Redis for Security Data

SecurityScorecard JVM Redis Usage

@PaaSDev

SecurityScorecard, in Brief

Founded in 2013 || Security DNA || Top-notch team of 50 || Top Investors

Executive Team

DR. ALEKSANDR YAMPOLSKIY

CEO & FOUNDER

SAM KASSOUMEH

COO & FOUNDER

ALEXANDER HEID

CRO (R&D)

SCOTT SCHNEIDER

VP Sales

Advisors

RICHARD SEEWALD

BOARD MEMBER

MARTIN GEDALIN

PARTNER LUMIA CAPTAIL

JOAN FEIGENBAUM

PROFESSOR YALE

**ALDO CORTESI**

CEO NULLCUBE

PETER Y. LEE

EVP SALES TIBCO

ALFRED BERKELEY

FMR. PRESIDENT NASDAQ

Investors

SEQUOIA CAPITAL
THE ENTREPRENEURS BEHIND THE ENTREPRENEURS

EVOLUTION EQUITY PARTNERS

boldstart
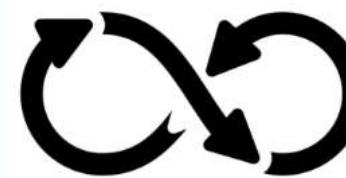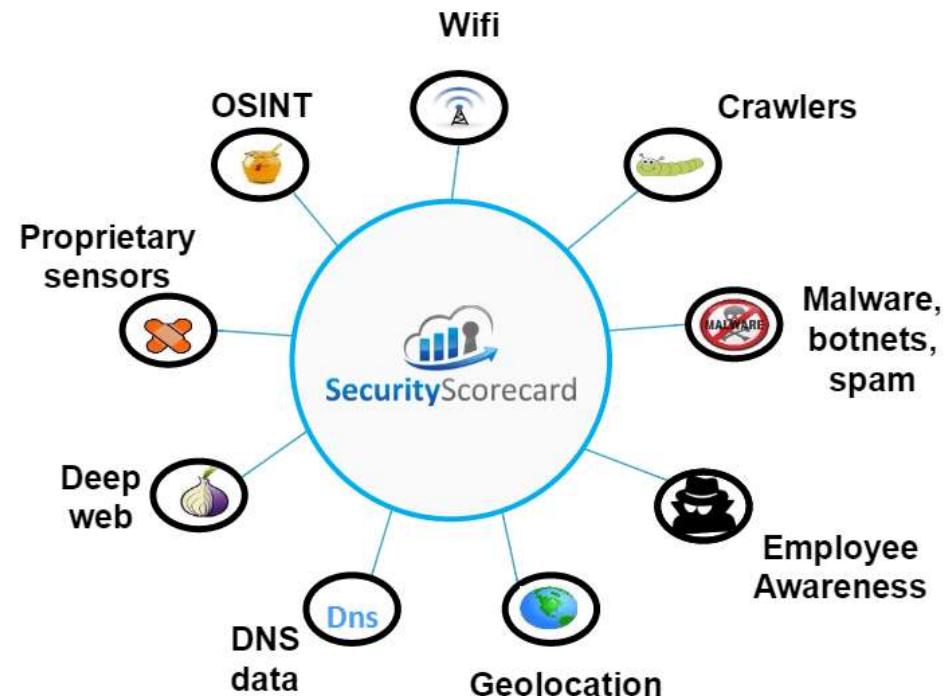
atlasventure

SecurityScorecard can help

UNPARALLELED, NON-INTRUSIVE THREATSCAPE ASSESSMENT
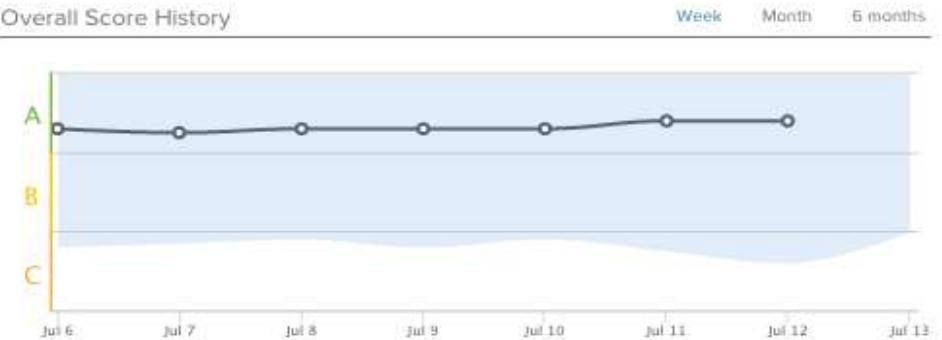
Dashboard for CNN

Overall Score History

Week   Month   6 months

A

B

C

Jul 6   Jul 7   Jul 8   Jul 9   Jul 10   Jul 11   Jul 12   Jul 13

Activity Feed

CNN   Vendors

Palo Alto Networks grade has changed from A to B
Last detected 3 hours ago

The Dana Foundation grade has changed from A to B
Last detected 15 hours ago

Fiorano Software Cubit Score percentile ranking has decreased by 17%, going from 84% to 67%
Last detected 17 hours ago

Fiorano Software grade has changed from A to B
Last detected 17 hours ago

Level 3 Communications Endpoint Security percentile ranking has decreased by 48%, going from 100% to 52%
Last detected 19 hours ago

Level 3 Communications grade has changed from A to B
Last detected 19 hours ago

Experian grade has changed from A to B
Last detected a day ago

Trademarkia Patching Cadence percentile ranking

Malware Events

July 2015

28	29	30	01	02	03	04
05	06	07	08	09	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	01

Top Issues

⚠ Company Emails on Social Networks: 54 social network user logins have been discovered using leaked employee email addresses.
Social Engineering

⚠ Hacker Chatter: The target 'cnn.com' has been mentioned in chatter within underground hacker sites 1 time(s).
Hacker Sites

⚠ Malware Infection Duration: Average malware infection duration is 1.417 days, which is higher than 63% of industry companies.
IP Reputation

Top Movers

		PERCENTILE	CHANGE
A	Sam's Club	97%	+17%
A	Dunkin' Donuts	100%	+17%
A	Navigant	96%	+17%
A	Macys	94%	+17%
A	Sharonregional	95%	+16%

Bottom Movers

		PERCENTILE	CHANGE
B	Bessemer Venture Partners	71%	-18%
B	United Airlines	69%	-16%
A	Sequoia Capital	81%	-12%
B	ViewRay Incorporated	79%	-12%
B	Capital One	69%	-11%

We're Hiring. Why Work Here?

- Well-funded security startup, solving a very big problem in cloud security.
- Patented technology utilized in a new way.
- Medical/dental/etc. benefits.
- Great office space in FlatIron right near subway.
- Flexible hours. Top-notch compensation + stock options.

Open Positions:

- **Front-end Engineer**
- **UI Designer**
- **Data Scientist**
- **DevOps Engineer**
- **Java Developer**
- **Software Engineer**
- **Threat Intel Researcher**
- **VP Engineering**
- **Data Engineer**

Contact us @ info@securityscorecard.io

SecurityScorecard

Senior Software Engineer @ SecurityScorecard

Former Senior Field Engineer @ Pivotal

15+ years of Java Development

DZone Most Valuable Blogger

BS and MS in Computer Science

https://twitter.com/PaaSDev/

http://www.agilemobiledeveloper.com/

Redis is an open source, flexible data store.   It does key-value pairs, but a lot more. You can store lists, hash, sets, hyperloglog, bitmaps and sorted sets. This leads to a lot of practice purposes like caching, counters, analytics and storing specialized data.

Redis is a NoSQL store that supports incrementing, appending to strings, adding to lists, set operations and more.

Redis is used for caching in Spring, sessions in Spring and for analytics in Spring XD. Redis is used by many of the Internet giants like Twitter.

In order to achieve its outstanding performance, Redis works with an in-memory dataset.

In a shared Redis cluster, every node in the cluster can have multiple shards (Redis servers), each potentially being a slave or a master itself.

We are using **Redis** also with **Scala** with **Akka** and Reactive programming.

SBT: ,"net.debasishg" %% "redisreact" % "0.7"

https://github.com/debasishg/scala-redis-nb

```scala
//  Redis Worker Actor
import com.redis.RedisClient
val redis =   RedisClient("localhost", 6379)
val getResult = redis.keys(datasource+":*")
    val res = for {
      r <- getResult.map(x => SecurityToProcess(x, datasource))
    } yield (r)
```

```scala
case GetRedisValue(key) => {
    log.debug("redis retrieving value for key {}", key)
    val getResult = redis.smembers(key)

    getResult match {
      case Some(res) => res.flatMap(_.toList)
      case None => log.error("no result came back key: {}", key)
    }
}
```

Java + Redis

There are many options for working with Java and Redis.   Sitting on top of several different Redis drivers is Spring Data Redis.

Since we use Spring Boot, using Spring Data is a no brainer. It's fast and easy to use.
Code for Spring Data Redis is nearly identical to code for Spring Data JPA (Postgresql) and Spring Data MongoDB.

It's very testable through SpringJUnitRunner and mockable with MockJedis and NoSQLUnit (EmbeddedRedisTest).

```
compile 'org.springframework.data:spring-data-redis:1.5.1.RELEASE'
```

```
@Autowired
 private RedisTemplate<String, String> template;
```

```
redisTemplate.boundListOps(userId).leftPush(url.toExternalForm());
```

Redis is a great NoSQL engine that is simple to run and use and supports more than just Key-Value storage.   It has drivers for every major language.

It can persist data and has more features than Memcache.

We use it for a number of purposes like caching, calculation storage, IP Address lookups, Spring XD analytics and data science applications.

It fits in well with a Lambda architecture and plays well with containers (Docker) and makes a fine storage option for one or more microservices.

For real-time ingest of data from sources like Twitter streams or security data, you can using Spring XD to easily stream it to Redis and tap it to go to multiple places like Postgresql, a message queue, HDFS and more at the same time in parallel.   With no code, using open source.

Spring XD has prewritten sources for: mongodb, postgresql jdbc, files, ftp, sftp, syslog, mail imap4, file tail, kafka, jms, twitter, cron, reactive streams and more.

Spring XD has stores/sinks for file, hdfs, jdbc, kafka, log, mail smtp, mongo, redis, shell, tcp and more.

Streams

This section lists all the stream definitions and provides the ability to deploy/undeploy or destroy streams.

Definitions

Quick filter

Name	Definition	Status ❓	Actions		
demoHTTPG	http | jdbc --tableName=APP.demodata --columns=id,name,value	deployed	☐ Undeploy	▶ Deploy	✖ Destroy
demoHTTPtapG	tap:stream:demoHTTPG > transform --expression=#{'new NameValue(payload)'} | hdfs-dataset --format=parquet --batchSize=250	deployed	☐ Undeploy	▶ Deploy	✖ Destroy
demorabbitG	rabbit --queues=springboot --outputType=text/plain --username=pivotal --password=password --addresses=localhost:5672 | jdbc --tableName=APP.demodata --columns=id,name,value	deployed	☐ Undeploy	▶ Deploy	✖ Destroy
demorabbittapG	tap:stream:demorabbitG > transform --expression=#{'new NameValue(payload)'} | hdfs-dataset --format=parquet --batchSize=250	deployed	☐ Undeploy	▶ Deploy	✖ Destroy

Redis SpringXD Sink

stream create --name demoredis1 --definition "http| **redis --key**=cvStore --**collectionType**=list --**hostname**=localhost --**port**=6379" —deploy

stream create --name demoredis3 --definition "tap:stream:demoredis1 > jdbc --tableName=cvStore" --deploy

stream create --name demoredis4 --definition "tap:stream:demoredis1 > mongodb --databaseName=test --collectionName=cvStore" --deploy
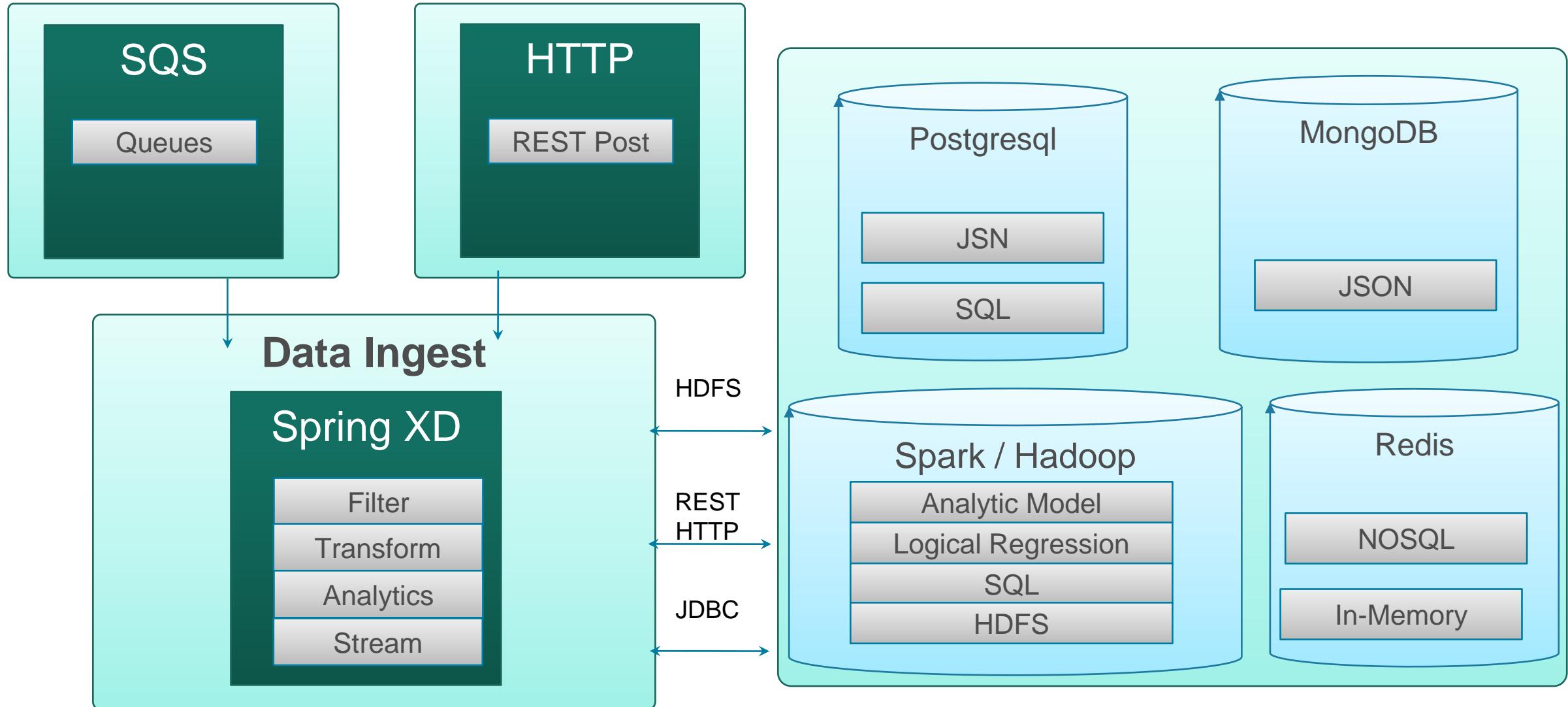
redis-cli

LLEN cvStore
INFO
MONITOR
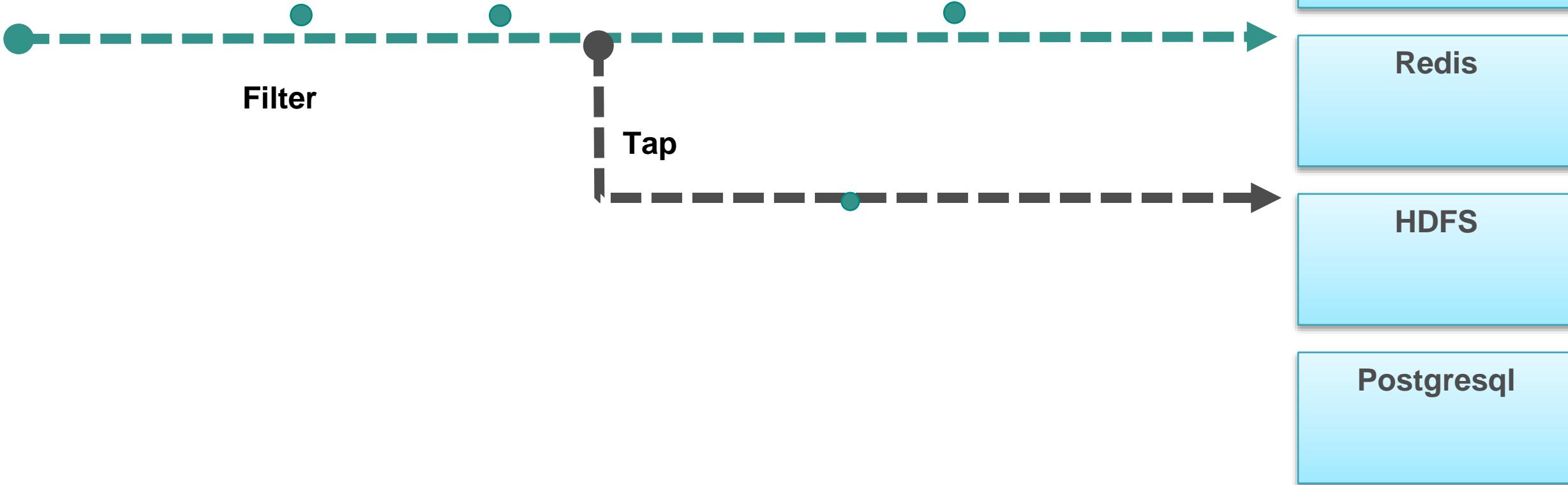
Big Data Workflow

Message Queue

Filter

Tap

MongoDB

Redis

HDFS

Postgresql

Thanks

Salvatore Sanfilippo and Itamar Haber of Redis Labs, Inc.

Matt Stancliff of Pivotal

Aleksandr Yampolskiy of NY Redis Meetup and SecurityScorecard

Mark Shilshtut of SecurityScorecard for Scala assistance

Salvatore Sanfilippo

Salvatore is the author of Redis
and also started as a security researcher.
He is the author of hping.

Links

- http://www.securityscorecard.com/

- http://openmymind.net/2012/1/23/The-Little-Redis-Book/

- http://projects.spring.io/spring-data-redis/

- Using Jedis

- Redis Security Tips

- http://docs.spring.io/spring-data/data-keyvalue/examples/retwisj/current/

- https://www.packtpub.com/books/content/using-redis-hostile-environment-advanced

Links

- ⑩ http://docs.spring.io/spring-xd/docs/current/reference/html/#redis
- ⑩ http://cloudtweaks.com/2015/06/redis-labs-tops-in-independent-nosql-performance-benchmark/
- ⑩ http://www.rediscookbook.org/index.html
- ⑩ https://github.com/50onRed/mock-jedis
- ⑩ https://github.com/knutwalker/rx-redis
- ⑩ http://www.slideshare.net/tobiastrelle/no-sql-testautomation
- ⑩ https://github.com/lordofthejars/nosql-unit

Links

- https://pivotallms.biglms.com/courses/PivotalAcademy/RDS101/VP/about
- https://pivotallms.biglms.com/courses/PivotalAcademy/SDC202/VN/about
- http://www.javacodegeeks.com/2015/03/spring-xd-for-data-ingestion.html
- http://springxd.ninja/2015/03/09/spring-xd-setup/
- http://redis.io/topics/security