How to Use Splunk To Detect and Defeat Fraud, Theft And Abuse

Joe Goldberg

Product Marketing, Splunk

Young Cho

Technical Product Marketing, Splunk

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Personal introduction

- Joe Goldberg
  - 3.5 years at Splunk
  - Product Marketing for anti-fraud/theft/abuse. Also security and compliance
  - Previously Symantec Data Loss Prevention (Vontu)

- Young Cho
  - 2 years at Splunk
  - Technical Product Marketing for anti-fraud/theft/abuse. Also security and compliance. Formerly Solutions Architect in APAC for 1.5 years
  - Previously Splunk Partner in APAC, MOS

Agenda

- Splunk for Fraud, Theft, & Abuse
- Detailed bank fraud use case
- Demo (time permitting)

Splunk for Anti-Fraud, Theft, Abuse (“Fraud”)

splunk>

Why You Should Care: Fraud is Costly

- High annual costs & growing: Merchants $200-250 billion; banks and financial institutions $12-15 billion [1]
- Reputation/brand damage
- Labor costs from manual investigations and review

1. Forrester Feb 2013

Business Moving Online Has Increased Fraud

Data breaches

Lead to downstream identify theft and credit card fraud

No boundaries

Fraudsters are able to act from continents away with impunity

Credential theft

Account takeovers are easier due to phishing and malware

More sophistication

Fraudsters use new tactics and change behavior to evade detection

Machine Data Contains Critical Fraud Insights

Sources

Card Payment System

[2013-09-04-14.45.54.608000] proc_source="B24A", tmst_target="2013-09-04-14.45.54.724000", serv_id="ISS", proc_input="MAST", proc_target="B24A Interface_acq="BNET_1", interface_iss="02008", cod_msg="1110", oper_rrn="090448764439", card_id="526430VS350Y2992" oper_amount="000000008000", oper_ currency="978", oper_country="380", term_id="00599307", circuito="", sett_merc="4722", bin_acq="002111", id_merc="329017246168", rcode="003000" action_code="000", approval_code ="H8H766", oper_ mod_input="1", channel="O", flag_dupl="Y", auth_rout_dst="INTFHI93", auth_ rout_id="HISO_AUTH", msg_subst="" ndg="0000000078507391", station_acq="STA-BNET-MI1", acceptor =“ TRAWEL SPA\\MILANO\ 380", tmst_ins="2013-09-04-14.48.56.277466", lpar="B"

Card ID

Amount

Merchant ID

Client ID

Web Proxy

2013-08-09 16:21:38 10.11.36.29 98483 148 TCP_HIT 200 200 0 622 - - OBSERVED GET HTTP/1.1 0 "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; www.neverbeenseenbefore.com InfoPath.1; MS-RTC LM 8; .NET CLR 1.1.4322; .NET CLR 3.0.4506.2152;) User John Doe,"

Source IP

Referring URL

Authentication

20130806041221.000000 Caption=ACME-2975EB\JohnDoe Description=User account Built-in account for administering the computer/domainDo\n ACME-2975EB InstallDate NULLLocalAccount = IP: 10.11.36.20 TrueName=Administrator SID =S-1-5-21-1390067121-920492009-725345543 500SIDType=1 Status=Degradedwmi_ type=UserAccounts

User Name

Source IP

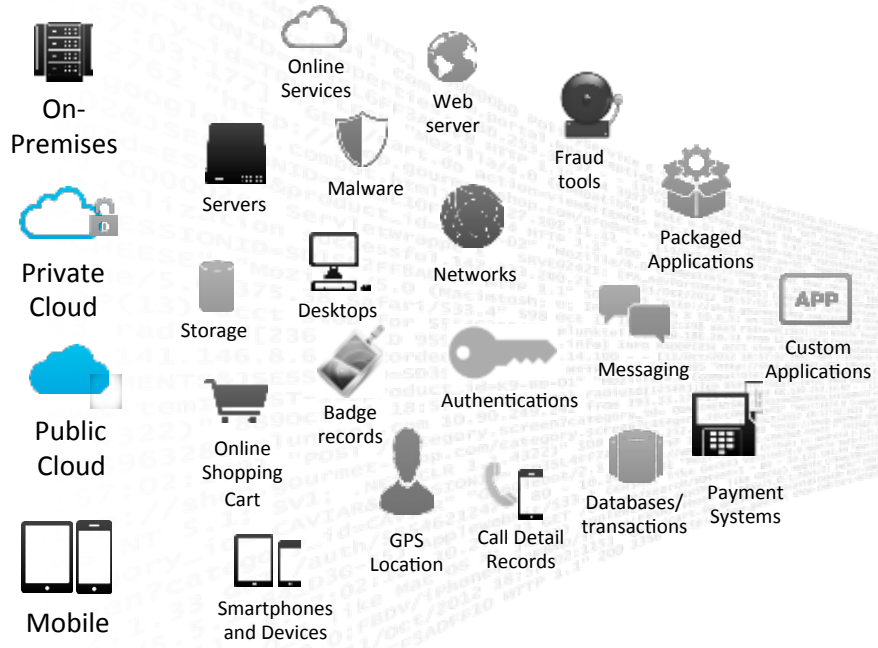
Example Patterns of Fraud in Machine Data

There are Hundreds of Patterns of Internal/External Fraud!

Industry	Type of Fraud	Pattern of fraud
Financial Services	Account takeover	High velocity of transactions under $10k
Healthcare	Physician billing	Physician billing for drugs outside their expertise area
E-tailing	Account takeover	Many accounts accessed from one IP or user agent string
Telecoms	Roaming abuse	Unlimited use customers doing excessive roaming on partner networks
Online education	Student loan fraud	Student IP in “high-risk” country and student absent from classes & assignments

Splunk: Machine Data Platform for Fraud Use Cases

Machine Data: Any Location, Type, Volume

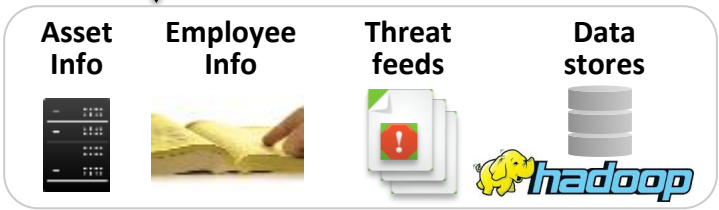


Answer Any Question

splunk>

>enterprise >cloud Hunk

External Lookups



Supports Many Needs of Anti-Fraud Teams

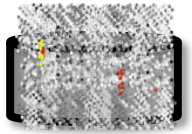
Fraud Monitoring and Detection

Fraud Investigations

Fraud Analytics and Reporting

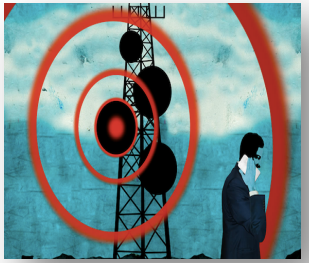
Enhance Existing Fraud Tools

Why Splunk for Fraud Detection?

Existing Fraud Tools		*Splunk for Fraud*
 RIGID AND INFLEXIBLE	→	 FLEXIBLE
 NARROW VIEW OF FRAUD	→	 BROAD VIEW
 SCALE AND SPEED ISSUES	→	 SCALE & SPEED
 DIFFICULT TO DEPLOY; LIMITED ROI	→	 FAST VALUE; COMPELLING ROI

Splunk For Fraud Detection Across Verticals

Financial Services



Mobile/Telecom

eCommerce

Health Care

Online Education

Government

Leading Online Retailer

- **Challenge:** Fraud investigations were too slow with no unified logging
  - Investigation took 12 hours using 10 resources
  - 90 minutes from alert to investigation

- **Enter Splunk:** Big data, flexible platform to accelerate investigations
  - Sample patterns of fraud Splunk looks for:
    - One referrer string or IP logging into multiple user accounts
    - One referrer string or IP creating many new accounts to get account opening incentives OR opening new account to fast to be human
    - Single IP excessively selecting the “I forgot my password” option for several accounts
    - User traffic coming from “rent a VM”, cloud-based services
    - Brute force password guessing
    - Customer info that should be stable changing often: email/physical address, payment card, etc
  - Splunk unites all context around possible fraud on single dashboard
  - Splunk adds together point fraud tool scores to give a consolidated transaction score
  - Many fraud visualizations, including geo-IP mapping
  - Investigation takes 0.2 hours using 2 resources
  - Under 10 minutes from alert to investigation
  - Use Splunk for fraud, security, compliance, IT Ops, and App Mgmt

Top 5 Online University

- **Challenge:** Needed solution to detect fraudulent student loans
  - Difficult to identify fraudulent loans and attendance activity

- **Enter Splunk:** Significant cost savings in reduced loan fraud
  - Cross-check students with loans against classroom activity to identify fraudsters
  - Stopped $10s of millions of fraudulent funds from distribution
  - Reputation and Dept of Education accreditation maintained
  - Single tool for fraud, compliance, cybersecurity, IT Operations, and Classroom Ops

Bank Fraud Use Case

splunk>

Successful Tier 1 Bank Real-Time Wire Blocking Reference

머니투데이 뉴스

정치 정책 증권 금융 산업 IT·과학 중기 부동산 국제 사회 생활문화 연예 스포츠 스페셜 전체

정책 | 은행 | 채권단 | 은행상품 | 생보업계 | 생보상품 | 손보업계 | 손보상품 | 제2금융 | 일반

금융범죄 파수꾼 FDS가 뜬다…도입 이후 탐지율 '급증'

지난 10월 FDS 도입한 하나은행 탐지율 70% 상회

머니투데이 정현수 기자 | 입력 : 2014.12.16 09:02

기사 | 소셜댓글(0) | 가 가

최근 신종금융범죄가 잇따르면서 이상금융거래탐지시스템(FDS) 고도화 작업도 병행되고 있다. 하지만 아직 은행들의 FDS 도입비율은 미미한 상황이다. 그만큼 은행들이 금융범죄 대응에 소홀했다는 방증이다.

하지만 선제적으로 FDS를 도입했던 은행들은 FDS의 효과를 톡톡히 보고 있는 것으로 나타났다. 금융당국까지 나서 시중은행들에 FDS 도입을 강조하고 있는 이유다.

16일 금융권에 따르면 하나은행의 지난달 이상금융거래 탐지율은 71.7%를 기록했다. 전체 이상금융거래 중 70% 이상을 걸러낸다는 의미다. 하나은행이 FDS를 도입한 것은 지난 10월. FDS 도입을 전후해 이상금융거래 탐지율은 두드러지게 향상됐다.

실제로 하나은행의 지난 1월 이상금융거래 탐지율은 24.8%에 그쳤다. 이후 꾸준히 탐지율이 높아졌지만 지난 8월까지만 하더라도 50%를 넘지 못했다. 하지만 FDS 도입을 위한 시범운용에 나선 지난 9월부터 탐지율이 66.8%까지 급증하는 등 성과를 내고 있다.

하나은행은 크게 3가지 유형으로 이상금융거래를 걸러낸다. 원격으로 이뤄지는 금융거래, 평소 아이디 기반으로 로그인을 하다가 갑자기 공인인증서로 로그인하는 경우, 기존 범죄에 악용된 인터넷주소나 컴퓨터 고유식별번호(MAC)로 금융거래가 이뤄지는 경우다.

Based a Korean financial news in 2014 :

(Money Today 2014 12-16)

On the 16th of December 2014, financial community revealed that "**Hana Bank**" (A tier 1 bank in Korea) overall bank's **fraud detection rate has risen** to **71.7%**. It means that Hana Bank were able to block 70% above all bank's fraudulent transactions. Hana Bank has deployed next generation fraud detection last October 2014. After they deployed the next generation fraud detection platform, there were significant increase of fraud detection rate, **originally** from **24.8%** in January of 2014. After Hana Bank started deploying the FDS, their fraud detection rate immediately increase to 66.8, starting from last September.

splunk>

Top Korean Tier 1 Banks, Splunk Based FDS Adoption

Splunk Based Real-time Fraud Adoption Status		
1	W Finance Holdings	✓ Splunk based FDS
2	S Financial Group	Not Decided
3	H Financial Group	✓ Splunk based FDS
4	K Financial Group	Local Competitor
5	I Bank	✓ Splunk based FDS
6	K Bank	Local Competitor
7	E Bank	✓ Splunk based FDS
8	S Bank	✓ Splunk based FDS

Out of eight tier 1 banks, five banks (63%) have selected Splunk as

High Impact Customer Values Created

Various Major Financial Institutions

Detection Rate of a tier 1 Bank

71%

24%

Asset **Blocked** Amount

$X0,000 Daily

Incident Investigation time

Fast Effective

Financial Credibility

Satisfaction

Long term Biz Impact

Rapid Increase

Turning all financial transactions to critical **Intelligence**

Finance Service Industry Needs >

What are some of the technical challenges in managing data?

Ability to process transactions in real-time for detection of fraud

Ability to process large volumes of transactional data for long period of time.

Ability to analyze complex patterns of transactions and be able to profile user objects

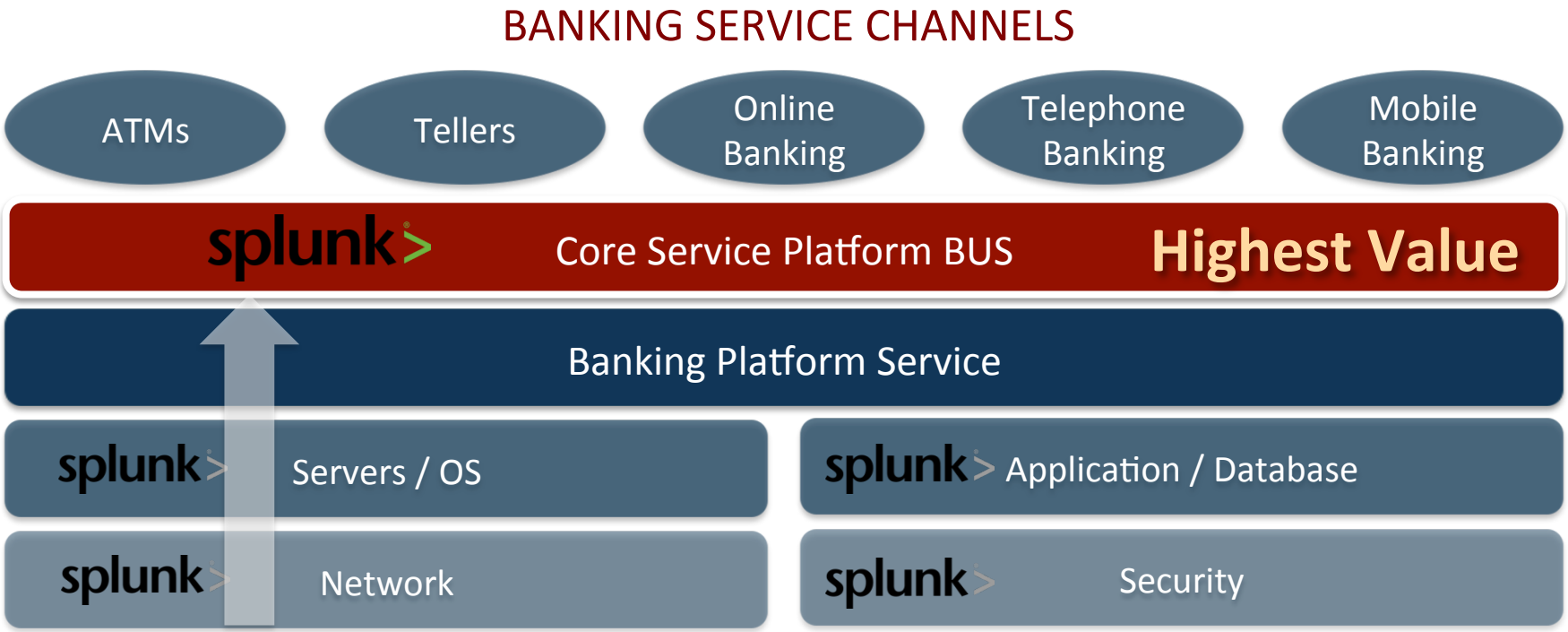
MISSION :

Advanced fraud detection platform that
COLLECT / PROCESS / ANALYZE
Financial transactions in real-time

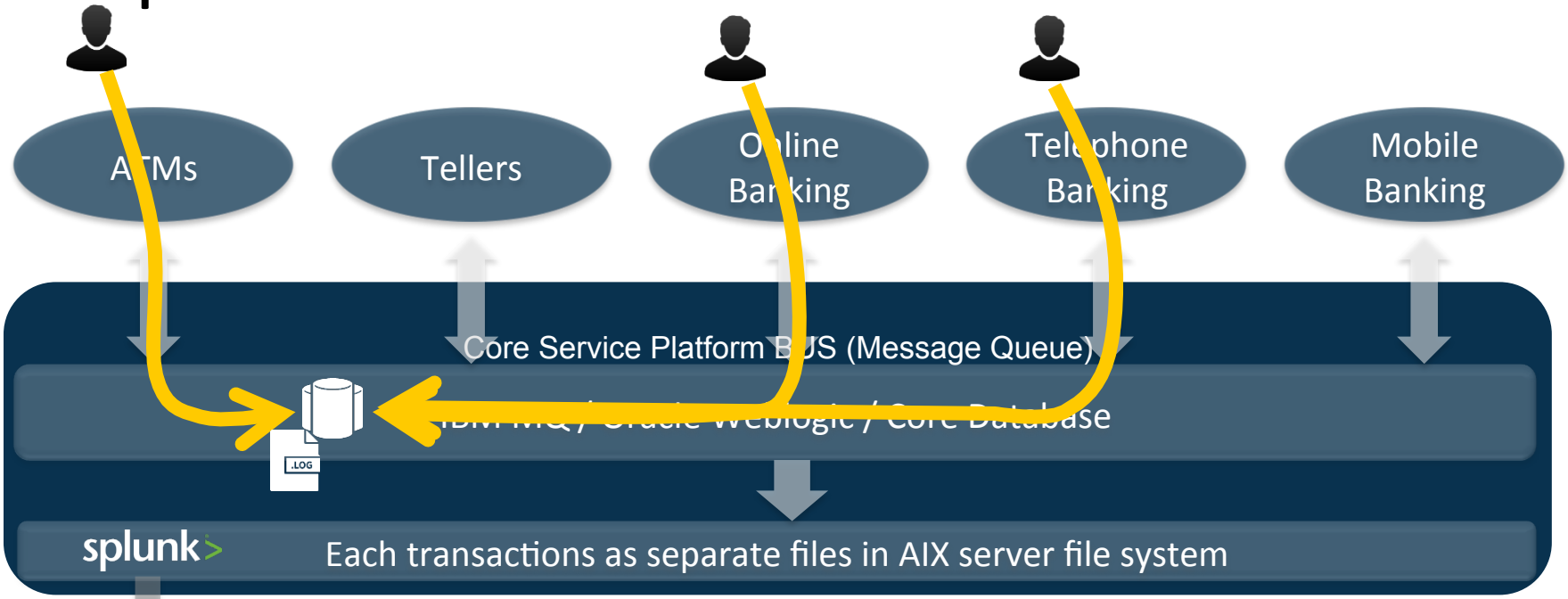
- Sensitive Data
- High Entrance Barrier
- Mission Critical
- Real-time Impact

The Jargon “Channels”

Tier 1 banks offer many different channels to access their services:



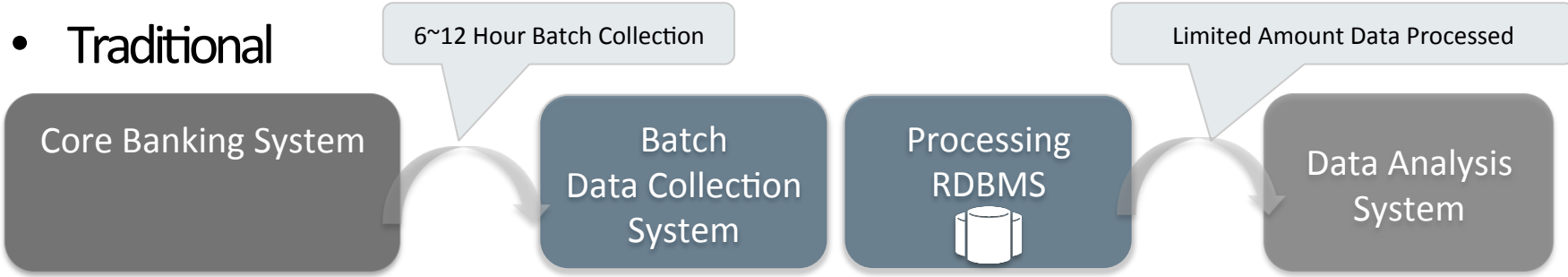
Splunk For Core Financial Transactions



- **Real-time collection** of core banking transactions
- **32,000+ Types** of different transaction formats

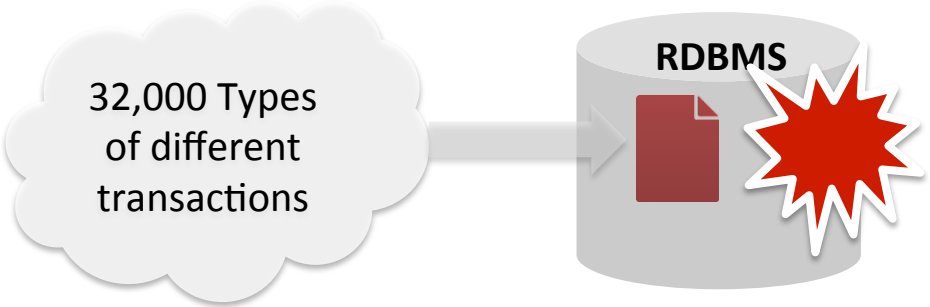
Why Is This Such A Big Deal? Reason 1

- Traditional

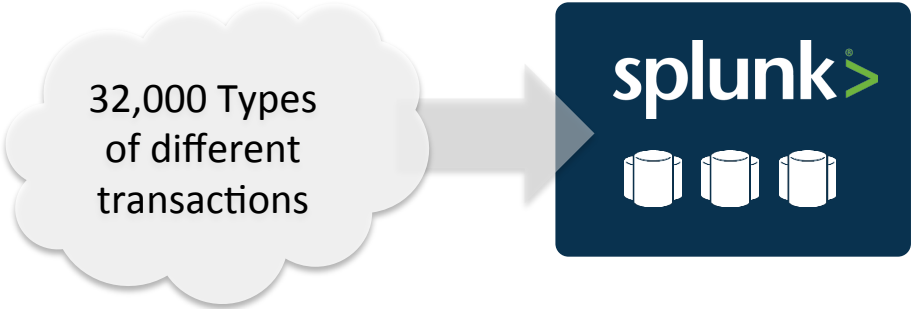


- Splunk

Why Is This Such A Big Deal? Reason 2



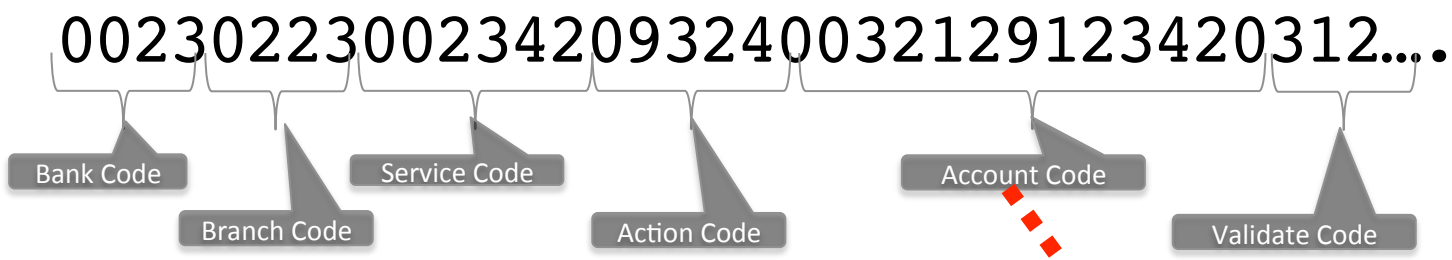
- RDMBS Can't model 32,000 types of different formats
- Because of that, can't query/ search



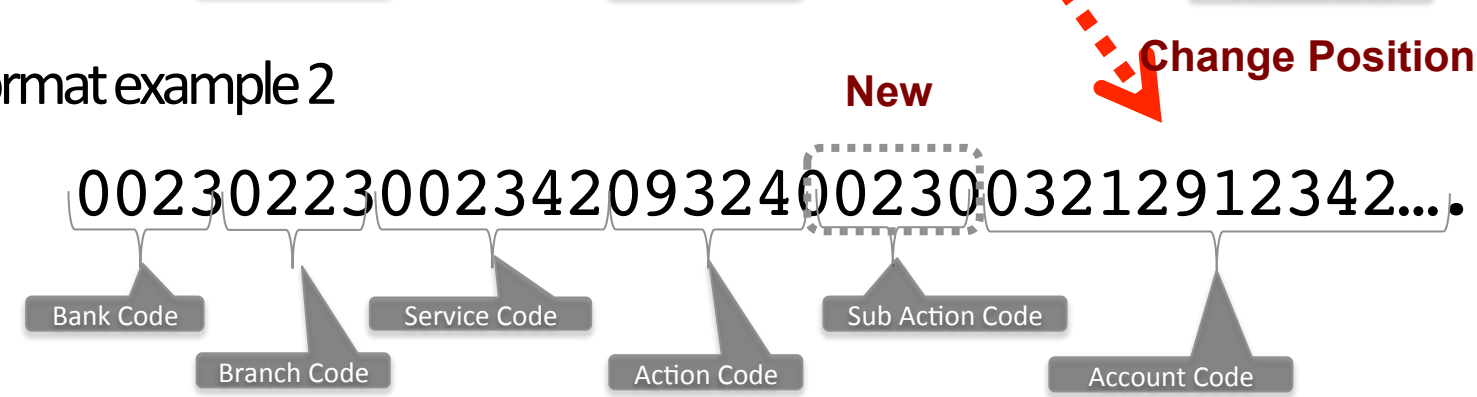
- As a No-SQL database process all 32,000 types
- Able to search all data based on value-pairs matching

How Do Transactions Look Like?

- Format example 1



- Format example 2



❖ 32,000 types of these formats

New Breed Of Bank Robbers

Today's bank robbers know you more than you know yourself….

Your Bank Info

Your Card Info

Your Personal Info

Your Bank Login

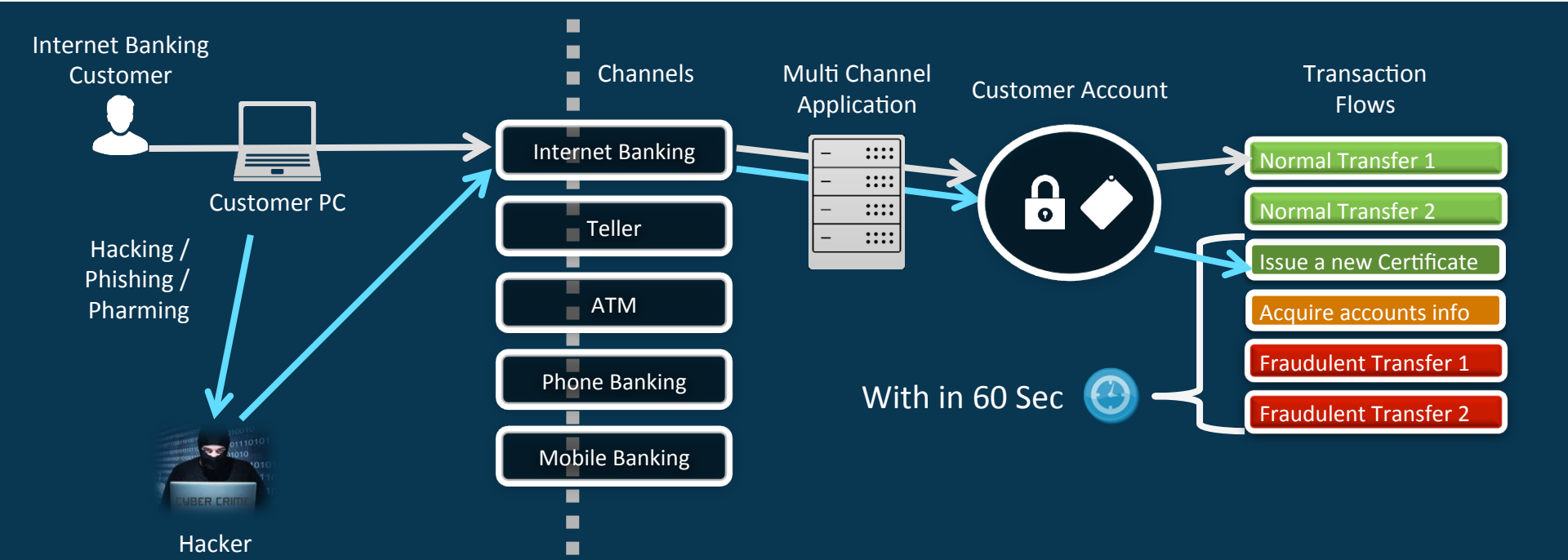
Your Human Network

Your Financials

Your Computer

ALL ABOUT YOU!

Banking Fraud Example : Phase 1



Characteristic Of Financial Fraud And Abuse

Fast

- Knows what to do, fast transfers to a temporary accounts

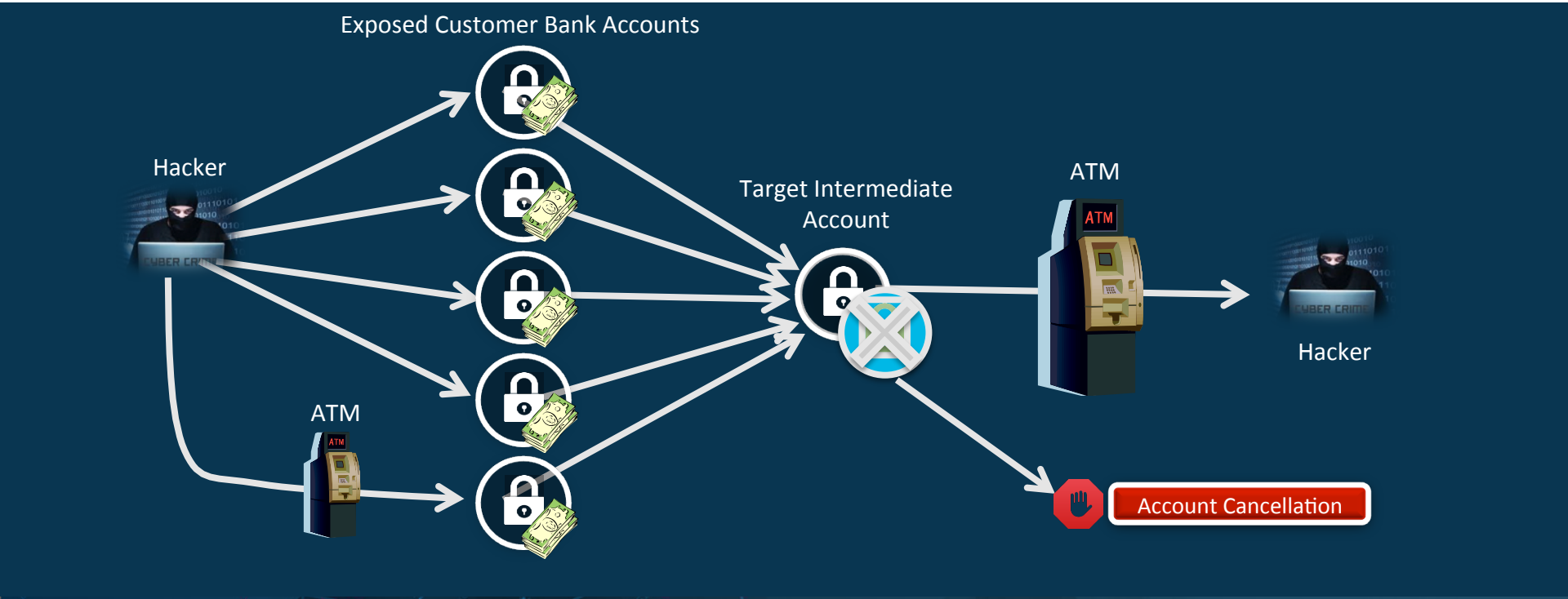
Intelligent

- Highly technical, access the target accounts with proper credentials and certificates

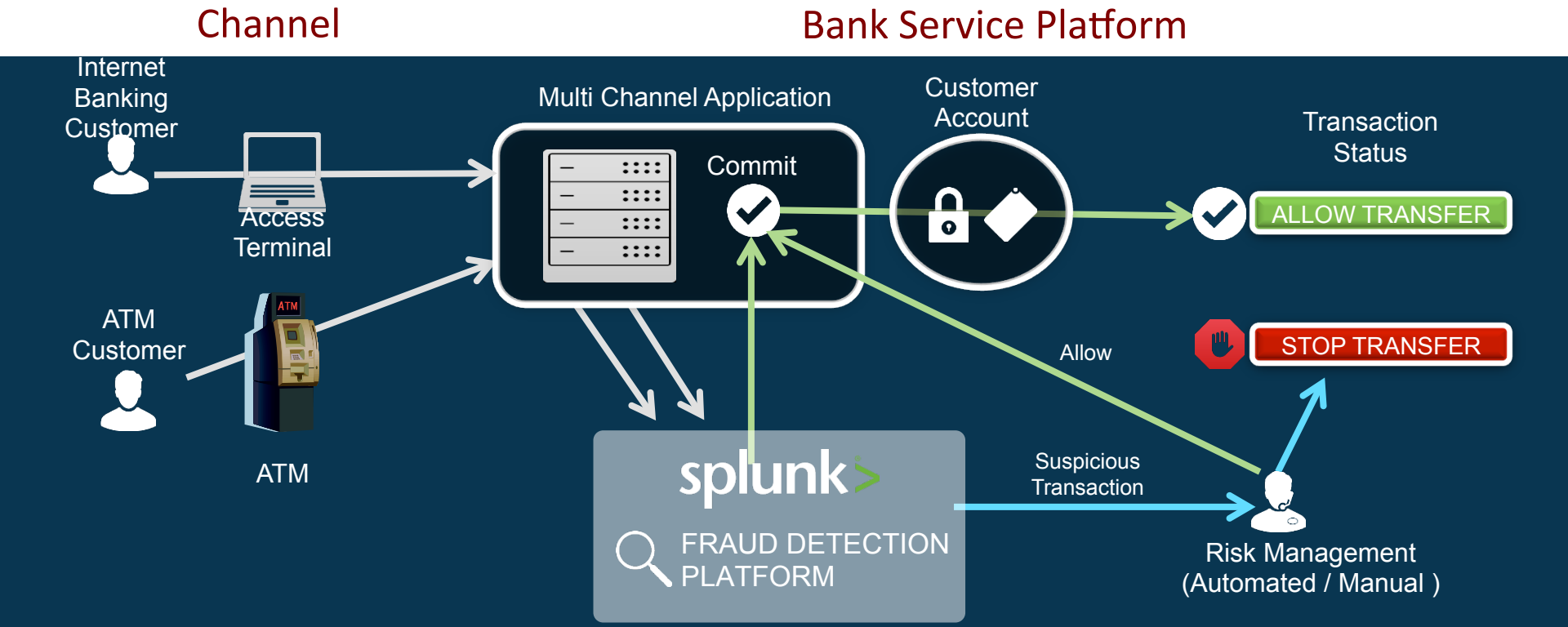
Structured

- Works as in teams for different roles

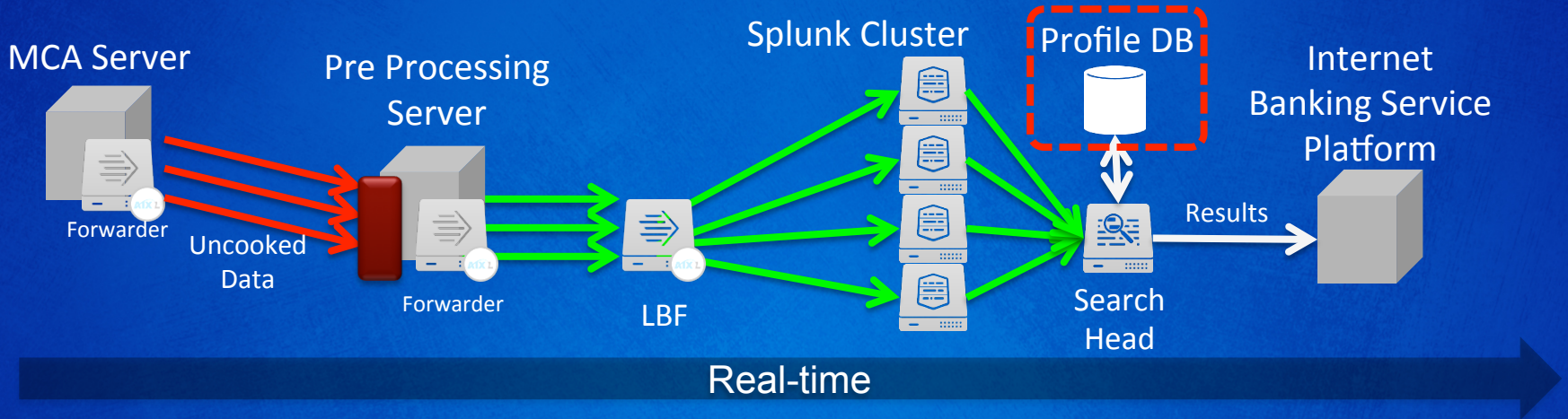
Banking Fraud Example : Phase 2



How Can Fraud Be Stopped?



Success Factor : Real-time



Processing Structure

Real-time collection of raw data send for pre processing	Turning banking format data into Key Value format (Cust Mod)	Splunk Cluster ingests Key Value format data into Indexers	Processing of marts and applying complex Fraud Rules	Results of Fraud detection results send over to Internet banking server	The fraudsters are warned with warning and aborts wire transfer

 |

How Does Splunk Make It Possible?

Online Banking Customer

Hacker

Account Transactions

- Normal Transfer 1
- Normal Transfer 2
- Issue a new Certificate
- Acquire accounts info
- Fraudulent Transfer 1
- Fraudulent Transfer 2

> Fraudulent Patterns / Conditions Combo

1. Different Channel
2. Different MAC Address with no prior history
3. Issue a new certificate
4. Target wire account with no prior history
5. Create new cert and wire transfer happens in 5 minutes

```
Index=multi_access | check_hist_mac mac |  check_hist_wire target_account
```

splunk> FRAUD DETECTION PLATFORM


Real-time Transactions


Account history Summary


MAC history Summary

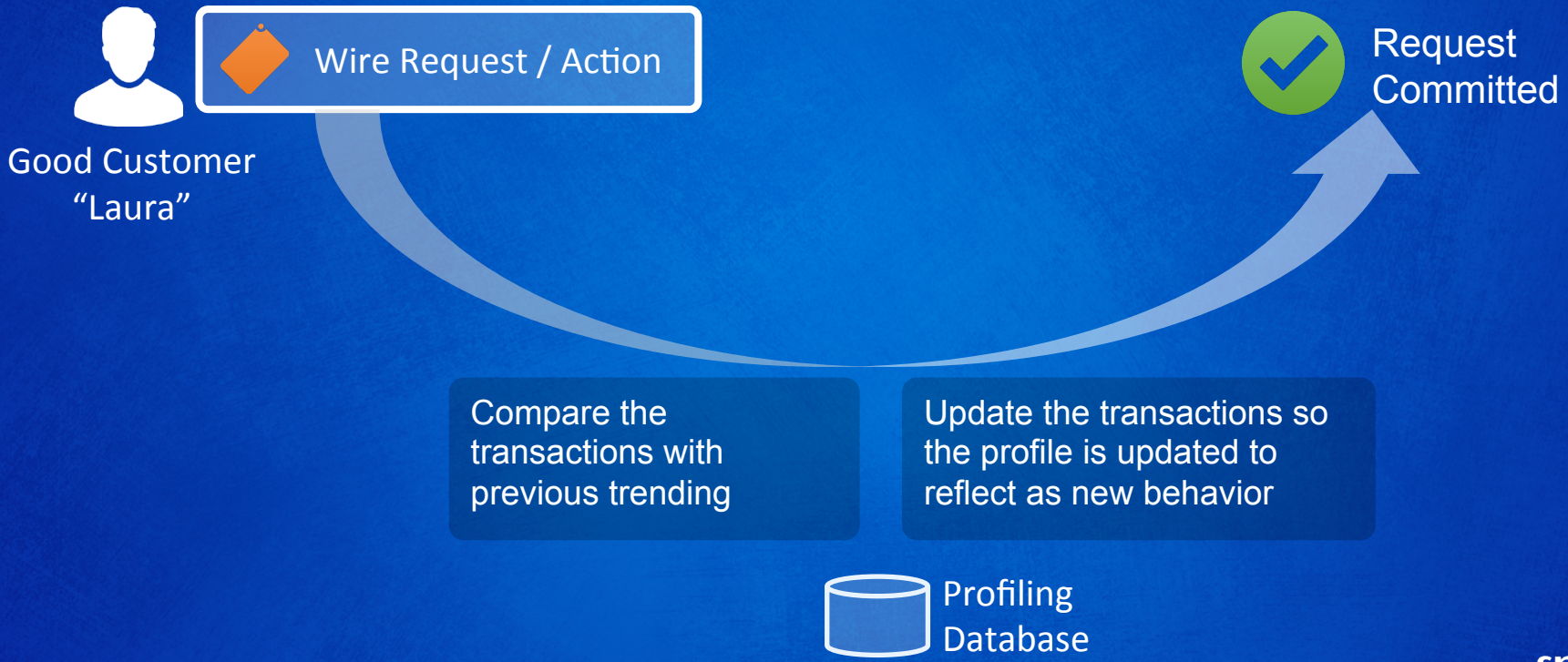

Wire history Summary

 |

splunk>

Concept of “Profiling”

- Extrapolation of information about something, based on known qualities.

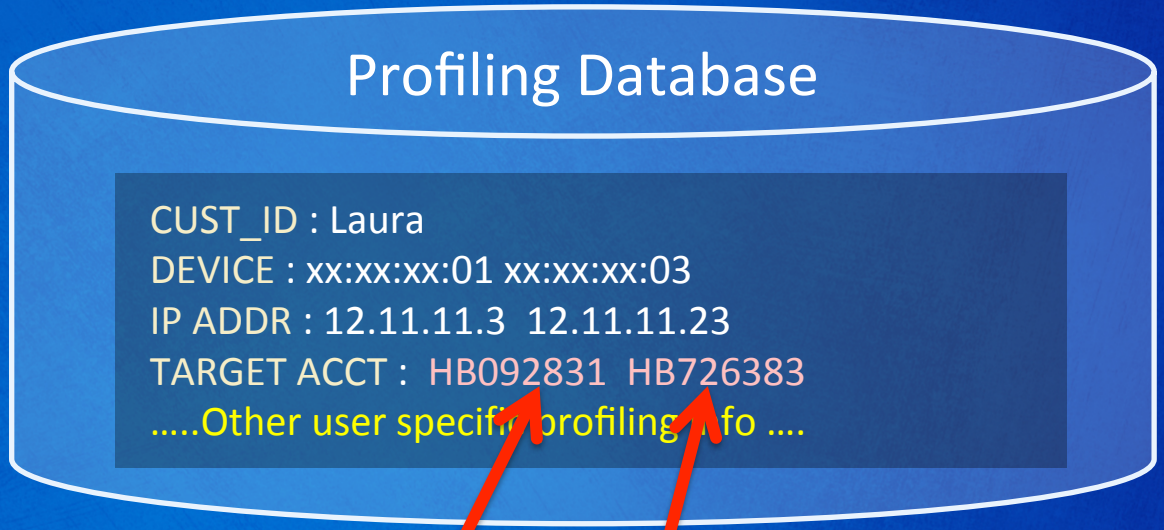


 |

Concept of “Entity Profiling”

Purpose

- Baseline customer behaviors
- Design analysis model



Good Customer “Laura”

Normal Transfer 1 : Target ACCT **HB092831**

Normal Transfer 2 : Target ACCT **HB726383**

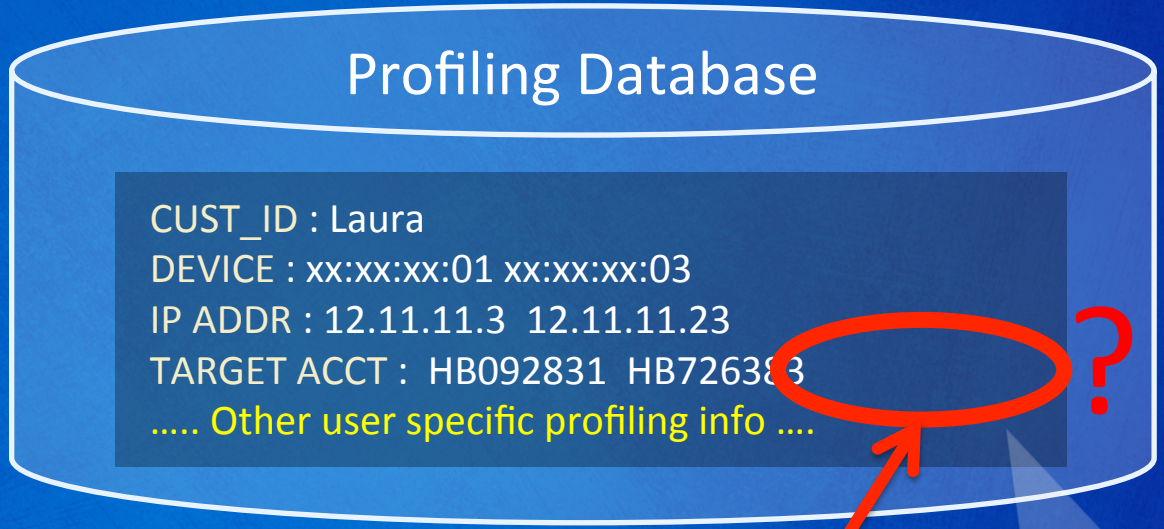
The target account exists already in profiling DB

 |

Concept of “Entity Profiling”

Purpose

- Baseline customer behaviors
- Design analysis model



Fraudster

Normal Transfer 1 : Target ACCT **HB092831**

Normal Transfer 2 : Target ACCT **HB726383**

Fraudulent Transfer 3 : Target ACCT **AB239242**

Since this is a unknown account, is this legitimate?

 |

splunk>

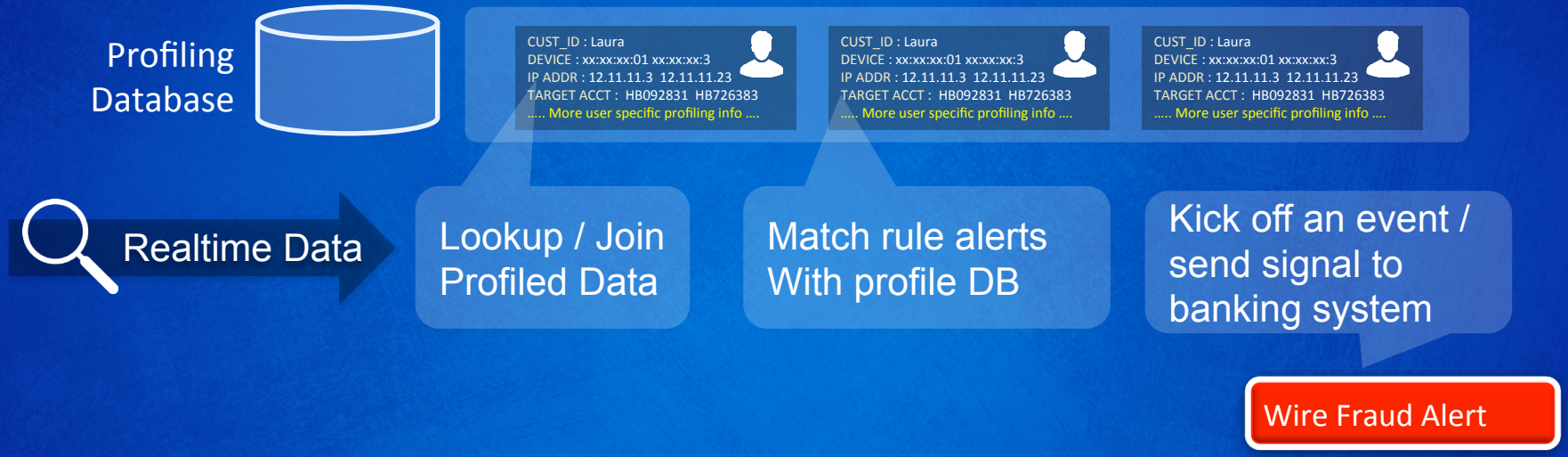
Detecting Based on Profiled Info: Profiling Search

Search 1 : Profiling Search (Scheduled -2m@m ~ -1m@m)

- Create new customer profiles
- Update atributes of profiles based on analysis criteria

 |

Detecting Based on Profiled Info: Detecting Search

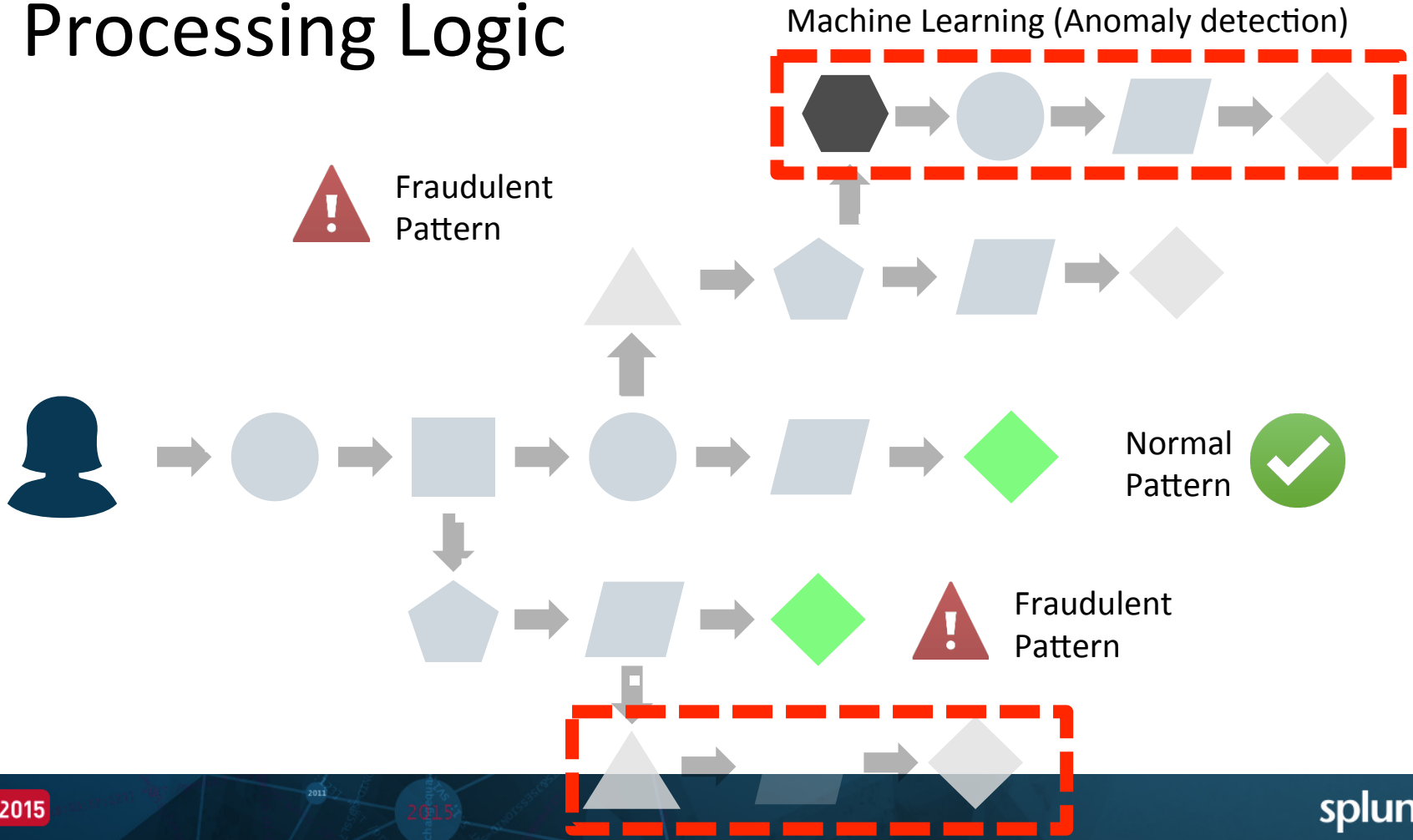


Search 2 : Pattern Detection Search (Real-time RT)

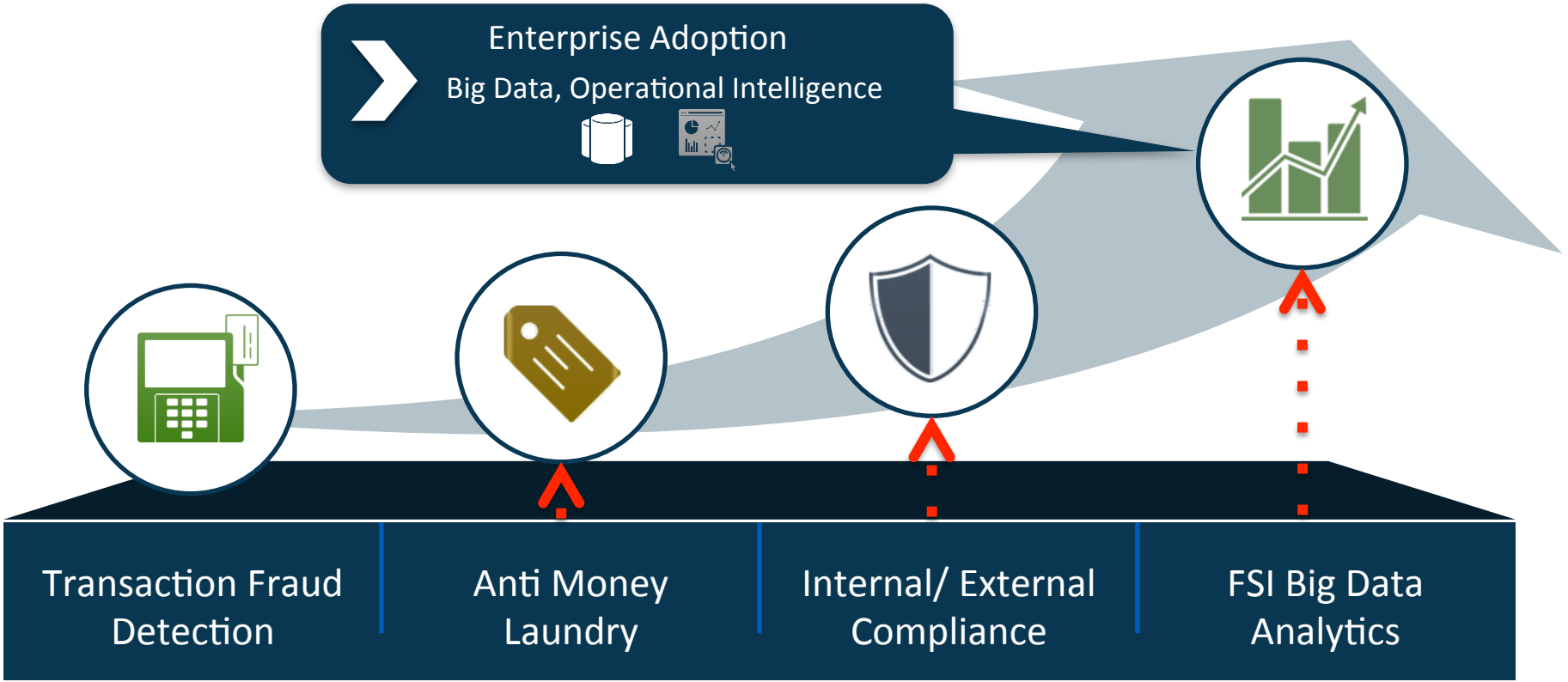
- Real-time searching, Joining lookups and other verification
- Match the status in profile DB for condition verification

 |

Processing Logic



Importance Of Being Transactions Data Store



Why is This So Significant?

These transaction data is at the heart of all financial service analysis

FDS
Fraud Detection System

Government Regulations

IT OPS

Security

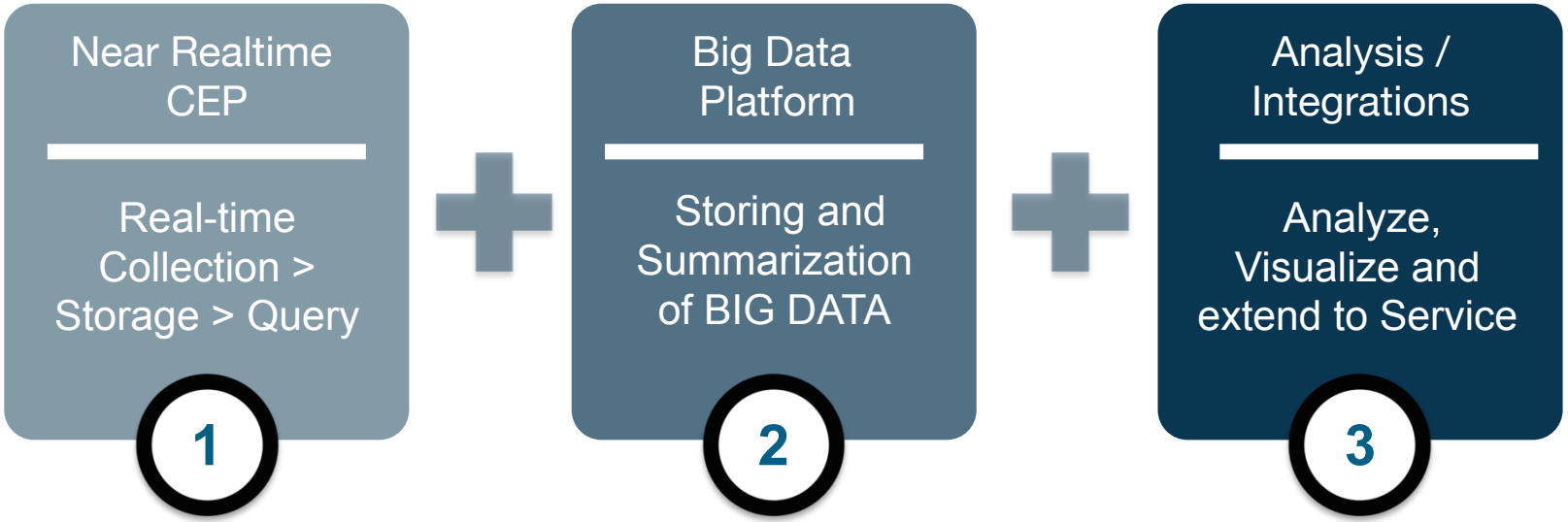
Expects various financial service Innovations

Big Data Target Marketing

Business Analytics

Future Data Projects

Synergy Factors of Splunk (To Joe)



Integrated Real-time Fraud Detection/ Prevention Platform

Demo

splunk>

Take-Aways

- Patterns of fraud are in machine data
- Splunk can harness machine data to detect, investigate, and report on a wide range of fraud
- Splunk can address the more demanding and technical fraud use cases (financial services, etc)

What Now?

- Go the “Compliance & Fraud” booth at the App Showcase
- Other sessions:
  - “Exposing Fraud and Risk for Health Agencies”, Tues, 3-3:45
  - “Orrstown Bank”, Tues, 5-5:45
  - “From Zero to Pretty Robust Fraud Detection Tool”, Wed, 10-10:45
  - “Detecting Bank Account Takeover and Fraud Attacks with Splunk”, Wed, 2-2:45
- Info, case study at:
  - Splunk.com > Solutions > Security & Fraud > Fraud
- Contact sales team at Splunk.com > Contact Us

Questions?

THANK YOU

splunk>