КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Как подготовиться к попыткам взлома

Зимарев Павел
Контур

СКБ Контур

SaaS
Software for Business

Клиентов: 2 млн.
Штат: 8’500 чел.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

контур.экстерн

Отчетность в контролирующие органы

контур.фокус

Проверка контрагентов

контур.эльба

Электронный бухгалтер

Защита web-приложения

- DDoS

- Уязвимости
  - Pentest (Red Team) / Аудит / BugBounty
  - Инструменты
    - Пассивный скан реплики трафика
    - Активный скан на этапе тестирования

- Ошибки в логике

- Аутентификация / Авторизация
  - Соц. инженерия
  - Базы логинов и паролей
  - Перебор по словарям
  - SSO


Outlook Web App

Что происходит?

Мониторинг логов 5	• Логи мониторятся в близком к реальному времени
Обзор логов 4	• Логи собираются и анализируются ежедневно
Отчетность по логам 3	• Логи собираются и анализируются ежемесячно
Расследование логов 2	• Логи собираются, но изучаются только в случае инцидента
Сбор логов 1	• Логи собираются, хранятся, но не анализируются
Игнорирование логов 0	• Логи не собираются

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

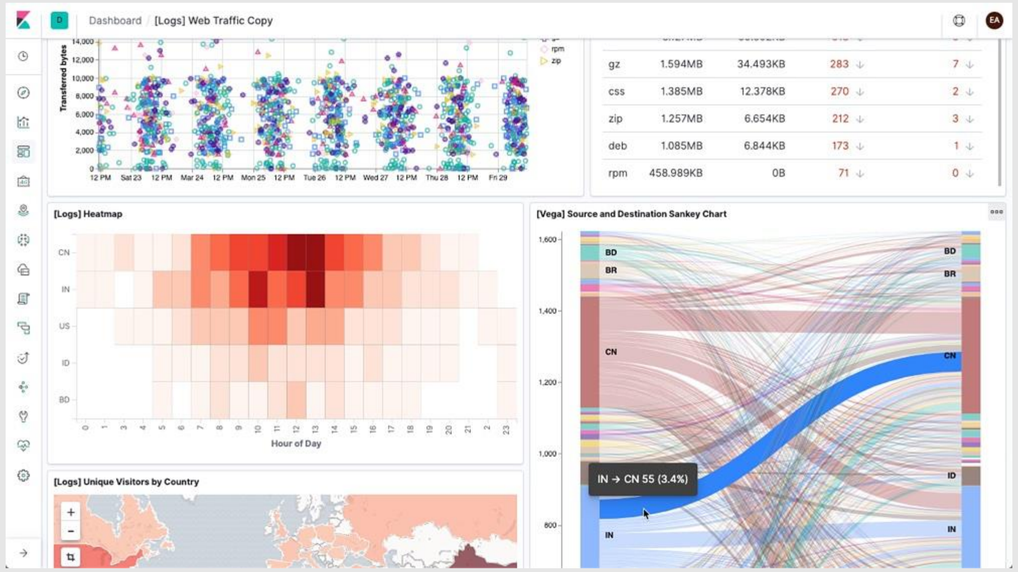
Как хранить?

Как анализировать?

- Текстовые файлики

- СУБД

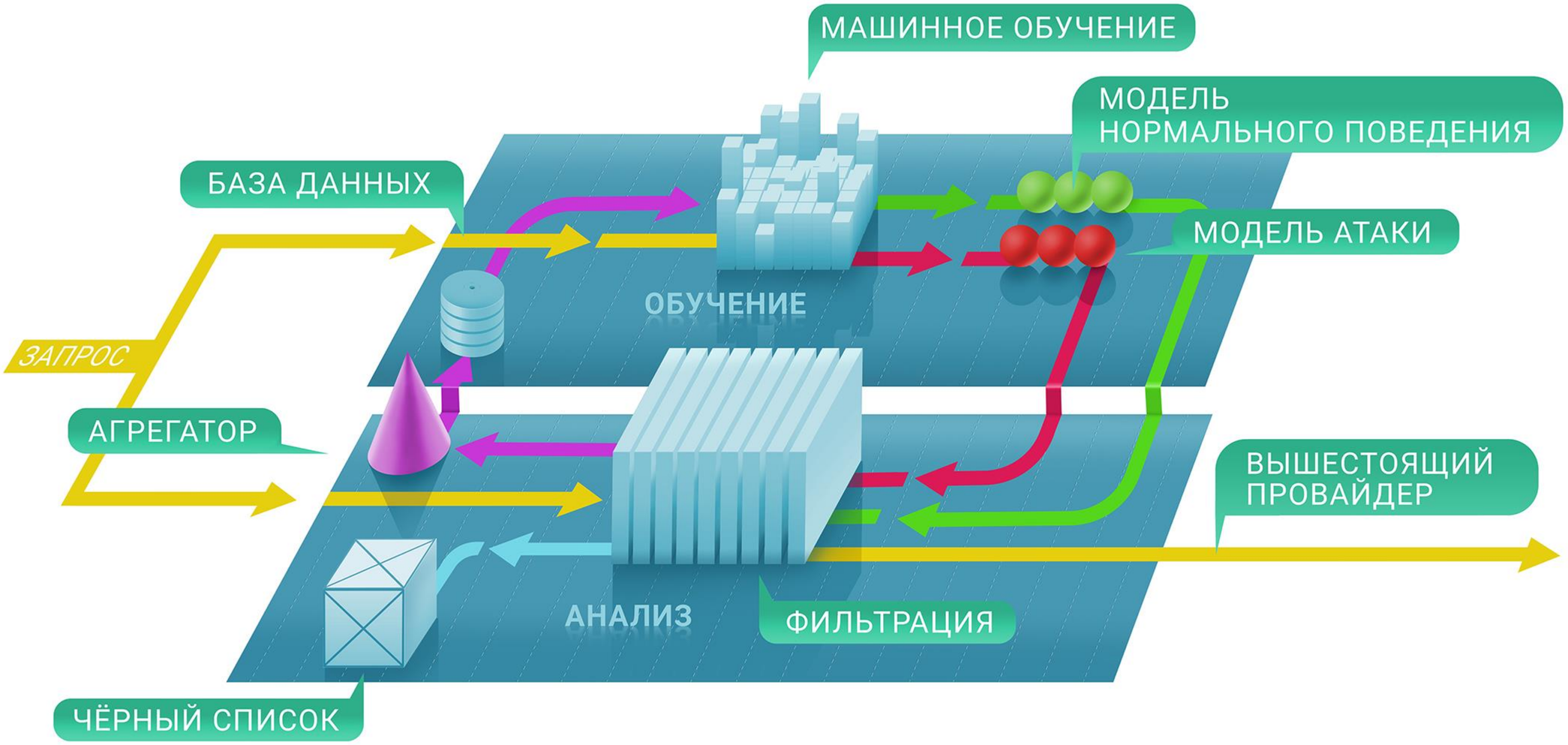
- ELK
  - Elastic
  - Logstash
  - Kibana



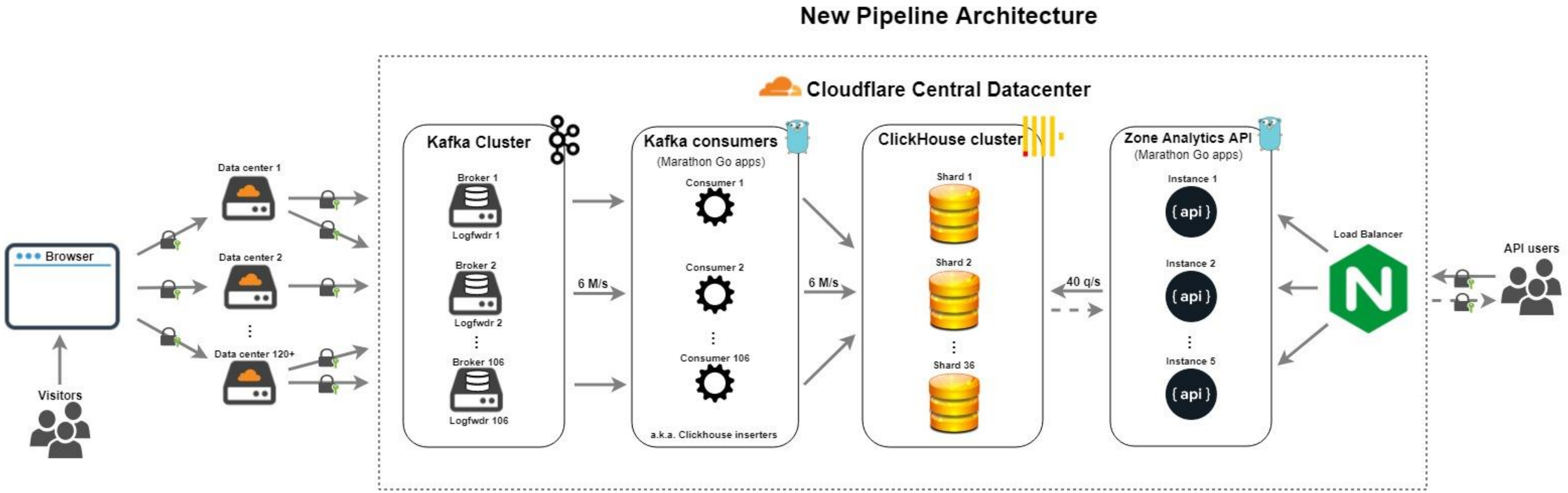
- Yandex.ClickHouse

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Qrator
ClickHouse в нейтрализации DDoS



Cloudflare
Http Analysis Pipeline



```
1  select UserName, UserAgent
2  from       exchange_logs
3  prewhere Date between '201
4      and HttpStatus = 200
5      and ClientIp not like
6      and ClientIp not like
7  where UserName = 'zimarev'
8  group by UserName, UserAge
9  order by maxDate desc
10 limit 100
```

RUN ALL ⇧ + ⌘ + ⏎

11:44:56

TABLE DRAW PIVO

	UserName	Use
1	zimarev	outlook-ios-android/
2	zimarev	msrpc
3	zimarev	microsoft+office/16.
4	zimarev	oc/16.0.4471.1000+(s
5	zimarev	microsoft+bits/7.8
6	zimarev	oc/16.0.4456.1001+(s
7	zimarev	microsoft+office/16.

(ClientIp)

99,595 rows.| 14 GB

groupUniqArray(Clie
52.33.212.52
195.[redacted]
195.[redacted]
195.[redacted]
195.[redacted]
195.[redacted]
195.[redacted]

52.33.212.52

Информация об IP

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2019, American Registry for Internet Numbers, Ltd.
#
NetRange:       52.32.0.0 - 52.63.255.255
CIDR:           52.32.0.0/11
NetName:        AT-88-Z
NetHandle:      NET-52-32-0-0-1
Parent:         NET52 (NET-52-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Amazon Technologies Inc. (AT-88-Z)
RegDate:        2015-09-02
Updated:        2015-09-02
Ref:            https://rdap.arin.net/registry/ip/52.32.0.0
OrgName:        Amazon Technologies Inc.
OrgId:          AT-88-Z
Address:        410 Terry Ave N.
City:           Seattle
StateProv:      WA
PostalCode:     98109
Country:        US
RegDate:        2011-12-08
Updated:        2017-01-28
```

И что теперь?

- Это повод для разговоров

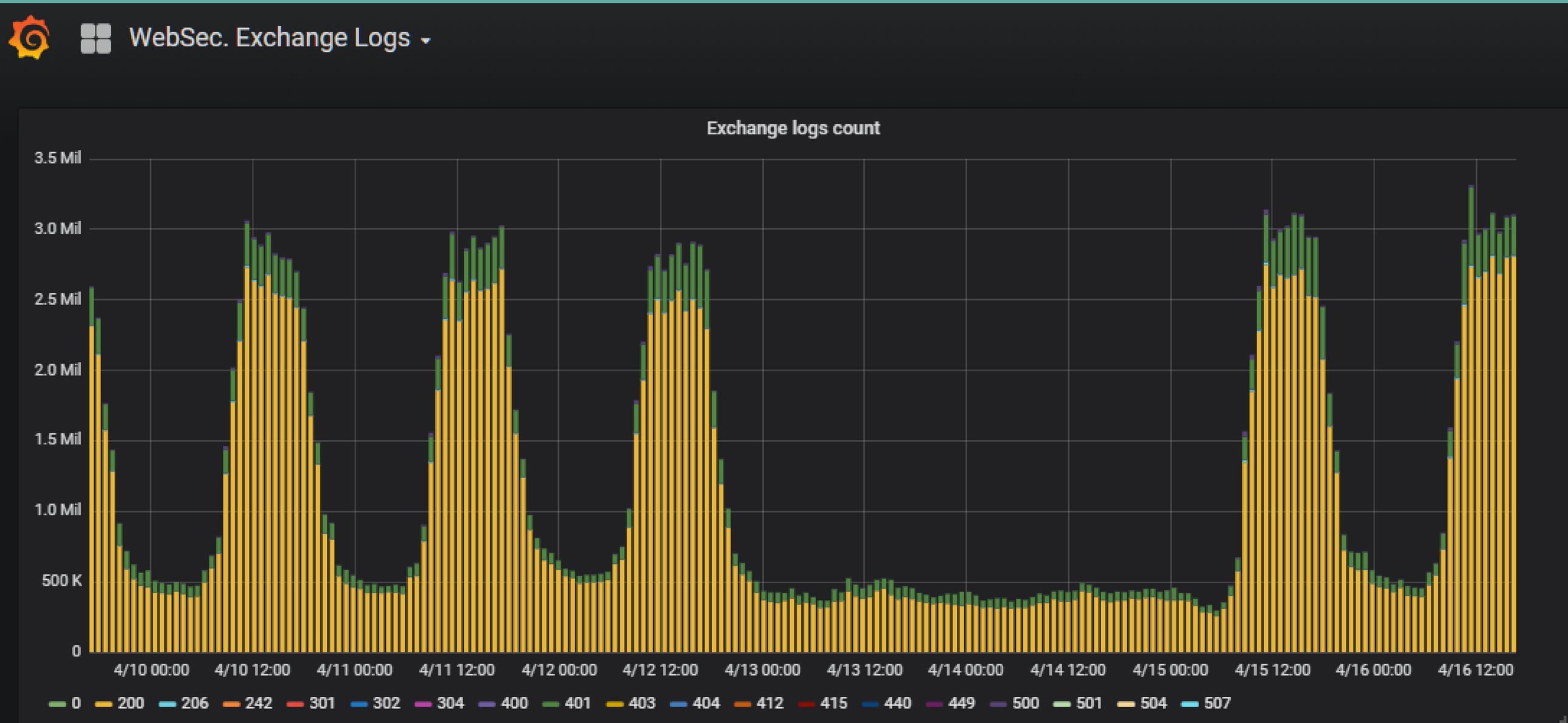
- Посмотреть по сторонам
  - Что в мире?
  - Что в отрасли?
  - Что в компании?

- План мероприятий

- Инструменты

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Grafana


WebSec. Exchange Logs
Exchange logs count
3.5 Mil
3.0 Mil
2.5 Mil
2.0 Mil
1.5 Mil
1.0 Mil
500 K
0
4/10 00:00
4/10 12:00
4/11 00:00
4/11 12:00
4/12 00:00
4/12 12:00
4/13 00:00
4/13 12:00
4/14 00:00
4/14 12:00
4/15 00:00
4/15 12:00
4/16 00:00
4/16 12:00
0
200
206
242
301
302
304
400
401
403
404
412
415
440
449
500
501
504
507

Что дальше?

- Мониторинг и оповещения
- Поведенческие эвристики
- Рейтинговые модели
- Корреляции
- Проактивная защита

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

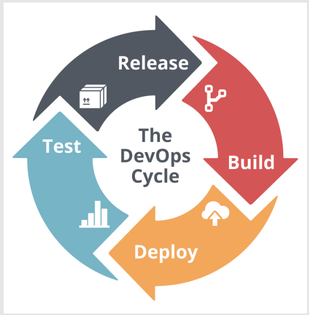
DEMO
Эвристики

Команда

Пентестеры

Разработчики

Аналитики



DevOps

Офицеры безопасности

Менеджеры

NB

Безопасность – это атрибут качества

Учитывайте специфику

Инструменты – не главное

Растите команду

Выстраивайте отношения с коллегами

Формируйте культуру. Это не быстро.

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

zimarev@kontur.ru
+7 912 468 52 98
facebook.com/pavel.zimarev

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ