 4, Forza Motorsport 7, Project Cars, Project Cars 2, F1 2019 and others that use compatible data payloads.

Category: IoT & Industrial Data | Author: Brett Adams | Downloads: 758 | Released: 12 days ago |

Last Updated: 12 days ago | [View on Splunkbase](#)

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 frequency of data by r

Port The UDP port to listen on

Bind IP The IP address to listen on

Metric Multi-Measurement

Filter Menu

Use Source Timestamp

Telemetry Whitelist Regex to filter metrics

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

Index

Set the destination index for this source.

Index

- forza_ev
- history
- main
- splunklogger
- summary
- default

```
← ↻ T ? ☰ ⚡ ☆ inputs.conf
./etc/apps/TA-racing-telemetry/local/
└─ indexes.conf
└─ inputs.conf
1
2 [racing-telemetry://Forza]
3 bindip = 0.0.0.0
4 filtermenu = 1
5 index = forza_ev
6 interval = -1
7 multimetric = 1
8 port = 5606
9 ratelimit = 100
10 sourcetype = racing-telemetry
11 usetimestamp = 0
12 whitelist = car\..+
13
14 [racing-telemetry://forza_metrics]
15 bindip = 0.0.0.0
16 filtermenu = 1
17 index = forza_m
18 interval = -1
19 multimetric = 1
20 port = 5607
21 ratelimit = 100
22 sourcetype = racing-telemetry
23 usetimestamp = 0
24 whitelist = car\..+
25
```

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

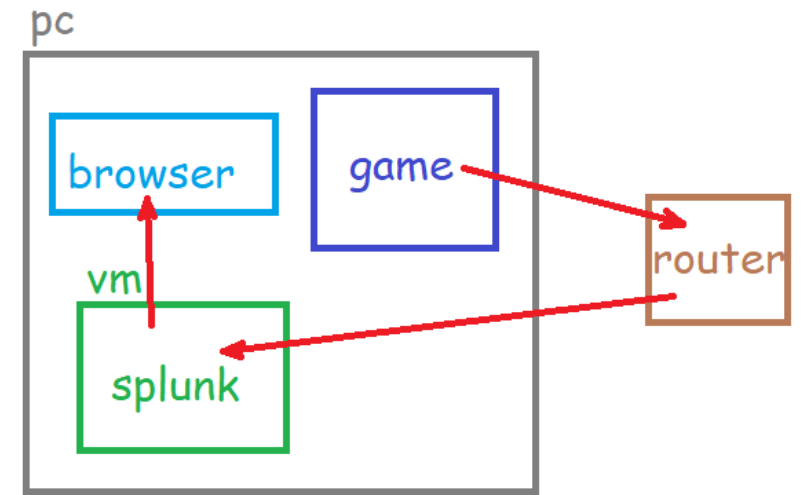
- Wydajność robi brrrrrr (od kilku do kilkudziesięciu razy szybciej niż eventy)



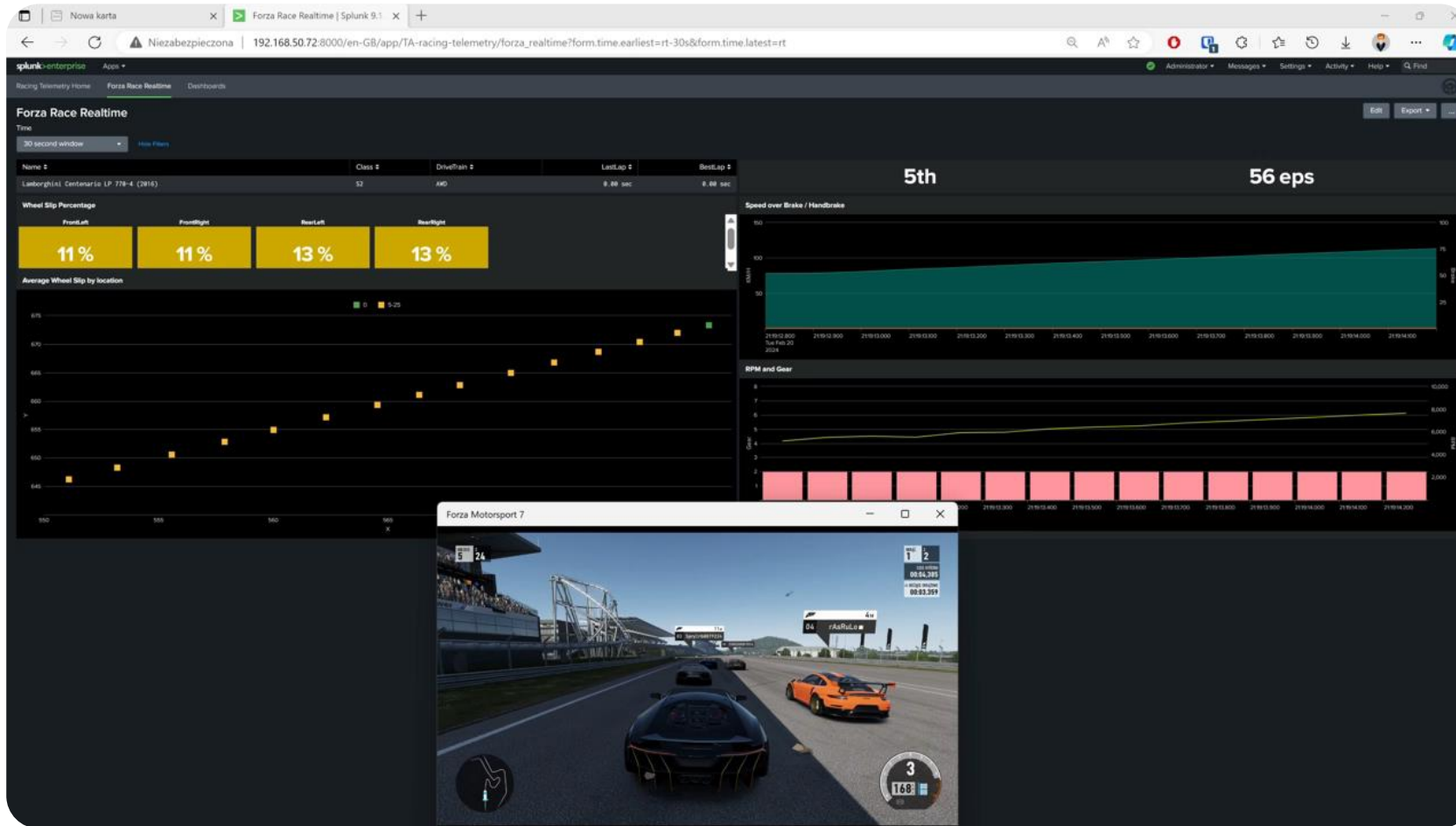
Przykład użycia

Przykład jak ja się za to zabrałem

- Środowisko
 - PC z systemem Windows
 - Maszyna wirtualna z systemem 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



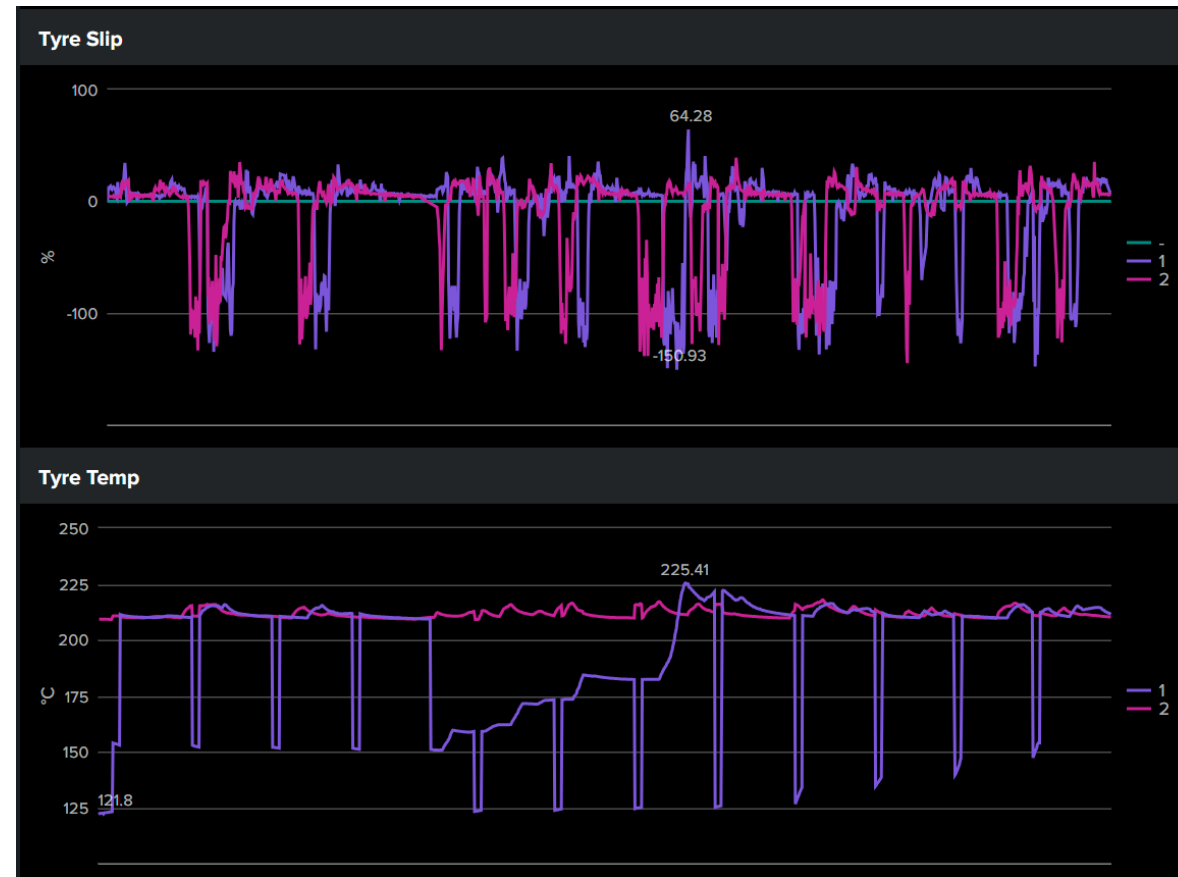
Dane po zakończeniu wyścigu

Ogólny dashboard



Dane po zakończeniu wyścigu

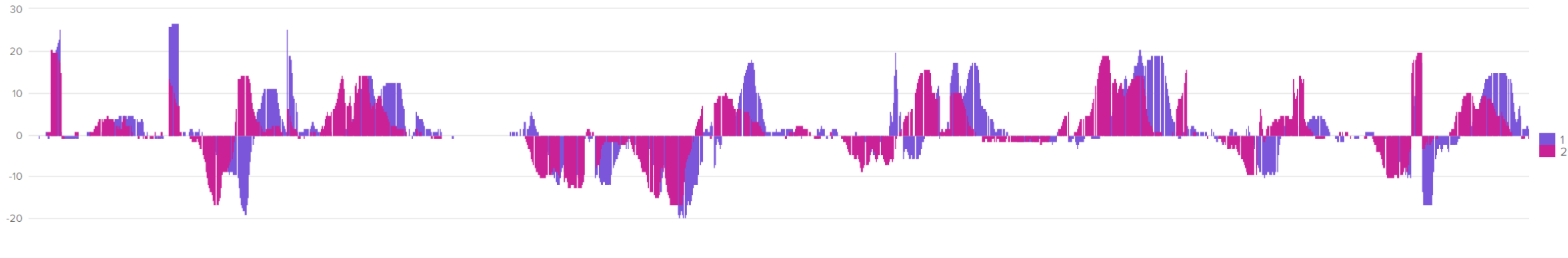
Szczegóły gazu, hamulca i dany dotyczących opon



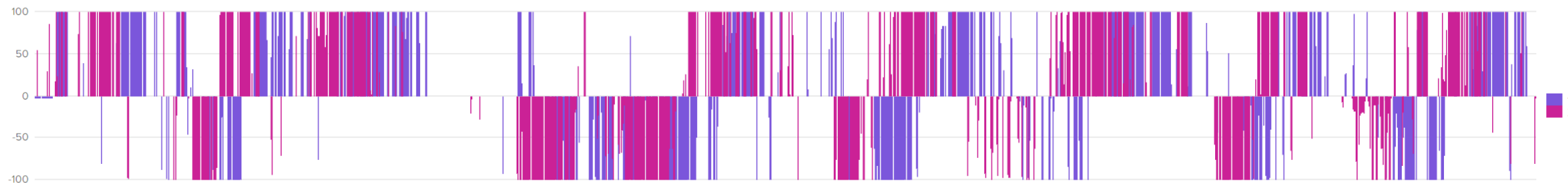
Dane po zakończeniu wyścigu

Porównaniu danych wejściowych kąta skrętu kół

Kierownica



Gamepad



Po co to wszystko?



Po co to wszystko?

Nauka poprzez
zabawę

Po co to wszystko?

Analiza danych i wykonanie dashboardów w pracy



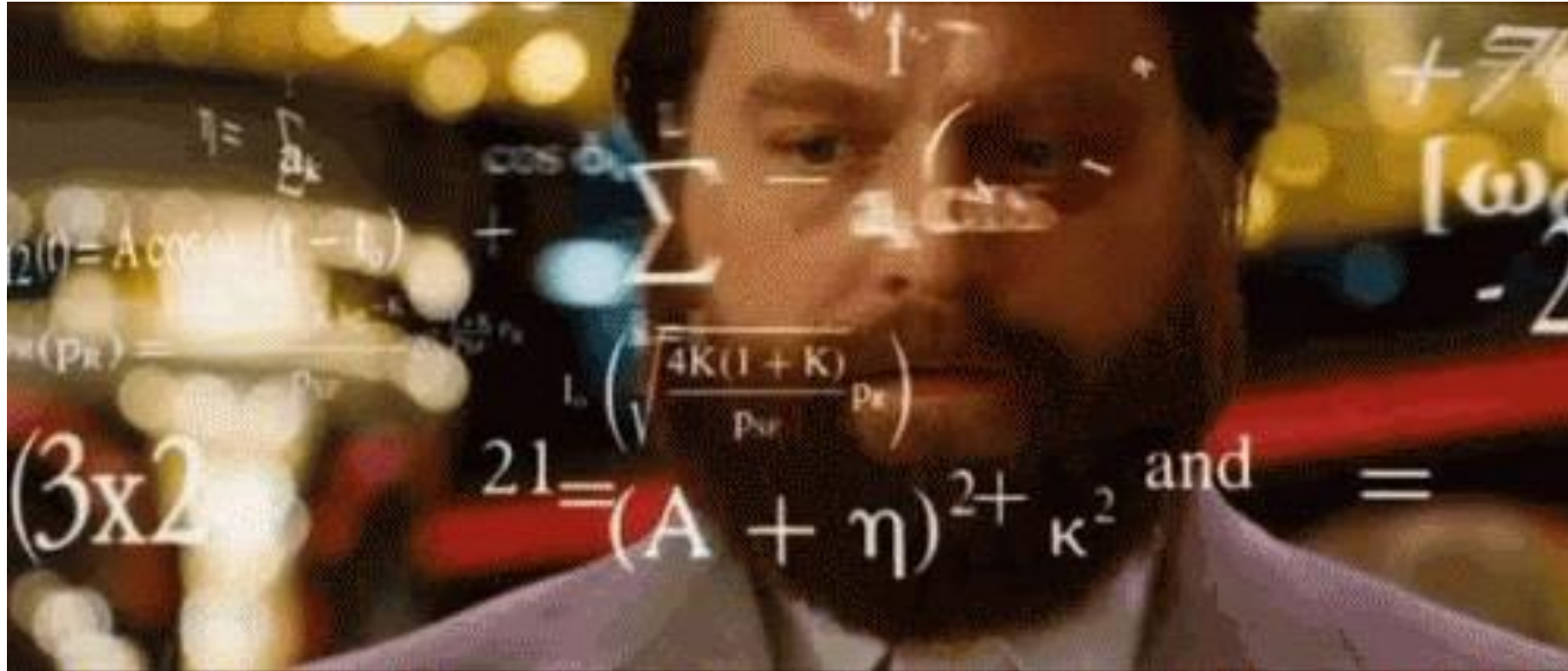
Po co to wszystko?

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



FREE

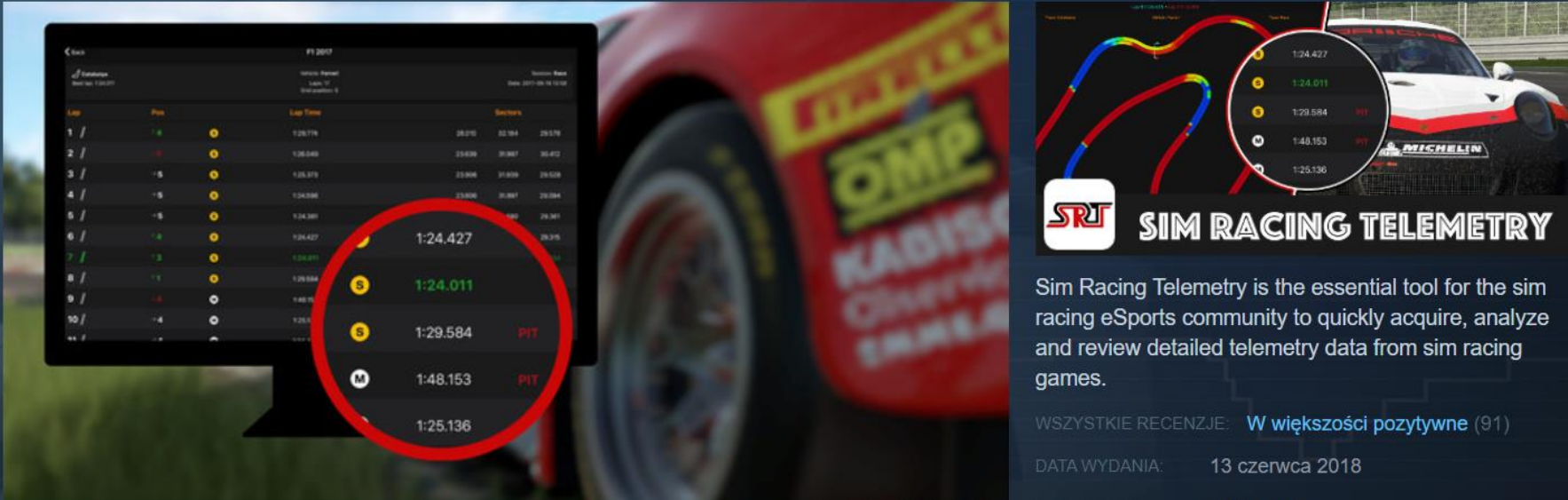
Alternatywy dla Splunka

Sim Racing Telemetry - Steam

Wszystkie programy > Narzędzia użytkowe > Sim Racing Telemetry

Sim Racing Telemetry

Centrum społeczności



Lap	Pos	Lap Time	Sections
1 /		1:26.776	28.070 32.364 29.376
2 /		1:26.648	27.838 31.987 30.472
3 /	-5	1:26.873	27.896 31.858 29.528
4 /	-5	1:24.586	27.808 31.987 29.284
5 /	-5	1:24.381	27.897 31.987 29.381
6 /	-4	1:24.427	27.897 31.987 29.376
7 /	-3	1:24.011	
8 /	-1	1:29.584	PIT
9 /	-	1:48.153	PIT
10 /	-4	1:25.136	

Review your whole race session lap-by-lap

Wyścigowe Simulatory Narzędzia użytkowe +

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?

