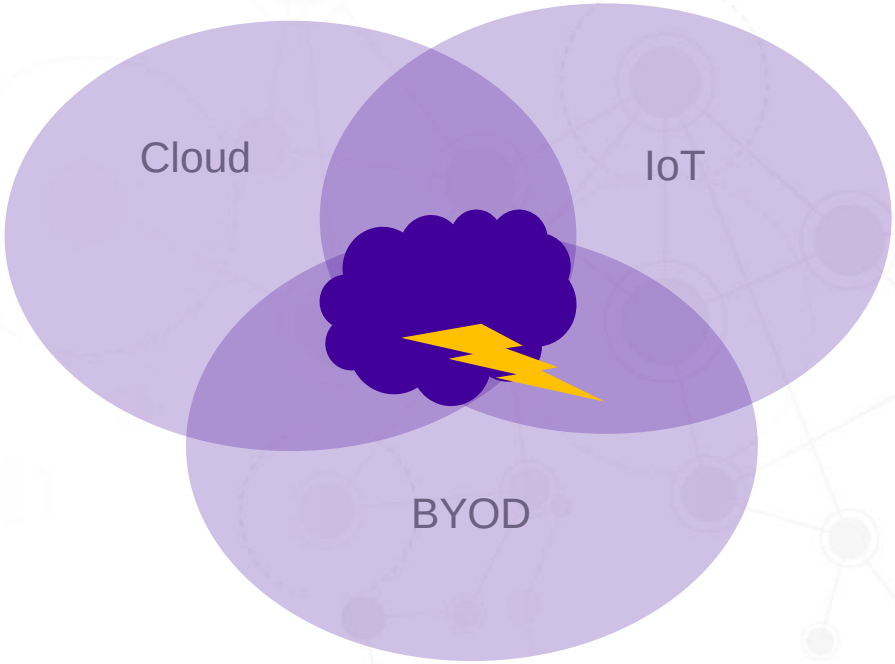
Безопасность в ЛВС: Идеальный шторм

Москва, 11 апреля 2019 г.

Cloud, IoT & BYOD… идеальный шторм

- Многие BYOD & IOT устройства требуют cloud сервисы для работы
- Это дает широчайший плацдарм для атак и открывает несколько серьезных уязвимостей в традиционной модели безопасности
- Нужны новые подходы



«Страшилки…»

Которые мы уже знаем

The Threats are Real

Las Vegas Casino Breached Through Connected Fish Tank

"S

vu

- J

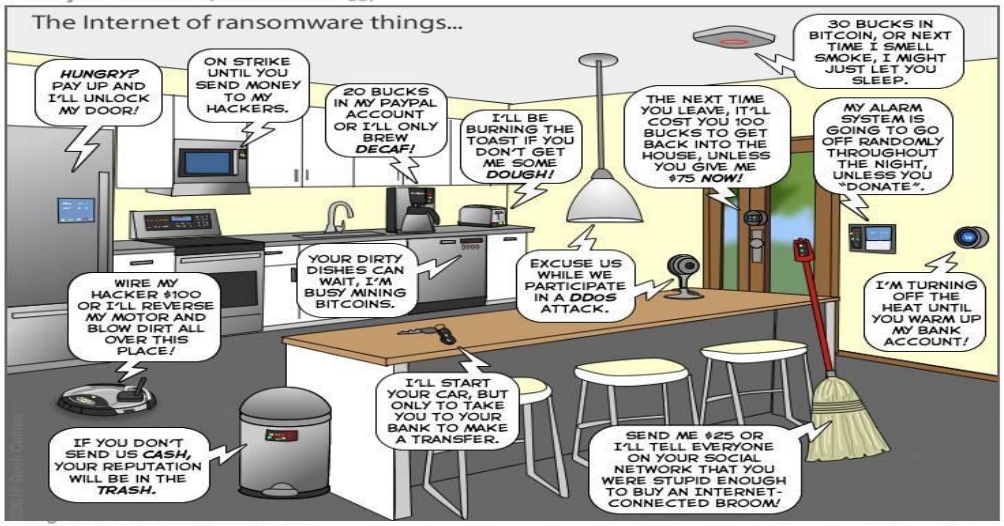
IoT D

Mirai Botnet Vi

"Mirai B
like se
effe
machin
popula
th

- The Guardian

The Joy of Tech™ by Nitrozac & Snaggy



«Страшилки…»

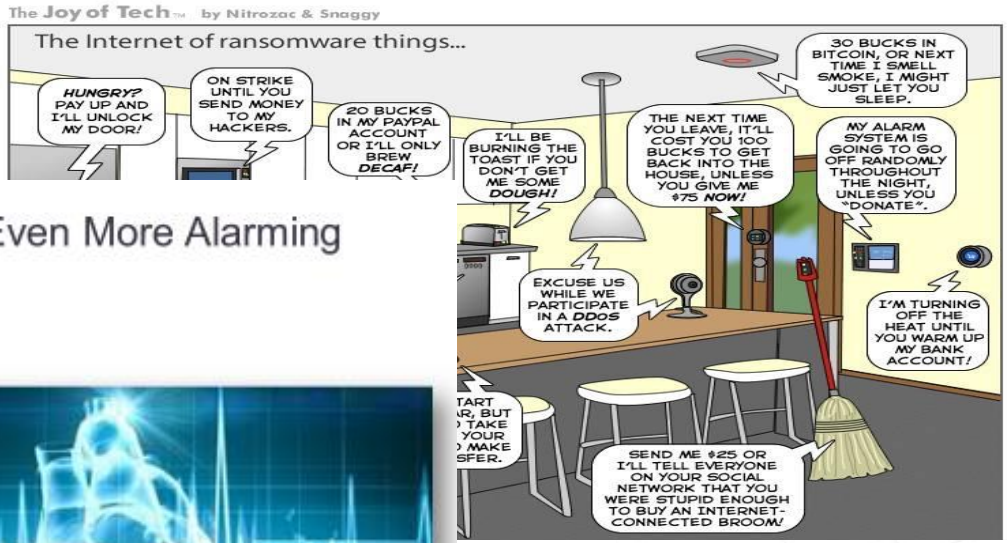
Которые мы уже знаем

The Threats are Real

Las Vegas Casino Breached Through Connected Fish Tank

But the Potential Impact to Patients is Even More Alarming

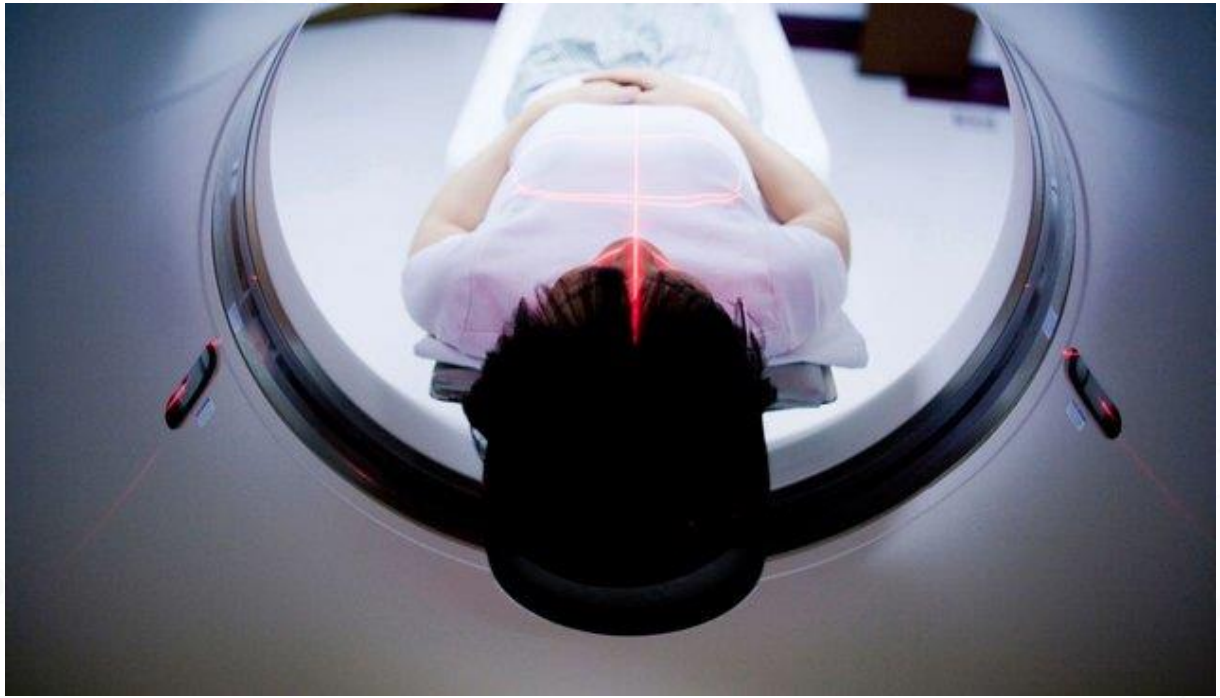
- In October 2016, Johnson & Johnson issued a warning that one of its insulin pumps for diabetics was at risk of being **hacked, causing a lethal overdose**.
- In August 2017, 465,000 U.S. residents **received notices** to update the firmware that runs their life-sustaining Abbott (formerly St. Jude Medical) pacemakers, or risk falling victim to potentially fatal hacks.



EXTREME NOW

Malware, которое может «заразить» вас раком

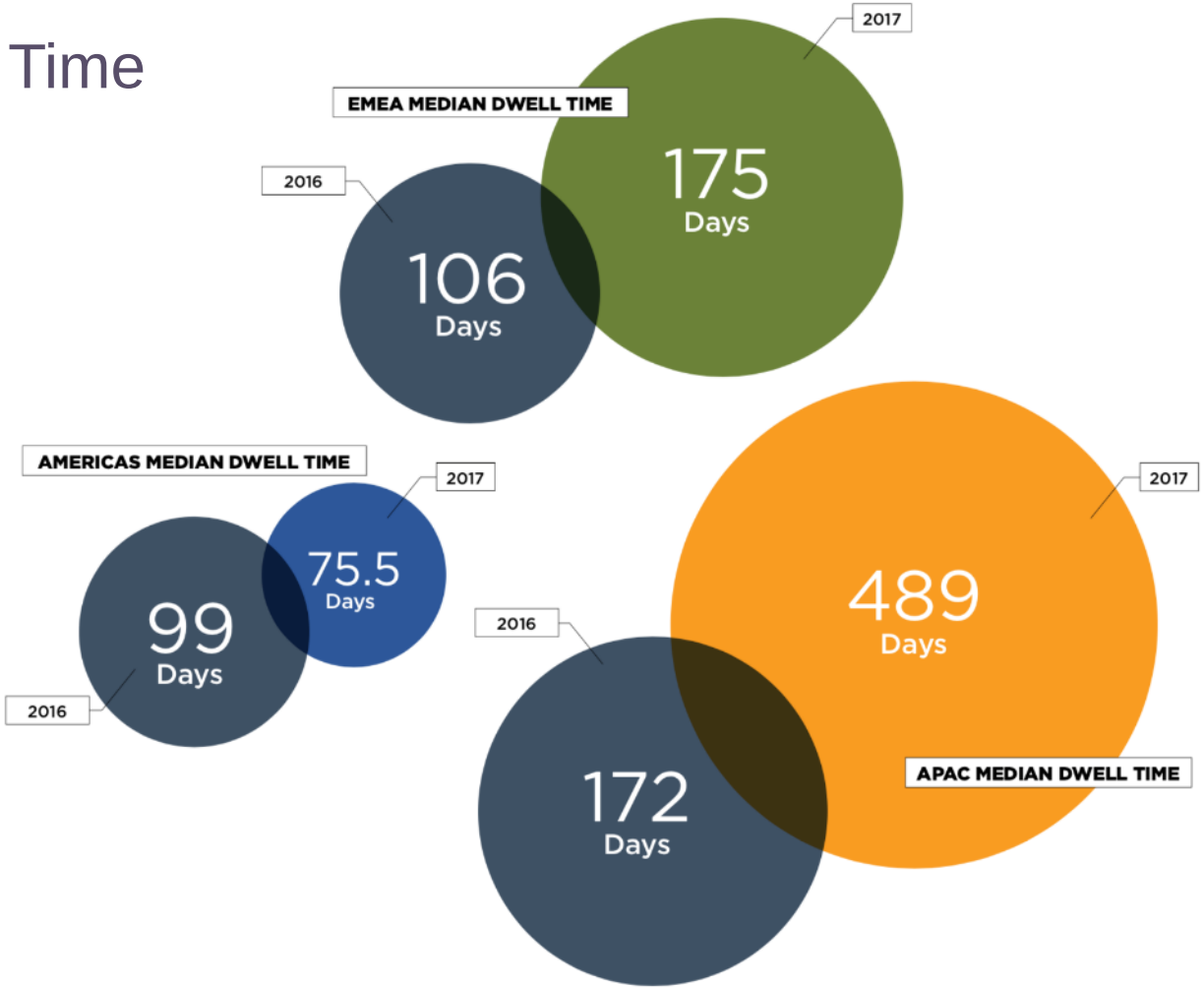
- **Создан компьютерный вирус, меняющий результаты МРТ и КТ. Врачи не в состоянии заметить подмену**



…вредоносное программное обеспечение, которое позволяло автоматически вносить изменения в результаты КТ и МРТ, прежде чем их изучат врачи. Программа могла добавлять в изображения реалистичные злокачественные опухоли или наоборот, удалять из них настоящие новообразования…

https://meduza.io/feature/2019/04/04/sozdan-kompyuternyy-virus-menyayuschiy-rezultaty-mrt-i-kt-iz-za-nego-vrachi-stavyat-nepravilnye-diagnozy-the-washington-post

Dwell Time



Dwell time is the number of days from first evidence of compromise that an attacker is present on a victim network before detection.

Source: FireEye M-Trend2018 Report

Как улучшить безопасность на уровне доступа ?

Risk Assessment

Isolation / Segmentation

Policy

Application Telemetry

Compliance

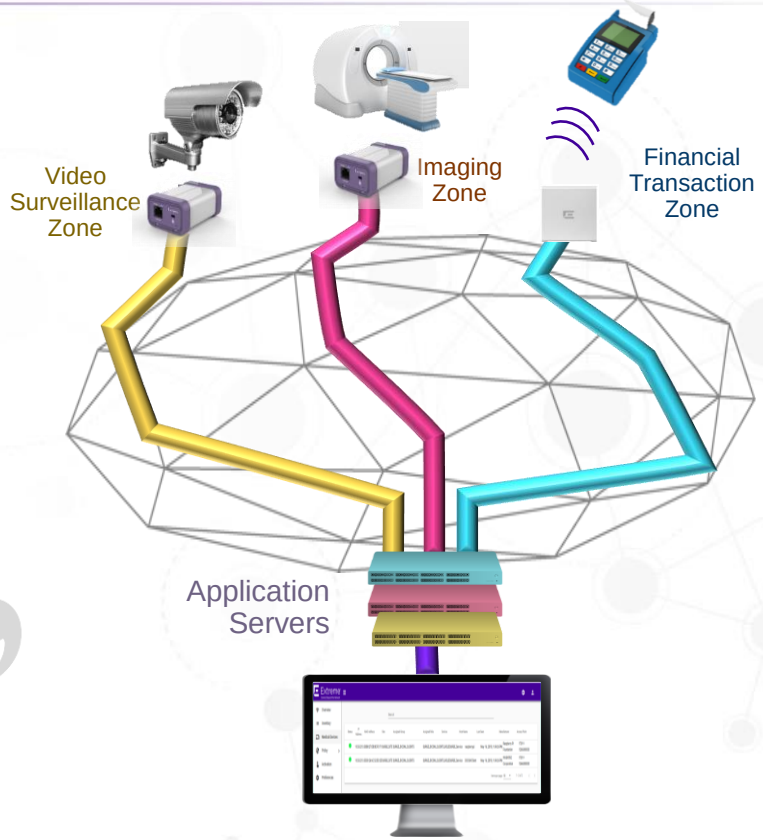
Emerging Technologies (AI/ML)

Open Security Ecosystem

Изоляция IoT устройств - Зоны безопасности

Только 5% устройств IoT сегодня сегментированы

Тем не менее, к 2021 должны быть 60%

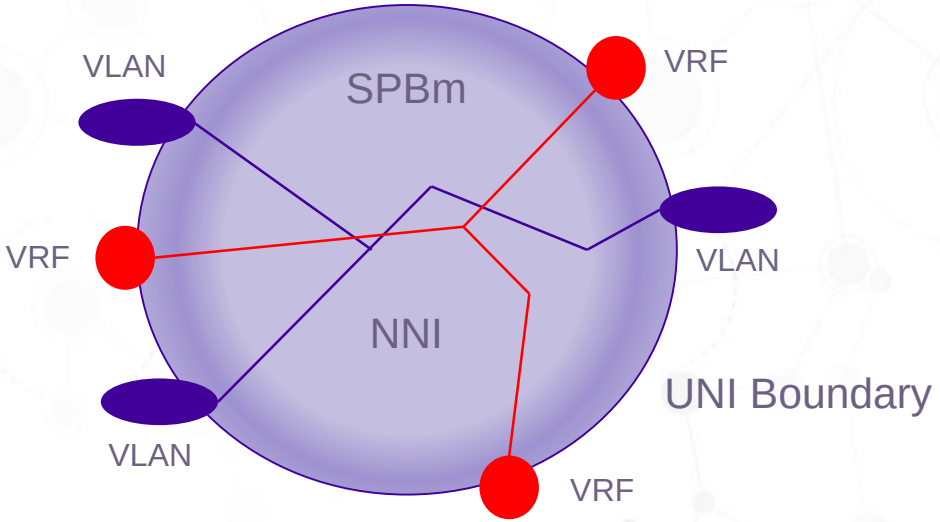


IoT Solutions Can't Be Trusted and Must Be Separated From the Enterprise Network to Reduce Risk

- Tim Zimmerman and Barika L Pace. May 2018

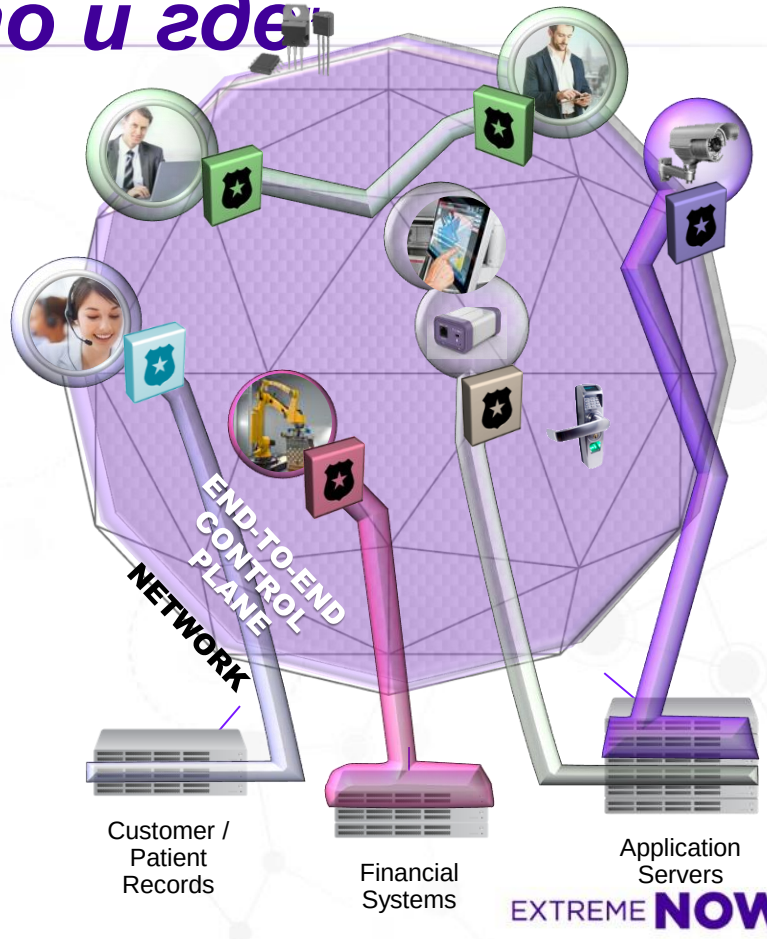
Extreme Fabric Connect ‘Worm Hole’ analogy

- Given that Fabric Connect is not based on IP routing but instead on Ethernet switched paths which are ‘dark’ to IP forensic techniques, Fabric Connect might be compared to a worm hole or black hole in physics.
- The inside of the Fabric is based on BVID, BMAC and I-SID values via Ethernet Switched Paths.
- All service phenomenon's are at the UNI edge could be equated to the ‘Event Horizon’.
- Visibility of the service core from the service edge is not possible



Policy:
“Кому можно делать что и где”

- Network Segmentation на базе политик
- Для IOT использовать Whitelist Profile; ЗАПРЕТИТЬ все за исключением указанного
- Строгое отслеживание пользователей в и из зоны безопасности
- Эластичные границы
- Эффективные CAPEX и OPEX

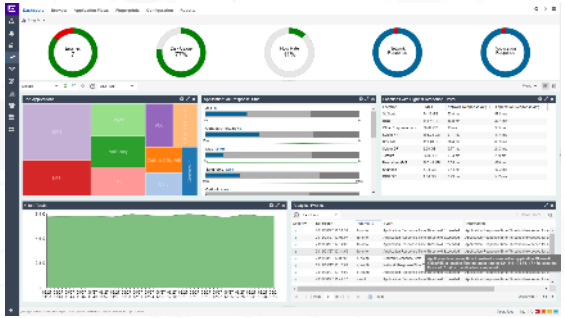


Application Telemetry & Analytics

- Критически важно для безопасности Инфраструктуры
- Трафика East/West все больше
- Центральный МСЭ хорош для North/South
  - Но не на столько для east/west peer to peer
- Аномальный трафик внутри сегмента может быть обнаружен или заблокирован

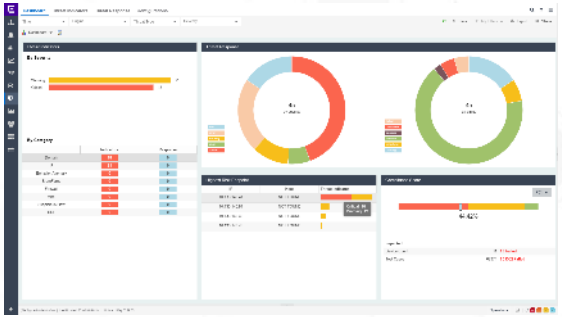
Analytics in 2019

IOT + Wireless + Edge Switching + Campus + DC + Virtual



Network Analytics

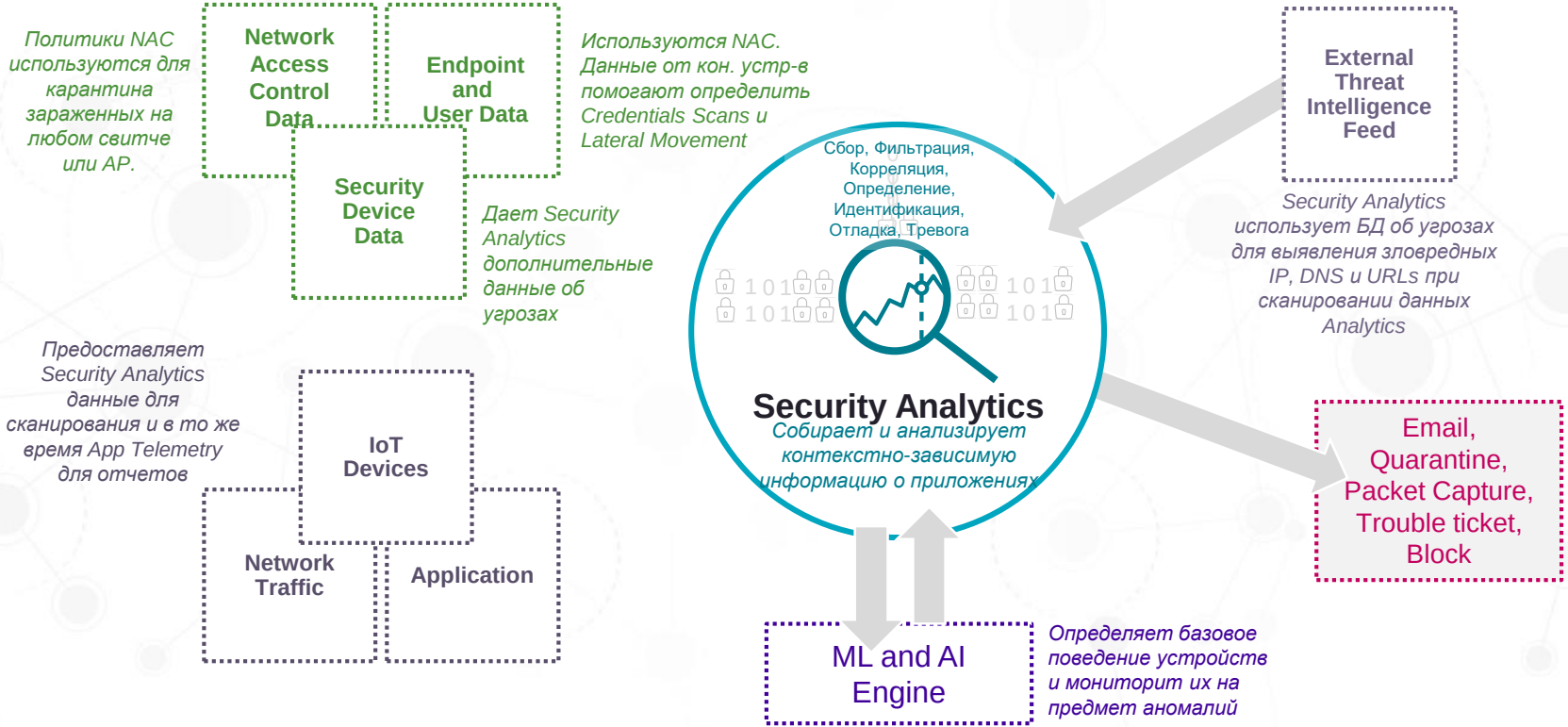
Application Analytics



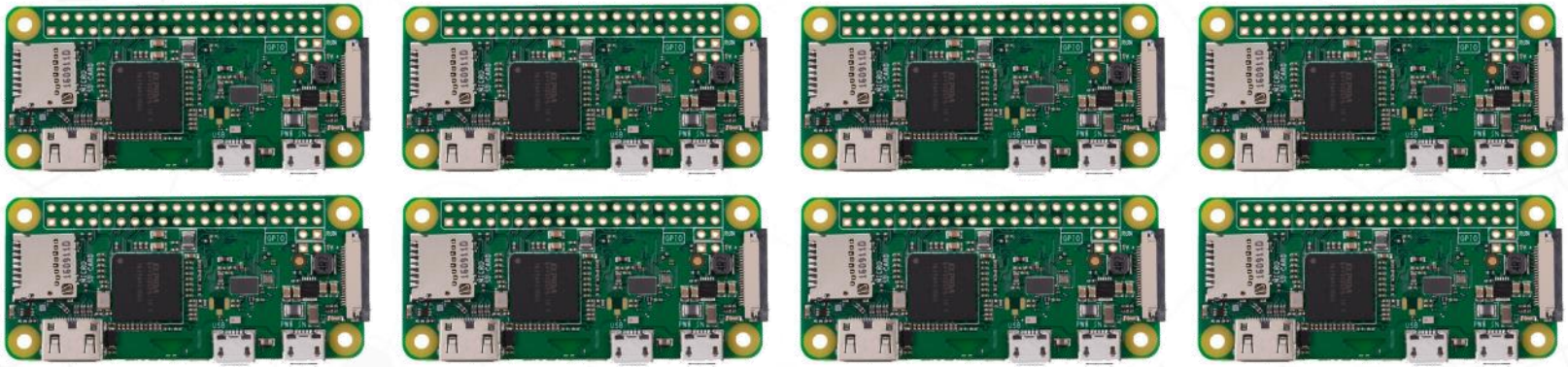
Security Analytics (2019)

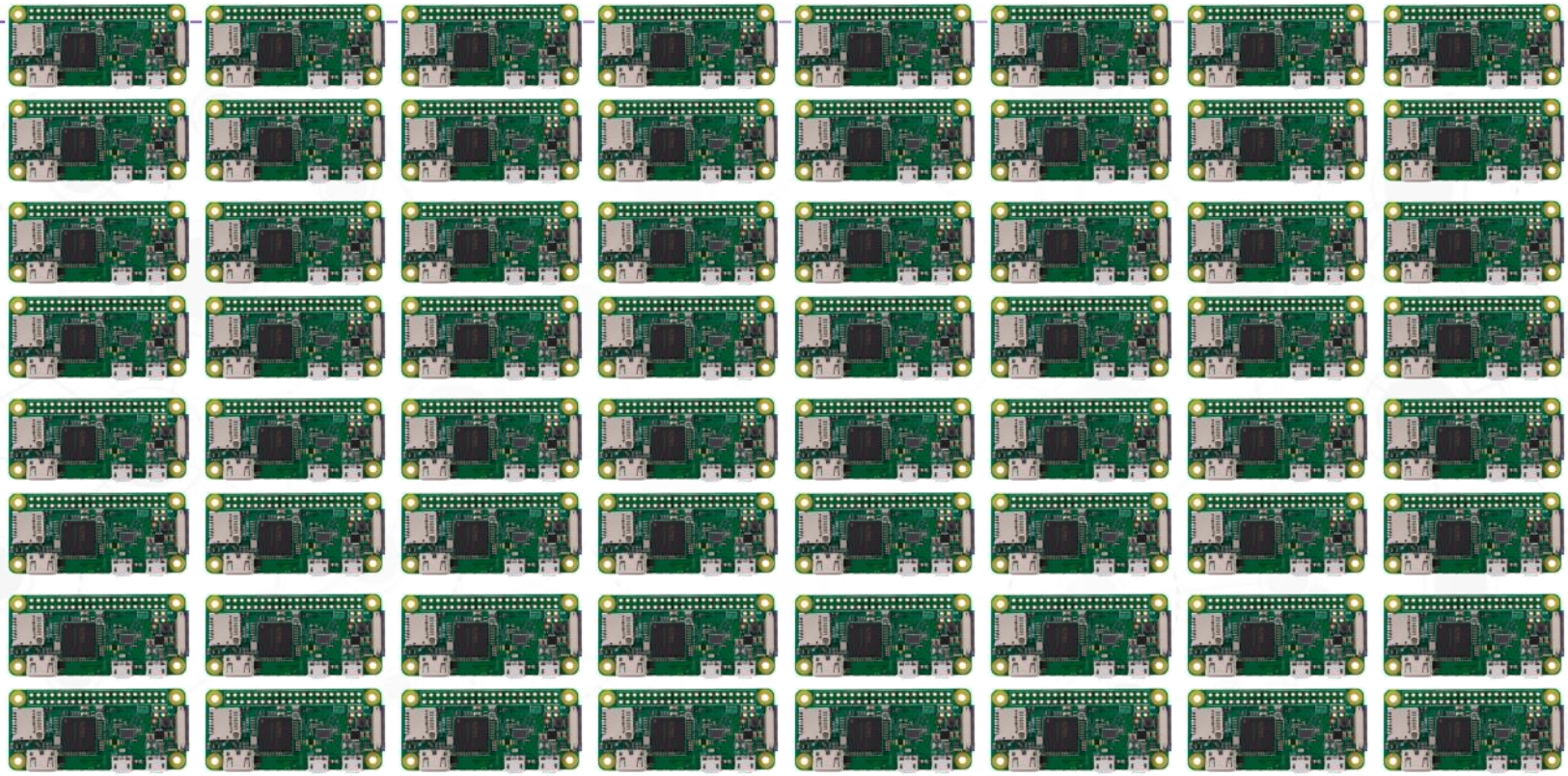
ML-усиленное определение аномалий (IoT)

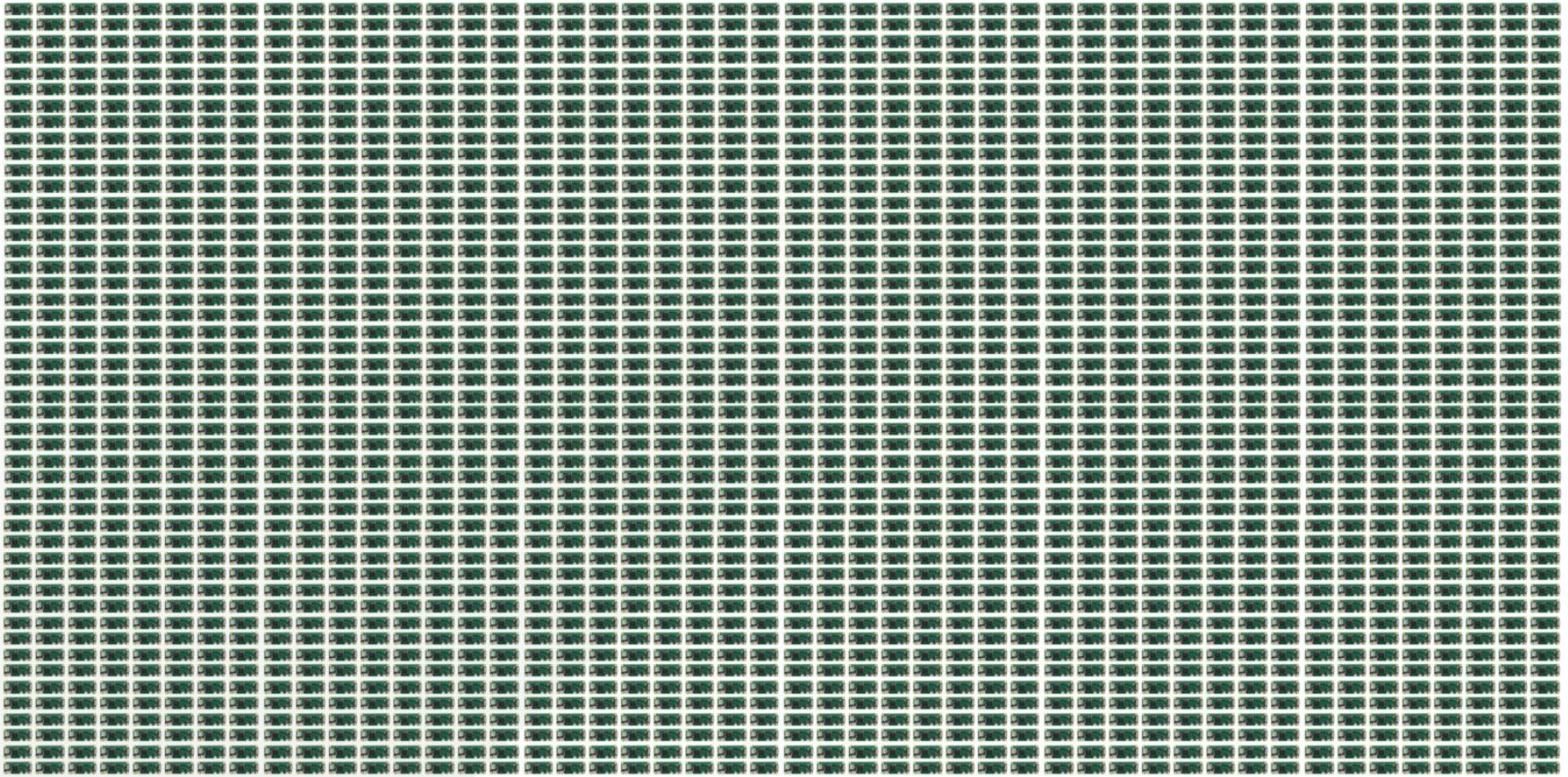
Под капотом Extreme Security Analytics

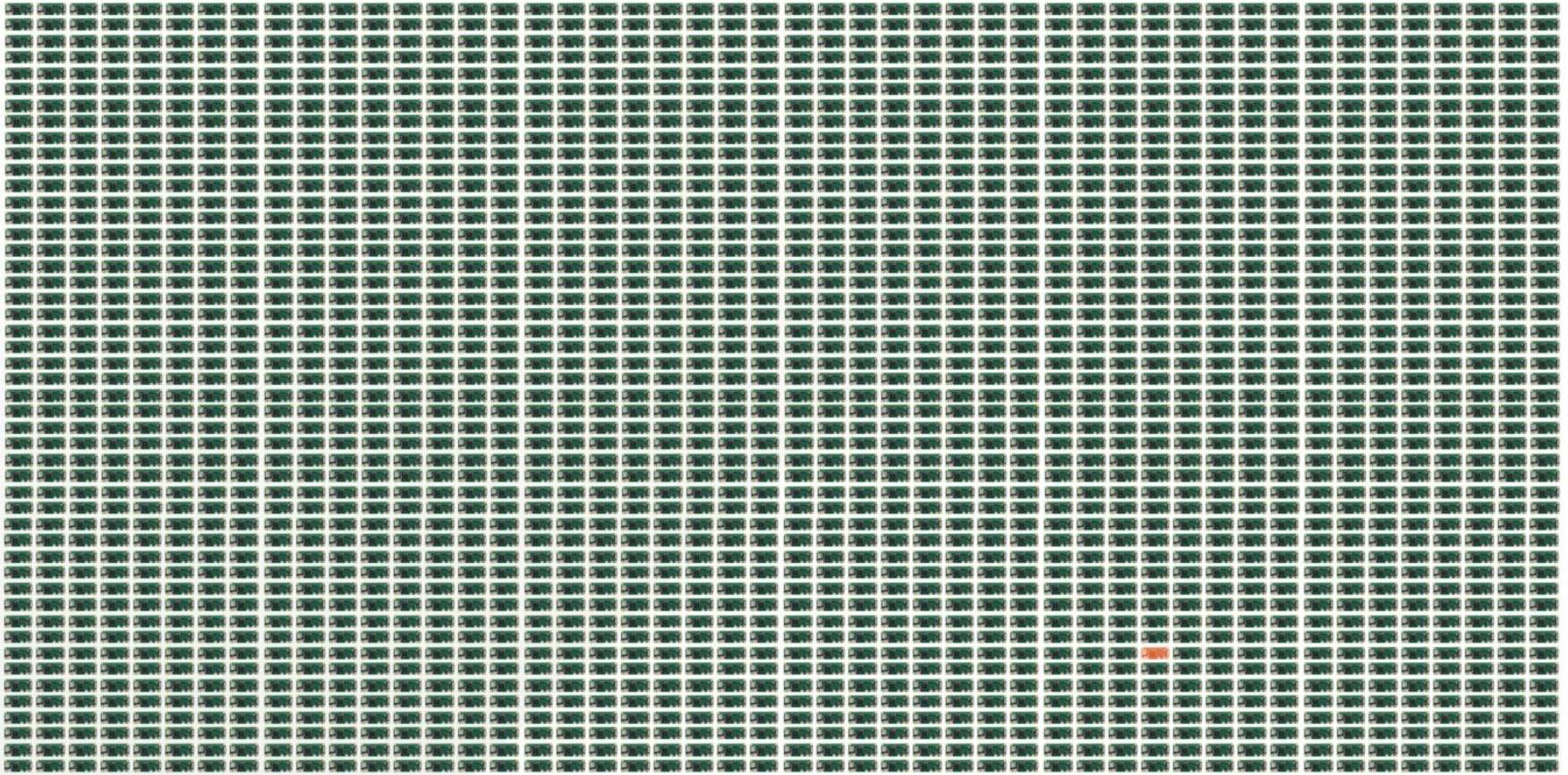


```
12:30:00 - 260B sent - 260B rcvd - NTP - 172.16.0.1:123
12:30:01 - 320B sent - 74B rcvd - HTTPS - iot.example.org:443
12:35:02 - 324B sent - 72B rcvd - HTTPS - iot.example.org:443
12:40:01 - 310B sent - 70B rcvd - HTTPS - iot.example.org:443
12:42:34 - 1KB sent - 1KB rcvd - SNMP - 172.32.0.5:161
12:45:02 - 324B sent - 90B rcvd - HTTPS - iot.example.org:443
12:50:02 - 330B sent - 70B rcvd - HTTPS - iot.example.org:443
12:55:03 - 310B sent - 80B rcvd - HTTPS - iot.example.org:443
12:00:00 - 260B sent - 260B rcvd - NTP - 172.16.0.1:123
12:00:01 - 308B sent - 84B rcvd - HTTPS - iot.example.org:443
12:03:12 - 1KB sent - 1KB rcvd - SNMP - 172.32.0.5:161
12:05:02 - 330B sent - 85B rcvd - HTTPS - iot.example.org:443
```









Поведенческое моделирование с нулевой площадью

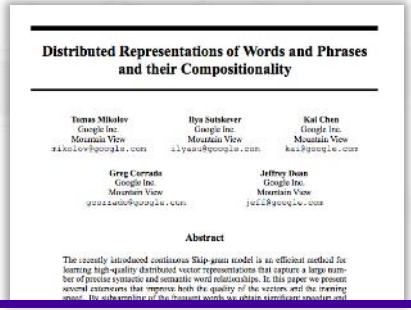
Online-learning

1. БЕЗ огромных хранилищ потоков и метаданных
2. БЕЗ технических, операционных, финансовых и юридических сложностей
3. БЕЗ «чувствительных» данных (но если хотите..)

Наше вдохновение: распознавание естественной речи

“You shall know a word by the company it keeps”

John Rupert Firth (1957)



Distributed Representations of Words and Phrases and their Compositionality

Tomas Mikolov
Google Inc.
Mountain View
tmikolov@google.com

Ilya Sutskever
Google Inc.
Mountain View
ilyasu@google.com

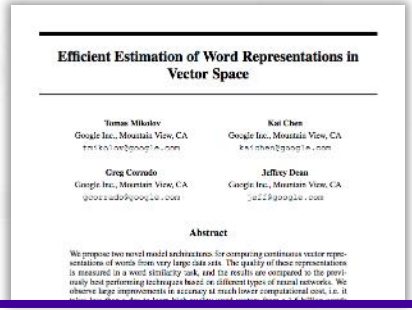
Kai Chen
Google Inc.
Mountain View
kai@google.com

Greg Corrado
Google Inc.
Mountain View
gcorrado@google.com

Jeffrey Dean
Google Inc.
Mountain View
jeff@google.com

Abstract

The recently introduced continuous Skip-gram model is an efficient method for learning high-quality distributed vector representations that capture a large number of precise syntactic and semantic word relationships. In this paper we present several extensions that improve both the quality of the vectors and the training speed. By subsampling of the frequent words we obtain significant speedup and



Efficient Estimation of Word Representations in Vector Space

Tomas Mikolov
Google Inc., Mountain View, CA
tmikolov@google.com

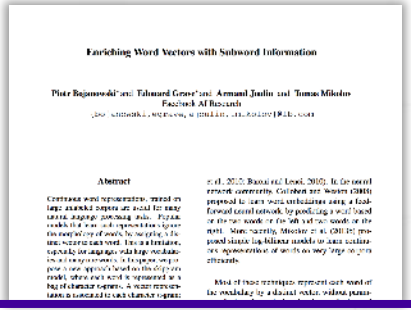
Kai Chen
Google Inc., Mountain View, CA
kaichen@google.com

Greg Corrado
Google Inc., Mountain View, CA
gcorrado@google.com

Jeffrey Dean
Google Inc., Mountain View, CA
jeff@google.com

Abstract

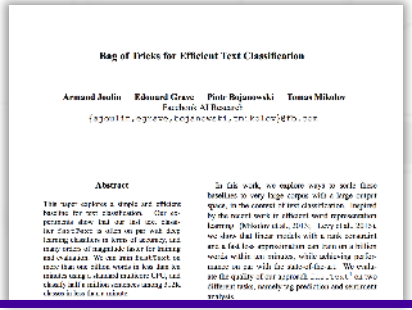
We propose two novel model architectures for computing continuous vector representations of words from very large data sets. The quality of these representations is measured in a word similarity task, and the results are compared to the previously best performing techniques based on different types of neural networks. We observe large improvements in accuracy at much lower computational cost, i.e. it



Enriching Word Vectors with Subword Information

Piotr Bojanowski* and Edouard Grave* and Armand Joulin and Tomas Mikolov
Facebook AI Research

Abstract

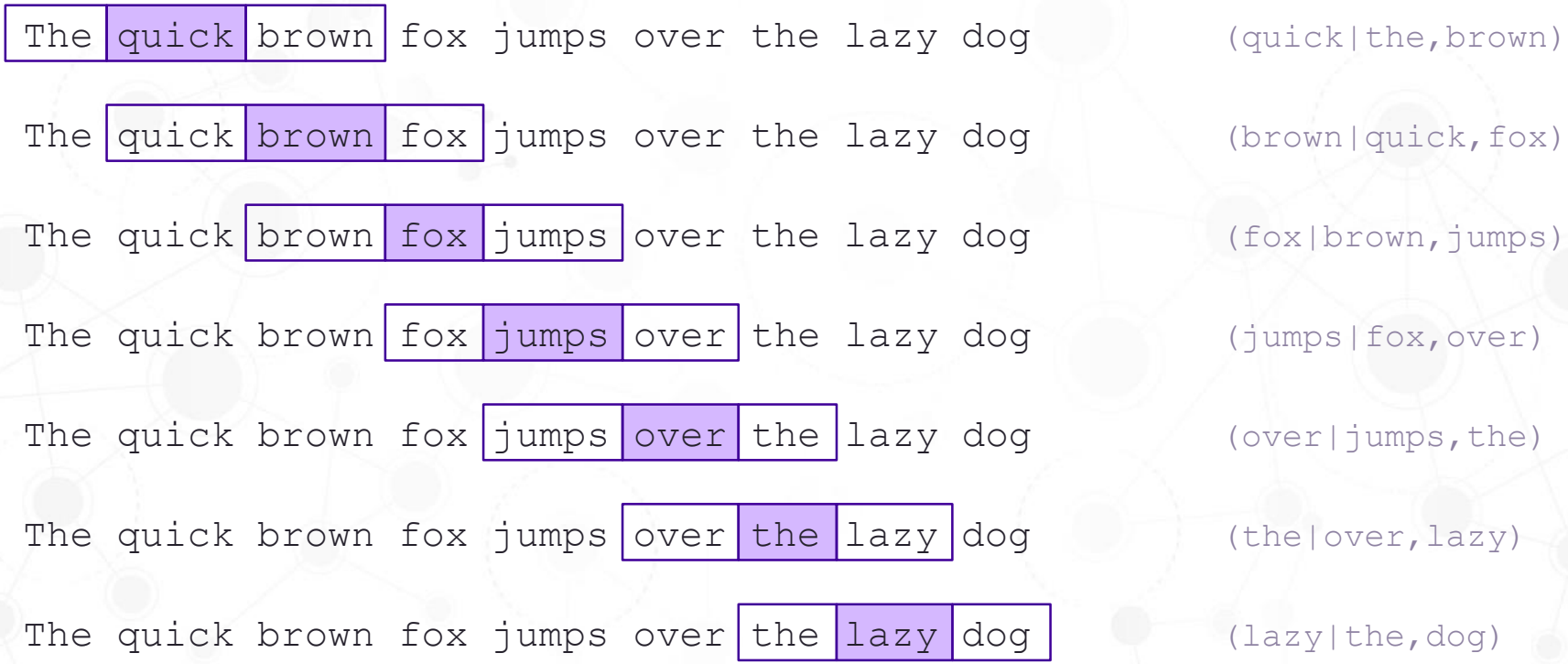


Bag of Tricks for Efficient Text Classification

Armand Joulin Edouard Grave Piotr Bojanowski Tomas Mikolov
Facebook AI Research

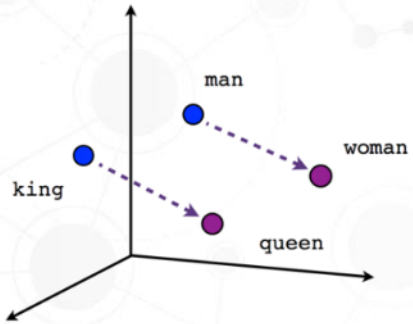
Abstract

The quick brown fox jumps over the lazy dog

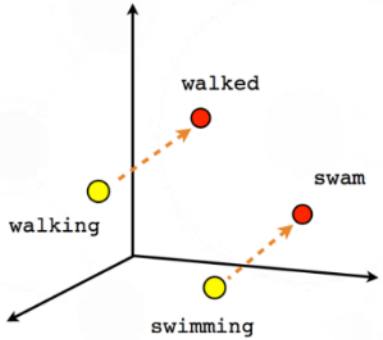


```
the   = [-0.102, -0.229,  1.075, ..., -0.716,  0.604,  0.566]
quick = [-0.298, -0.059, -0.077, ..., -0.010, -0.405,  0.610]
brown = [ 0.601, -1.198, -0.376, ..., -1.035, -2.240, -0.505]
fox   = [-0.301, -0.891, -0.187, ...,  1.193, -1.315,  2.083]
jumps = [ 0.737,  0.070,  0.887, ...,  1.674,  0.271,  0.551]
over  = [-1.068, -0.177, -1.622, ...,  1.270,  0.775, -0.580]
lazy  = [-0.814,  1.358,  0.745, ..., -0.227, -0.366,  0.403]
dog   = [-0.379,  0.550, -0.350, ..., -1.228,  0.386, -0.672]
```

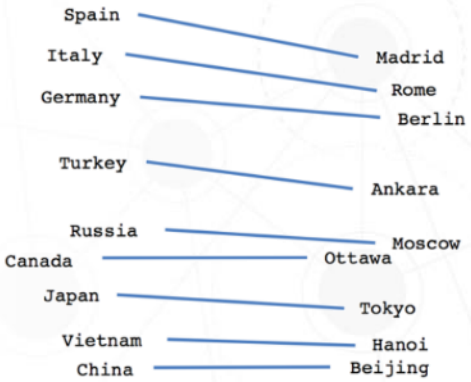
Each word is a **point** in **multi-dimensional space**



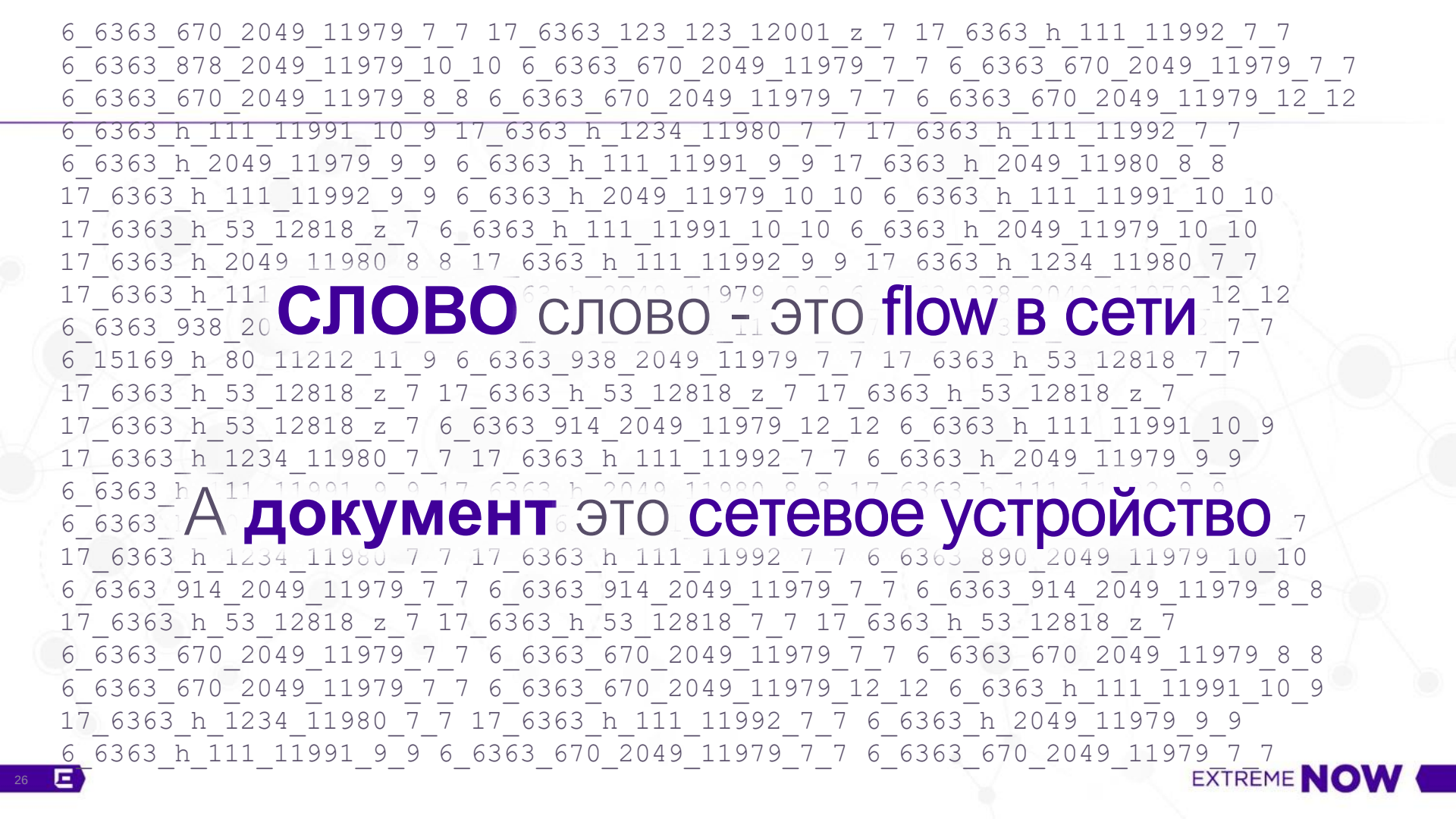
Male-Female



Verb tense



Country-Capital



СЛОВО слово - это **flow в сети**

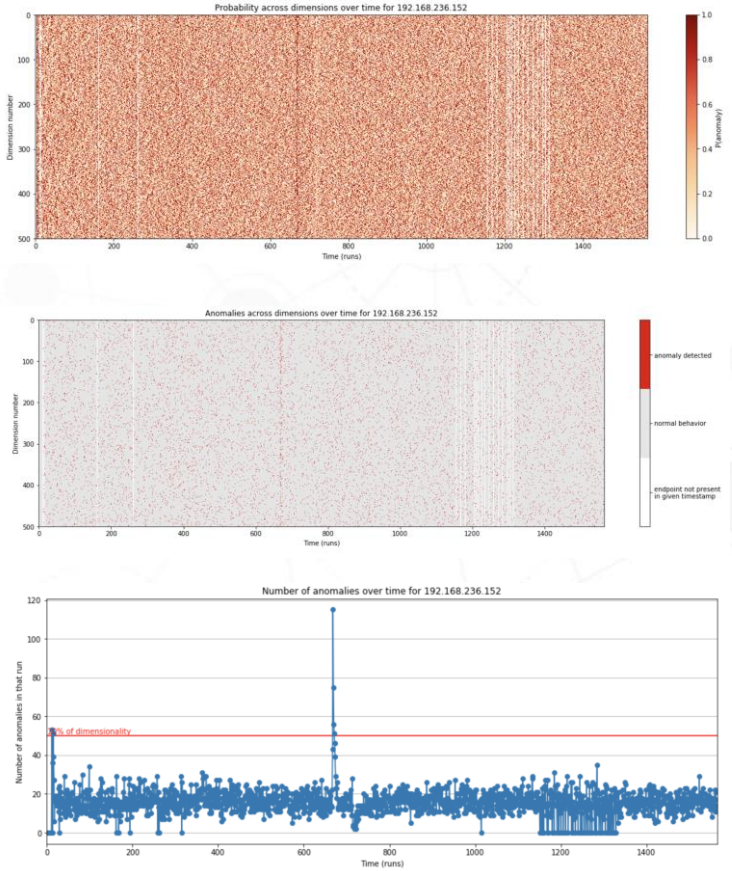
А **документ** это **сетевое устройство**

Определение аномалий с нулевым следом

- Поведение каждого устройства в каждый момент времени **~5KB**
  - **Миллионы** устройств могут быть смоделированы нашими серверами XMC
  - L2-to-L5 flow data, дополненные технологией **Extreme DPI**

- Мы используем вероятностную модель программирования для определения **правдоподобности того, что данное поведение “аномально”**
  - PEWMA (Probabilistic Exponentially Weighted Moving Average) для размещения **многомерного нормального распределения** в пространстве векторов конечных устройств

- Следующая цель - выявление **когнитивных причинно – следственных связей высшего порядка** (аналогия, случайность, соответствие, etc.) для ИТ и ИБ аналитики



EXTREME NOW

Демонстрация

Несколько слов об AI

AI for cybersecurity is a hot new thing – and a dangerous gamble

- We don’t have artificial intelligence (yet)
- Algorithms are getting ‘smarter’, but experts are more
- Stop throwing algorithms on the wall – they are not spaghetti
- Understand your data and your algorithms
- Invest in people who know security (and have experience
- Build systems that capture “expert knowledge”
- Think out of the box, history is bad for innovation but good for insight
- Focus on advancing insights

Raffael Marty’s findings
BlackHat 2018


EXTREME
NOW
WORLD TOUR