SEC1905 - 159 Security Use Cases In Record Time With Splunk and Kafka

Lock Landgon - Global Director - Security Analytics at McKesson
Nik Macroglou – Sales Engineer at Splunk

May 2018 | Version 1.0

Forward-Looking Statements

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 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.

splunk> .conf18

Agenda

- Who is McKesson?
- Kafka Overview
  - What is Kafka
  - Why did we choose Kafka
  - Trouble Shooting
  - Splunk Cloud overview
- How they work together
  - Use Case Process
  - Examples of the some of the 159 use cases
  - Connectors
- Share the love

splunk> .conf18

Who are we?

Who is Nik Macroglou

Born/Raised in Pittsburgh, PA - Da Burgh

Love to play Golf

Networking/Telcom Background

Music Producer/DJ (love dirty bass music)

Started using Splunk 4.x in 2012 @ Echostar

Primary Admin supporting 1TB on prem install for CAS and surrounding groups

Joined Splunk in 2017 as a SE

Live in Phoenix since 2004
Married with 4 kiddos (9/10/11/20)

Senior Engineer I @ AMEX 2014 - 2017 designing/supporting/growing the AMEX Splunk CoE to 6TB on prem Cross Site Replicated instance supporting 43 internal departmental use cases across the stack

splunk> .conf18

Who is Lock Langdon

- Born/Raised in Cottonwood, CA
- Love to read and play video games.
- Systems, Storage, Medical Imaging, and evil pointy haired manager background

First used Splunk in 2009 @ Mayo Clinic to track storage array logging issues. Also used it in Medical imaging to track DICOM Tagging Issues

Moved to AZ in 1993

Really started using Splunk at Stanford in Palo Alto, and at a small VAR named cStor in Arizona to develop provide application performance dashboards, and help customers solve security issues.

Joined McKesson in 2018 as The Global Director of Security Analytics to Deploy Splunk and deliver a SIEM for the Global iSOC

splunk> .conf18

Who is MCKESSON

The biggest company you probably haven't heard of

1/3 *of all pharmaceuticals*

used each day in North America are delivered by McKesson

4th *largest pharmacy chain*

4,800+ retail pharmacies are members of our Health Mart® franchise

Company founded: **1833**	Fortune 500: **Ranked 6th**
Headquarters: **San Francisco**	Employees: **78,000+**

16,000+ owned and banner *pharmacies* delivering patient care

McKesson is an industry leader in:

- Pharmaceutical distribution in North America and Europe
- Medical-surgical distribution to alternate care sites
- Generics pharmaceutical distribution
- Business and clinical services for providers
- Healthcare technology solutions

275,000+ SKUs of brand & private label medical-surgical supplies

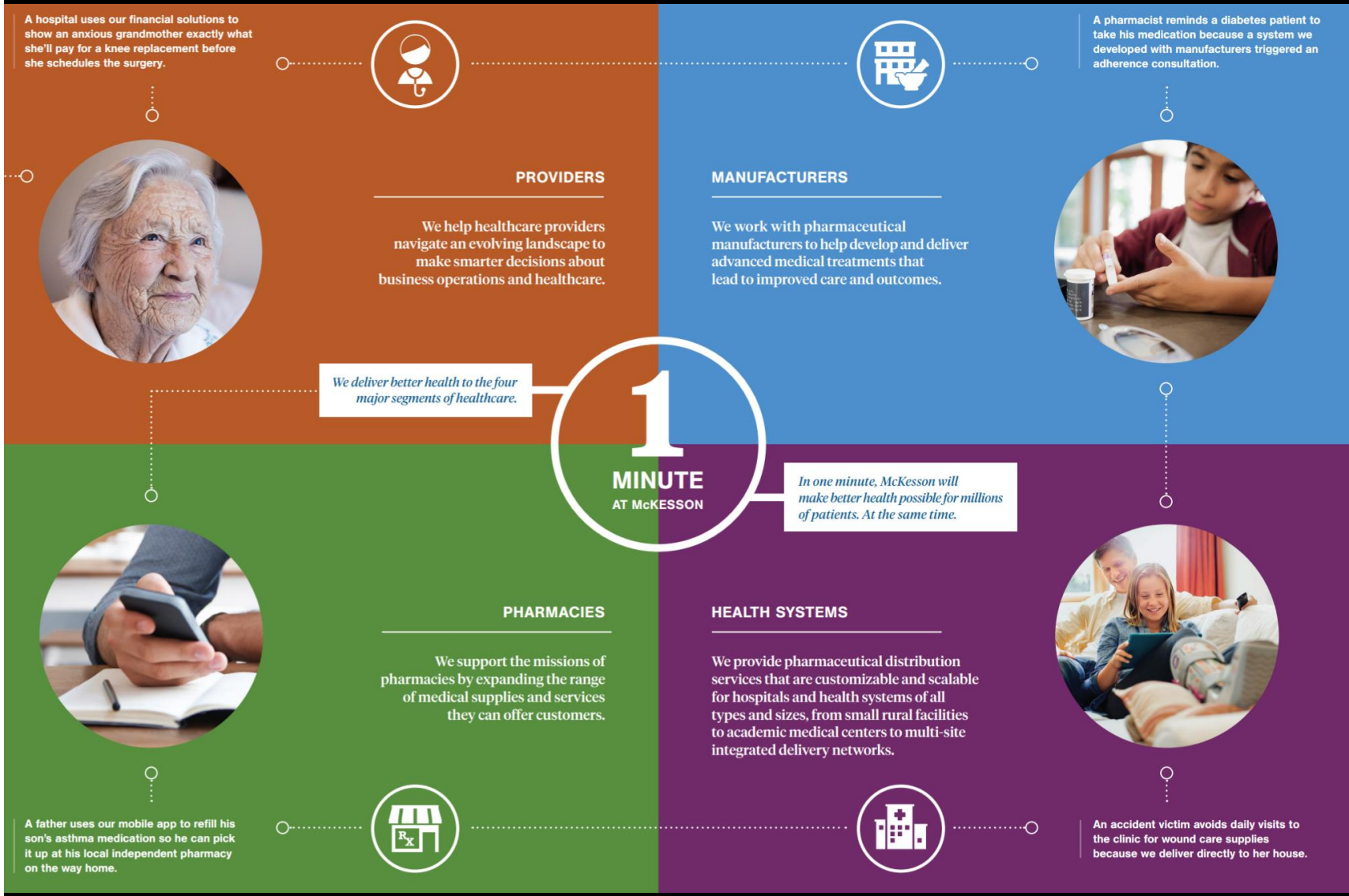
9,100+ oncologists & other specialists supported with specialty solutions

mckesson.com

08.17.2018

Who is McKESSON

The biggest company you probably haven't heard of



splunk> .conf18

Poll

What is Kafka

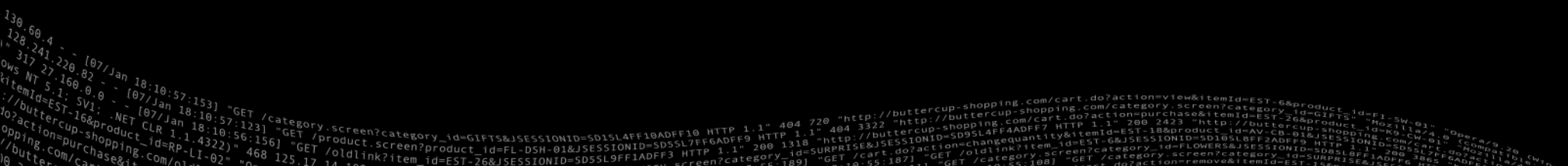
Apache Kafka was originally developed by LinkedIn, and was subsequently open sourced in early 2011.

- **Kafka** is used for building real-time data pipelines and streaming apps. It is horizontally scalable, fault-tolerant, wicked fast, and runs in production in thousands of companies.

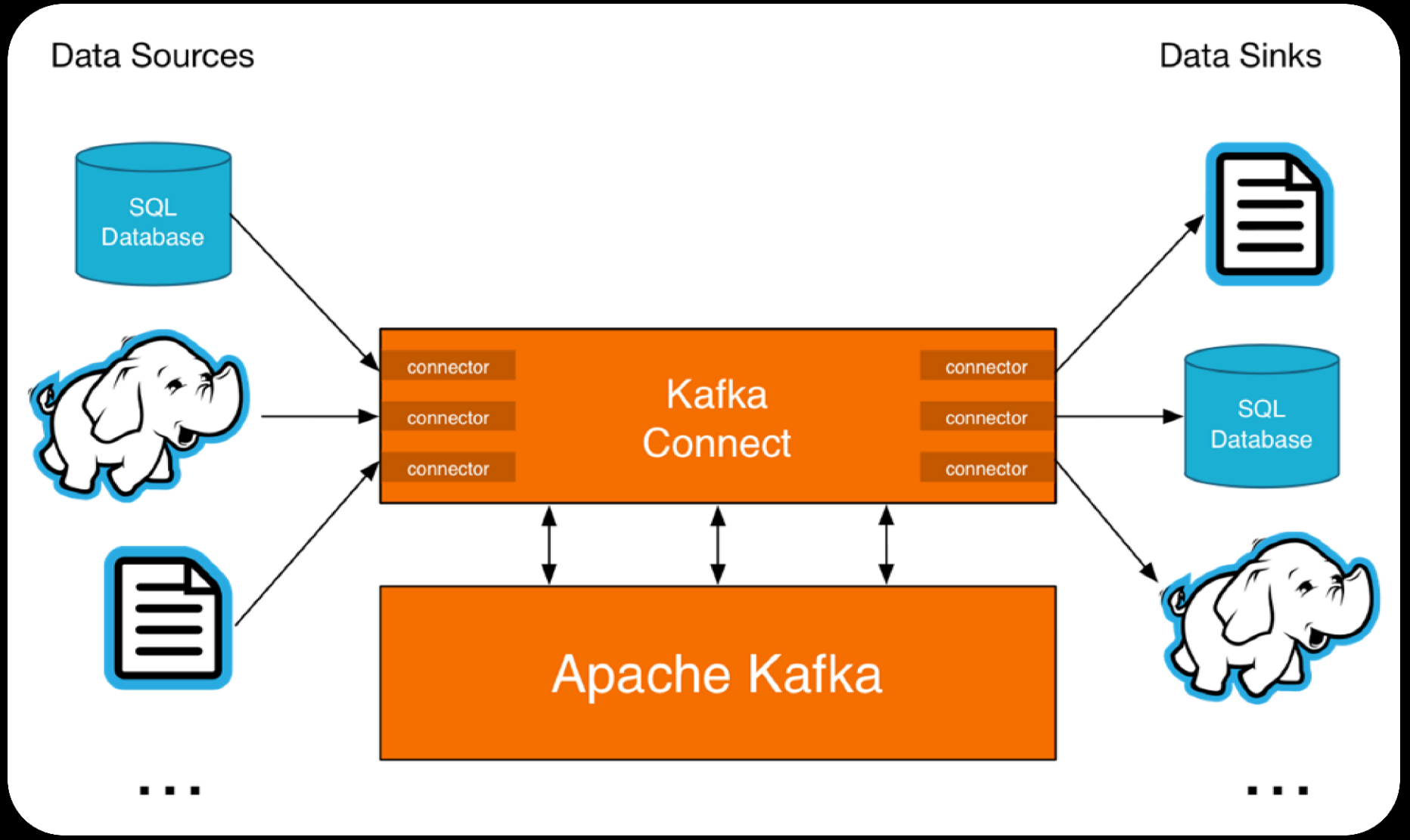
https://kafka.apache.org/

- **Kafka Connect** is a framework included in Apache Kafka that integrates Kafka with other systems. Its purpose is to make it easy to add new systems to your scalable and secure stream data pipelines.

https://www.confluent.io/product/connectors/



Kafka Data Flow



“ Press Release
Confluent Grows Subscriptions By Over 700 Percent in 2016 as Businesses Seize the Power of Real-Time Data

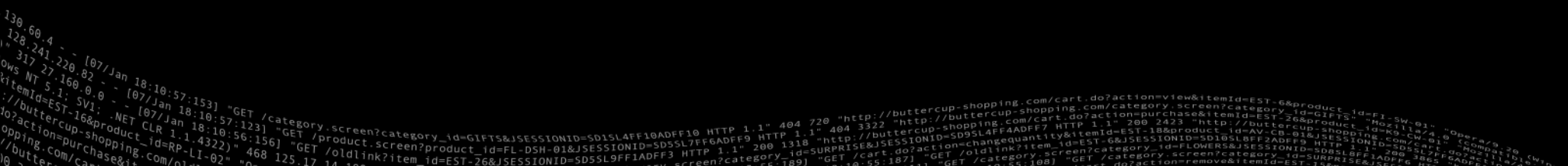
Company growth in 2016 driven by strong demand for streaming platforms and Apache Kafka® as enterprises go real time

https://www.confluent.io/press-release/confluent-grows-subscriptions-700-percent-2016-businesses-seize-power-real-time-data/

splunk> .conf18

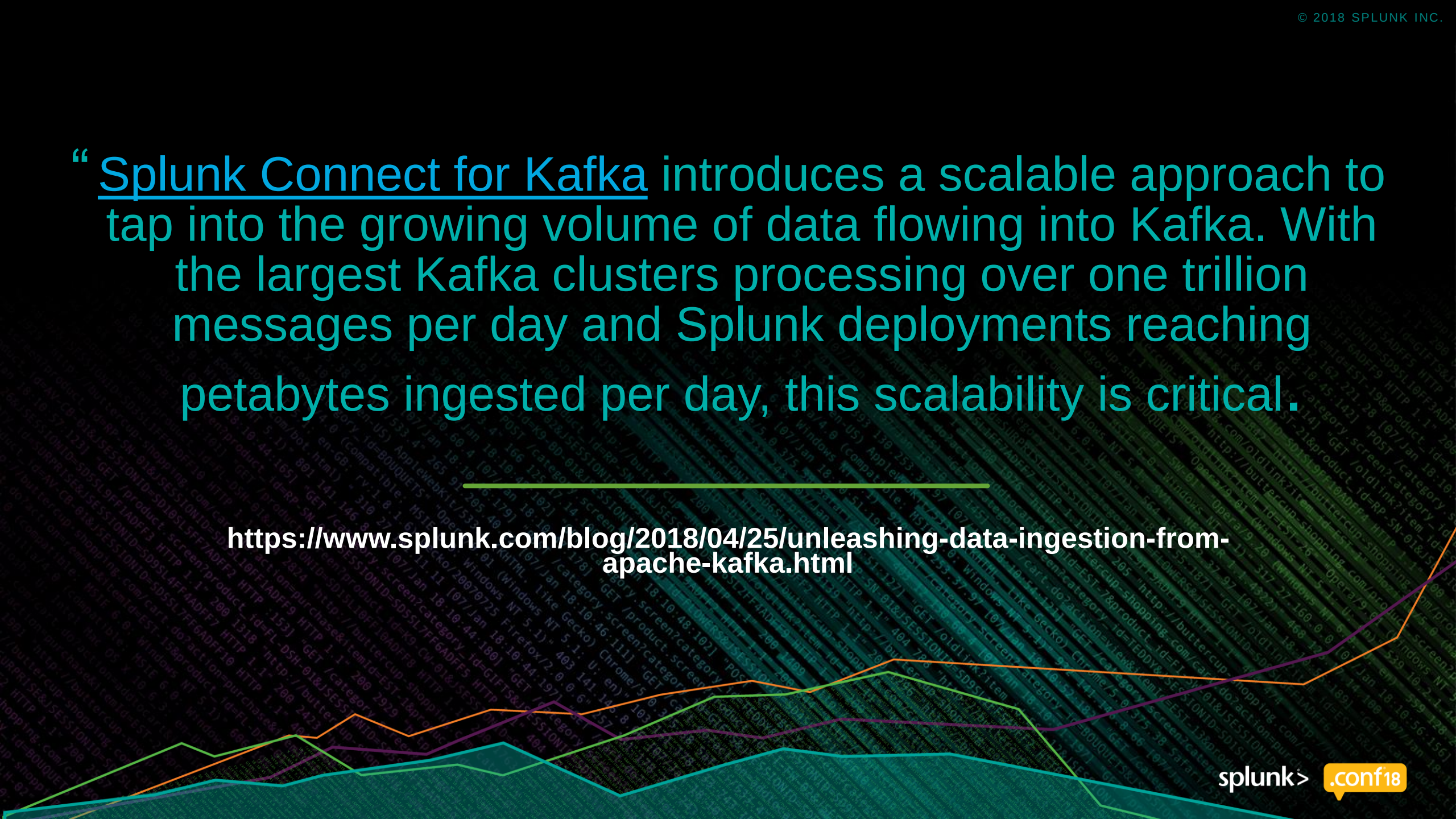
Why did we choose Kafka

1. No existing solution
2. Supports other areas
3. Decades of legacy
4. Looking to the future
5. The Team

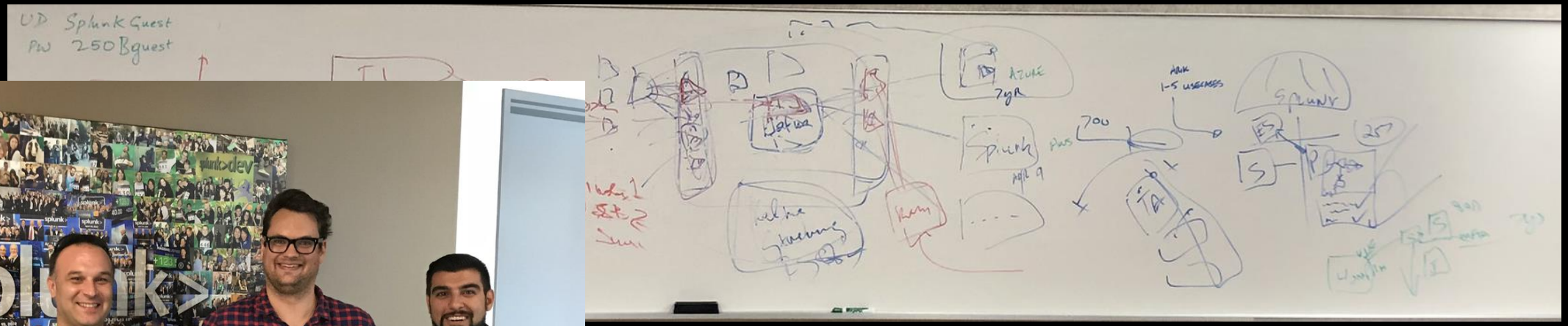


“ Splunk Connect for Kafka introduces a scalable approach to tap into the growing volume of data flowing into Kafka. With the largest Kafka clusters processing over one trillion messages per day and Splunk deployments reaching petabytes ingested per day, this scalability is critical.

https://www.splunk.com/blog/2018/04/25/unleashing-data-ingestion-from-apache-kafka.html



Kafka Connector Co-Engineering Efforts



- Splunk Product Manager and Lead Kafka Engineer validated McKesson's approach aligns to Splunk's vision with Kafka
- Monthly joint sessions scheduled at Splunk Corp HQ (270 Brannan St) in San Francisco
- Specific feature requests (i.e. Kafka Headers) have been prioritized by Splunk Engineering

How is McKesson Using Kafka?

Our Hardware Config

if wanting a cluster locally

- Full HA Kafka Cluster
  - All servers Linux
  - 3 x Zookeeper: 8G RAM, 2 CPU, 150G HDD
  - 3 x Kafka Broker: 32G RAM, 8 CPU, 1T HDD
  - 3 x Connect/Schema registry: 16G RAM, 4 CPU, 100G HDD
  - 1 x Rep/CC/Mgmt: 16G RAM, 4 CPU, 1T HDD
  - 2 x Load Balancer Servers HAProxy
    - 1 Virtual IP for the load balancers

Troubleshooting and Other tidbits

Methods to confirm Kafka services running and listening:

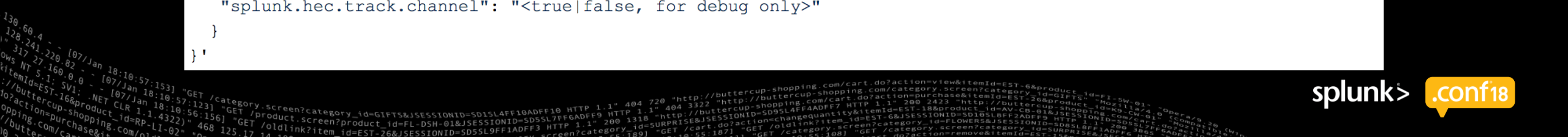
```
# List active connectors
curl http://localhost:8083/connectors

# Get kafka-connect-splunk connector info
curl http://localhost:8083/connectors/kafka-connect-splunk

# Get kafka-connect-splunk connector config info
curl http://localhost:8083/connectors/kafka-connect-splunk/config

# Delete kafka-connect-splunk connector
curl http://localhost:8083/connectors/kafka-connect-splunk -X DELETE

# Get kafka-connect-splunk connector task info
curl http://localhost:8083/connectors/kafka-connect-splunk/tasks
```

Sending test syslog data to test source and sink

- Send sample log using logger command:
- logger --udp --server 10.10.10.4 --port 5521 "Test message from logger" (sometimes it is useful to add more info in the message to specify more detail)
- logger --tcp --server 10.10.10.5 --port 6514 "Test message from logger”
- “server” can be load balancer VIP or the active source connector, depending on what you are trying to test

Splunk Connector

```
curl localhost:8083/connectors -X POST -H "Content-Type: application/json" -d '{
"name": "kafka-connect-splunk",
"config": {
   "connector.class": "com.splunk.kafka.connect.SplunkSinkConnector",
   "tasks.max": "3",
   "topics": "<list-of-topics-separated-by-comma>",
   "splunk.indexes": "<list-of-indexes-for-topics-data-separated-by-comma>",
   "splunk.sources": "<list-of-sources-for-topics-data-separated-by-comma>",
   "splunk.sourcetypes": "<list-of-sourcetypes-for-topics-data-separated-by-comma>",
   "splunk.hec.uri": "<Splunk-HEC-URI>",
   "splunk.hec.token": "<Splunk-HEC-Token>",
   "splunk.hec.raw": "<true|false>",
   "splunk.hec.json.event.enrichment": "<key value pairs separated by comma, only applicable to /event HEC>",
    "splunk.hec.raw.line.breaker": "<line breaker separator>",
   "splunk.hec.ack.enabled": "<true|false>",
   "splunk.hec.ack.poll.interval": "<event ack poll interval>",
   "splunk.hec.ack.poll.threads": "<number of threads used to poll event acks>",
   "splunk.hec.ssl.validate.certs": "<true|false>",
   "splunk.hec.http.keepalive": "<true|false>",
   "splunk.hec.max.http.connection.per.channel": "<max number of http connections per channel>",
   "splunk.hec.total.channels": "<total number of channels>",
   "splunk.hec.max.batch.size": "<max number of kafka records post in one batch>",
   "splunk.hec.threads": "<number of threads to use to do HEC post for single task>",
   "splunk.hec.event.timeout": "<timeout in seconds>",
   "splunk.hec.socket.timeout": "<timeout in seconds>",
   "splunk.hec.track.channel": "<true|false, for debug only>"
  }
}'
```



splunk> .conf18

What is the value?

Normal Pan* Data

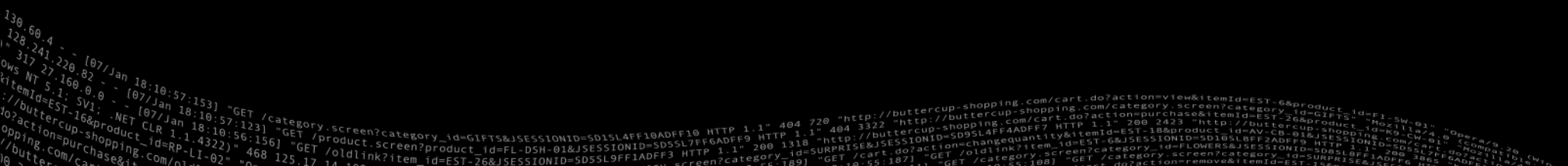
```
Jul 12 17:08:38 host 0,2018/07/12 17:08:38,007200002538,TRAFFIC,end,0,2018/07/12 17:08:38,221.202.126.46,10.154.9.132,,,Unexpected Traffic,,pancademo\michael.rodriqu,unknown-udp,vsys1,L3-TAP,L3-TAP,ethernet1/2,ethernet1/2,ToUS1RAM
Jul 12 17:08:37 host 0,2018/07/12 17:08:37,007200002539,TRAFFIC,end,0,2018/07/12 17:08:37,10.154.1.5,8.18.65.52,,,Watch Public DNS and SMTP,pancademo\dorothy.morrill,,dns,vsys1,L3-TAP,L3-TAP,ethernet1/2,ethernet1/2,ToUS1RAMA,2018/
Jul 12 17:08:38 host 0,2018/07/12 17:08:38,007200002539,TRAFFIC,end,0,2018/07/12 17:08:38,10.154.196.169,161.69.14.52,,,Watch Public DNS and SMTP,pancademo\jordan.bowery,,dns,vsys1,L3-TAP,L3-TAP,ethernet1/2,ethernet1/2,ToUS1RAMA,2
Jul 12 17:08:36 host 0,2018/07/12 17:08:36,007200002539,TRAFFIC,end,0,2018/07/12 17:08:36,10.154.7.147,74.125.53.101,,,General Web Infrastructure,pancademo\florence.lapete,,google-analytics,vsys1,L3-TAP,L3-TAP,ethernet1/2,ethernet
Jul 12 17:08:36 host 0,2018/07/12 17:08:36,007200002538,TRAFFIC,end,0,2018/07/12 17:08:36,202.96.209.26,10.154.196.161,,,Watch Public DNS and SMTP,,pancademo\marc.albrighton,dns,vsys1,L3-TAP,L3-TAP,ethernet1/2,ethernet1/2,ToUS1RAM
Jul 12 17:08:38 host 0,2018/07/12 17:08:38,007200002536,TRAFFIC,end,0,2018/07/12 17:08:38,10.154.196.169,200.12.199.1,,,Watch Public DNS and SMTP,pancademo\jordan.bowery,,dns,vsys1,L3-TAP,L3-TAP,ethernet1/2,ethernet1/2,ToUS1RAMA,2
Jul 12 17:08:36 host 0,2018/07/12 17:08:36,007200002538,THREAT,wildfire-virus,0,2018/07/12 17:08:36,66.1.1.6,10.154.10.133,,,Watch Public DNS and SMTP,,,smtp,vsys1,L3-TAP,L3-TAP,ethernet1/2,ethernet1/2,ToUS1RAMA,2018/07/12 17:08:3
Jul 12 17:08:36 host 0,2018/07/12 17:08:36,007200002539,TRAFFIC,end,0,2018/07/12 17:08:36,10.154.227.49,198.189.255.230,,,General Web Infrastructure,pancademo\scott.sinclair,,web-browsing,vsys1,L3-TAP,L3-TAP,ethernet1/2,ethernet1/
Jul 12 17:08:38 host 0,2018/07/12 17:08:38,007200002539,THREAT,url,0,2018/07/12 17:08:38,10.154.213.20,69.2.103.13,,,General Web Infrastructure,pancademo\jack.wilshire,,web-browsing,vsys1,L3-TAP,L3-TAP,ethernet1/2,ethernet1/2,ToUS
Jul 12 17:08:38 host 0,2018/07/12 17:08:38,007200002536,TRAFFIC,end,0,2018/07/12 17:08:38,137.145.204.10,10.154.12.101,,,Watch Public DNS and SMTP,,pancademo\lori.mccullough,dns,vsys1,L3-TAP,L3-TAP,ethernet1/2,ethernet1/2,ToUS1RAM
```

MCK Kakfa Pan* Data

```
536 <14>1 2018-07-12T12:59:54-04:00 MKSC-GMD-TCC-IPS2.mckesson.ca - - - - 1,2018/07/12 12:59:54,012001004884,TRAFFIC,end,0,2018/07/12 12:59:54,10.80.144.152,10.80.148.160,0.0.0.0,0.0.0.0,pdpSecMplsPHI,ca\tdemets,ca\svc-ad-
bkp,dns,vsys1,ptnzMplsIn,ptnzMplsOut,ethernet1/2,ethernet1/1,pdoLogPanAll_SyslogNoTraffic,2018/07/12 12:59:54,102166,1,57411,53,0,0,0x19,udp,allow,260,77,183,2,2018/07/12 12:59:24,0,any,0,134669729,0x0,10.0.0.0-10.255.255.255,10.0.0.0-
10.255.255.255,0,1,1,aged-out,15,67,0,0,,MKSC-GMD-TCC-IPS2,from-policy,,,0,,0,,N/A

535 <14>1 2018-07-12T12:59:54-04:00 MKSC-GMD-TCC-IPS2.mckesson.ca - - - - 1,2018/07/12 12:59:54,012001004884,TRAFFIC,end,0,2018/07/12 12:59:54,10.80.144.152,10.80.148.160,0.0.0.0,0.0.0.0,pdpSecMplsPHI,ca\tdemets,ca\svc-ad-
bkp,dns,vsys1,ptnzMplsIn,ptnzMplsOut,ethernet1/2,ethernet1/1,pdoLogPanAll_SyslogNoTraffic,2018/07/12 12:59:54,86614,1,50728,53,0,0,0x19,udp,allow,222,90,132,2,2018/07/12 12:59:24,0,any,0,134669730,0x0,10.0.0.0-10.255.255.255,10.0.0.0-
10.255.255.255,0,1,1,aged-out,15,67,0,0,,MKSC-GMD-TCC-IPS2,from-policy,,,0,,0,,N/A

530 <14>1 2018-07-12T12:59:54-04:00 MKSC-GMD-TCC-IPS2.mckesson.ca - - - - 1,2018/07/12 12:59:54,012001004884,TRAFFIC,end,0,2018/07/12
12:59:54,10.80.136.114,10.80.144.16,0.0.0.0,0.0.0.0,pdpSecMpls,,,msrpc,vsys1,ptnzMplsOut,ptnzMplsIn,ethernet1/1,ethernet1/2,pdoLogPanAll_SyslogNoTraffic,2018/07/12 12:59:54,101836,1,59716,49165,0,0,0x1a,tcp,allow,2226,1394,832,13,2018/07/12
12:59:21,18,any,0,134669731,0x0,10.0.0.0-10.255.255.255,10.0.0.0-10.255.255.255,0,8,5,tcp-rst-from-client,15,67,0,0,,MKSC-GMD-TCC-IPS2,from-policy,,,0,,0,,N/A

558 <14>1 2018-07-12T12:59:54-04:00 MKSC-GMD-TCC-IPS2.mckesson.ca - - - - 1,2018/07/12 12:59:54,012001004884,TRAFFIC,end,0,2018/07/12 12:59:54,10.80.72.239,10.80.144.16,0.0.0.0,0.0.0.0,pdpSecMplsPHI,ca\kchung,,print-over-ms-
smb,vsys1,ptnzMplsOut,ptnzMplsIn,ethernet1/1,ethernet1/2,pdoLogPanAll_SyslogNoTraffic,2018/07/12 12:59:54,70093,1,52346,49165,0,0,0x1a,tcp,allow,32878,16617,16261,55,2018/07/12 12:59:25,14,any,0,134669732,0x0,10.0.0.0-10.255.255.255,10.0.0.0-
10.255.255.255,0,29,26,tcp-rst-from-client,15,67,0,0,,MKSC-GMD-TCC-IPS2,from-policy,,,0,,0,,N/A

529 <14>1 2018-07-12T12:59:54-04:00 MKSC-GMD-TCC-IPS2.mckesson.ca - - - - 1,2018/07/12 12:59:54,012001004884,TRAFFIC,end,0,2018/07/12
12:59:54,10.80.136.37,10.80.144.16,0.0.0.0,0.0.0.0,pdpSecMpls,,,msrpc,vsys1,ptnzMplsOut,ptnzMplsIn,ethernet1/1,ethernet1/2,pdoLogPanAll_SyslogNoTraffic,2018/07/12 12:59:54,64848,1,53880,49165,0,0,0x1a,tcp,allow,3744,1754,1990,15,2018/07/12
12:59:26,13,any,0,134669733,0x0,10.0.0.0-10.255.255.255,10.0.0.0-10.255.255.255,0,9,6,tcp-rst-from-client,15,67,0,0,,MKSC-GMD-TCC-IPS2,from-policy,,,0,,0,,N/A

529 <14>1 2018-07-12T12:59:54-04:00 MKSC-GMD-TCC-IPS2.mckesson.ca - - - - 1,2018/07/12 12:59:54,012001004884,TRAFFIC,end,0,2018/07/12
12:59:54,10.80.136.37,10.80.144.16,0.0.0.0,0.0.0.0,pdpSecMpls,,,msrpc,vsys1,ptnzMplsOut,ptnzMplsIn,ethernet1/1,ethernet1/2,pdoLogPanAll_SyslogNoTraffic,2018/07/12 12:59:54,77924,1,53881,49165,0,0,0x1a,tcp,allow,6492,3514,2978,16,2018/07/12
12:59:26,13,any,0,134669734,0x0,10.0.0.0-10.255.255.255,10.0.0.0-10.255.255.255,0,9,7,tcp-rst-from-client,15,67,0,0,,MKSC-GMD-TCC-IPS2,from-policy,,,0,,0,,N/A

506 <14>1 2018-07-12T12:59:55-04:00 MKSC-GMD-TCC-IPS2.mckesson.ca - - - - 1,2018/07/12 12:59:55,012001004884,TRAFFIC,end,0,2018/07/12
12:59:55,10.123.6.242,10.80.144.1,0.0.0.0,0.0.0.0,pdpSecMpls,,,ping,vsys1,ptnzMplsOut,ptnzMplsIn,ethernet1/1,ethernet1/2,pdoLogPanAll_SyslogNoTraffic,2018/07/12 12:59:55,50412,1,0,0,0,0,0x100019,icmp,allow,124,62,62,2,2018/07/12
12:59:43,0,any,0,134669735,0x0,10.0.0.0-10.255.255.255,10.0.0.0-10.255.255.255,0,1,1,aged-out,15,67,0,0,,MKSC-GMD-TCC-IPS2,from-policy,,,0,,0,,N/A

535 <14>1 2018-07-12T12:59:55-04:00 MKSC-GMD-TCC-IPS2.mckesson.ca - - - - 1,2018/07/12 12:59:55,012001004884,TRAFFIC,end,0,2018/07/12 12:59:55,10.80.144.152,10.80.148.160,0.0.0.0,0.0.0.0,pdpSecMplsPHI,ca\tdemets,ca\svc-ad-
bkp,dns,vsys1,ptnzMplsIn,ptnzMplsOut,ethernet1/2,ethernet1/1,pdoLogPanAll_SyslogNoTraffic,2018/07/12 12:59:55,40292,1,64681,53,0,0,0x19,udp,allow,329,76,253,2,2018/07/12 12:59:25,0,any,0,134669736,0x0,10.0.0.0-10.255.255.255,10.0.0.0-
10.255.255.255,0,1,1,aged-out,15,67,0,0,,MKSC-GMD-TCC-IPS2,from-policy,,,0,,0,,N/A

535 <14>1 2018-07-12T12:59:55-04:00 MKSC-GMD-TCC-IPS2.mckesson.ca - - - - 1,2018/07/12 12:59:55,012001004884,TRAFFIC,end,0,2018/07/12 12:59:55,10.80.144.152,10.80.148.160,0.0.0.0,0.0.0.0,pdpSecMplsPHI,ca\tdemets,ca\svc-ad-
bkp,dns,vsys1,ptnzMplsIn,ptnzMplsOut,ethernet1/2,ethernet1/1,pdoLogPanAll_SyslogNoTraffic,2018/07/12 12:59:55,32175,1,57208,53,0,0,0x19,udp,allow,212,76,136,2,2018/07/12 12:59:25,0,any,0,134669737,0x0,10.0.0.0-10.255.255.255,10.0.0.0-
10.255.255.255,0,1,1,aged-out,15,67,0,0,,MKSC-GMD-TCC-IPS2,from-policy,,,0,,0,,N/A

536 <14>1 2018-07-12T12:59:55-04:00 MKSC-GMD-TCC-IPS2.mckesson.ca - - - - 1,2018/07/12 12:59:55,012001004884,TRAFFIC,end,0,2018/07/12 12:59:55,10.80.144.152,10.80.148.160,0.0.0.0,0.0.0.0,pdpSecMplsPHI,ca\tdemets,ca\svc-ad-
bkp,dns,vsys1,ptnzMplsIn,ptnzMplsOut,ethernet1/2,ethernet1/1,pdoLogPanAll_SyslogNoTraffic,2018/07/12 12:59:55,129019,1,49256,53,0,0,0x19,udp,allow,213,81,132,2,2018/07/12 12:59:25,0,any,0,134669738,0x0,10.0.0.0-10.255.255.255,10.0.0.0-
10.255.255.255,0,1,1,aged-out,15,67,0,0,,MKSC-GMD-TCC-IPS2,from-policy,,,0,,0,,N/A
```

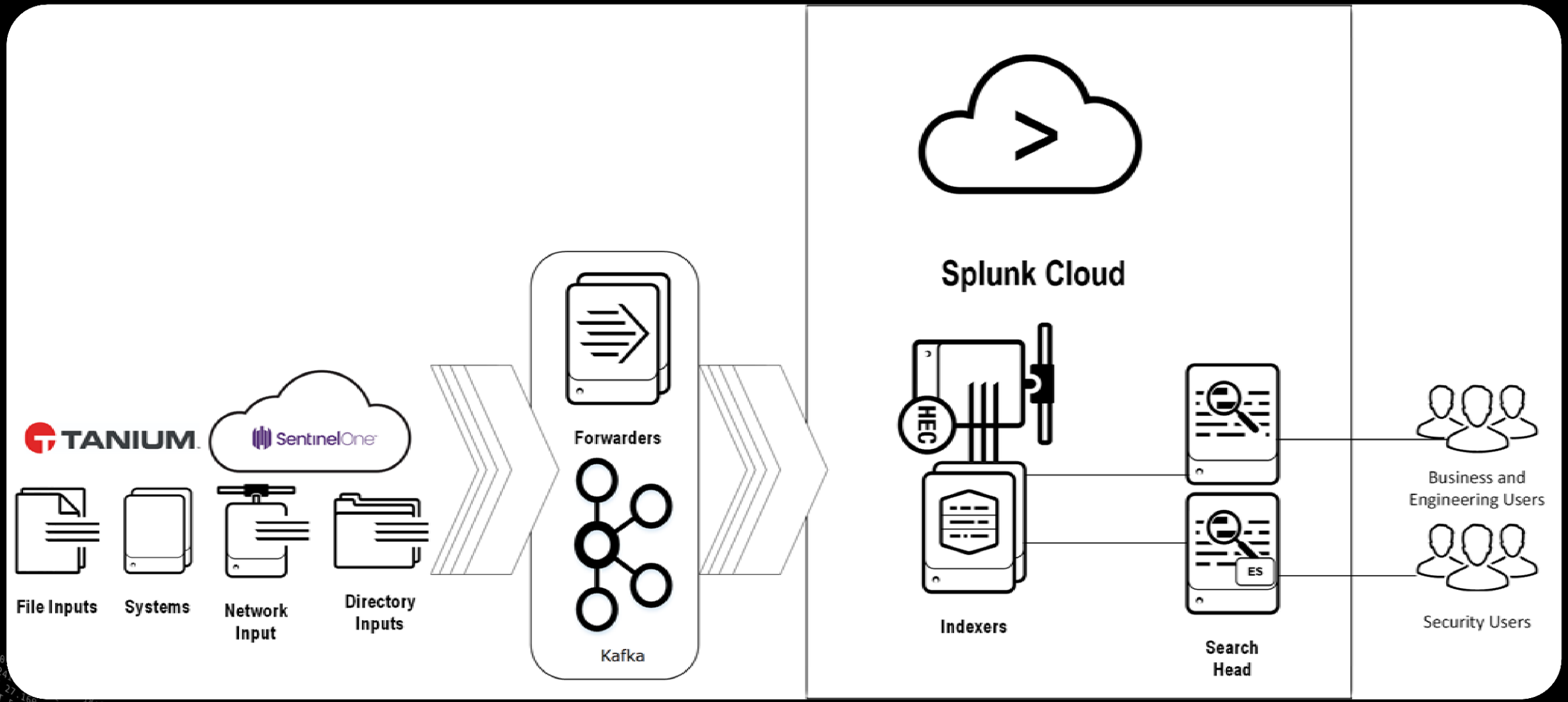
Kafka Connectors in Prod

Pipeline / Type of data
Avro Logs
Azure Blob Storage
Azure Logs
Cisco ASA
F5 Load Balancers
IAM
IBM enforcive (iSeries)
IMPERVA_DAM
ImpervaWAF
JUNIPER_SSLVPN
JUNOS_FW
Lancope Syslog Feed – Network
Level3 Threat Logs
LOGINSIGHT
LTS_ALL
McAfee ESM Receiver
MCAFEE_ESM
O365 Activity Data
O365 Blob
O365 DLP Data
Proofpoint
Proofpoint TAP
RSA_SECURID
Tanium
Trend Micro
ZSCALER

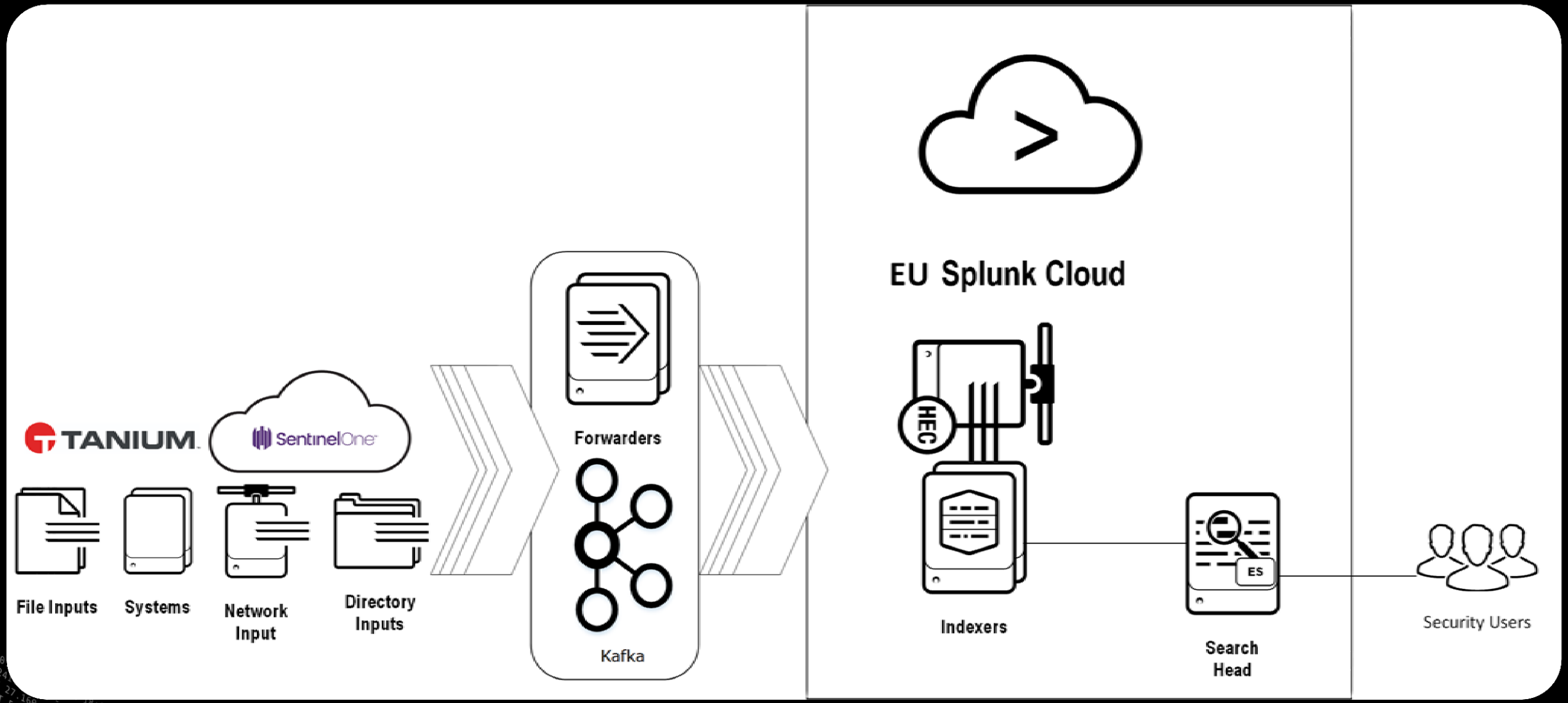


splunk> .conf18

US Architecture Overview



EU Architecture Overview

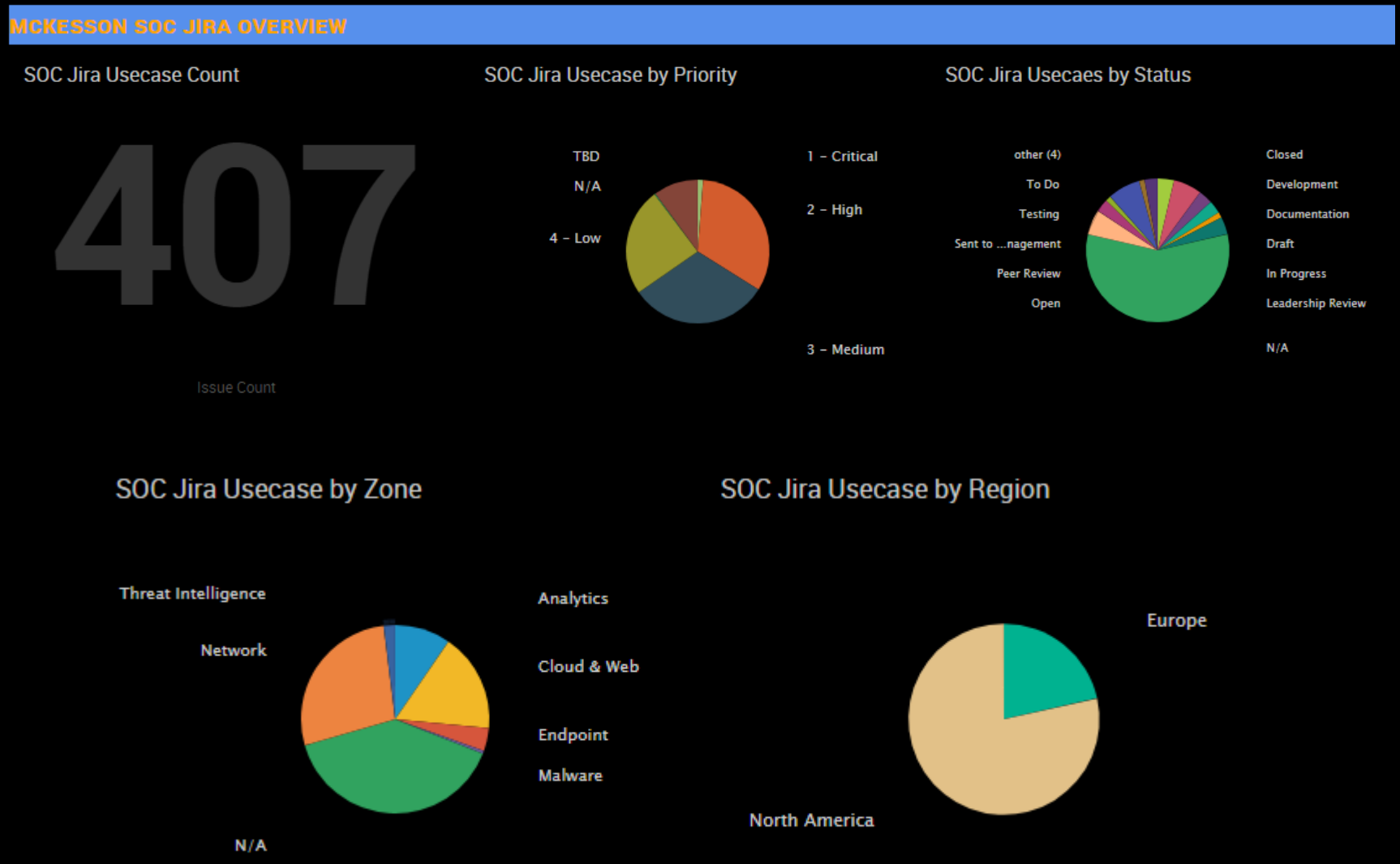


Putting It All Together!

What we did in 3 months

- Onboarded 27 new indexes,
- 74 new Data Source types
- Over 200 new devices and systems (not servers and workstations)
- Connected 5 new Business Units to our SOC
- 3 new acquisitions are providing data to the SIEM that aren’t even connected to the McKesson Network.
- We have North American visibility into Azure, O365, and Core Active Directory Services
- Global deployment of O365, Proofpoint, ZScaler, and Tanium.

Getting the Use Cases Done!



Use Case Process

SOC-Master / SOC-12082

P1 - UC0004 Excessive number of emails sent from internal user

Edit | Comment | Assign | More | Reject | Test | Hold

Details

Type:	Use Case	Status:	DEVELOPMENT (View Workflow)
Priority:	2 - High	Resolution:	Unresolved
Labels:	None		

SOC Use Case Matrix: Use Case SOP: https://mckessoncorp.sharepoint.com/:w:/r/sites/GRPActiveD/Shared%20Documents/General/Final/iSOC_SOP-Use_Case_Development_Review_Process.docx?d=w78b43d6a576e4bc2aebacccdf30b61da&csf=1&e=vvpu33

Purpose
This use case is alert when there is an excessive number of emails from an internal user. This can help detect a possible compromised user, that is sending malicious emails.

Technical Context
This section is targeted at the SIEM engineer or individual that will be creating the logic behind the alert. Include the following, if known:
- Data sources that should be referenced to trigger an alert and any fields that should be queried on
- Any AND/OR logic statements that would be necessary to create the desired output
- Limits that should be applied, i.e. “only alert on 5 or more events in 20 minutes per source IP”
- Sample searches

Categorization & Zone
Categories are based on the MITRE ATT&CK for enterprises model .Zones are defined by the McKesson Active Defense team. Refer to the Use Case SOP for a table of available values.

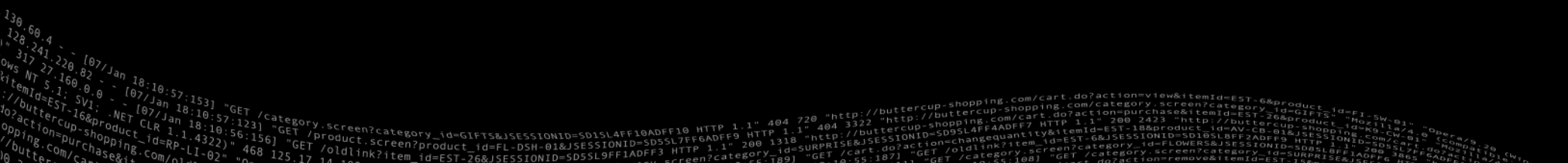
Priority
The initial priority level is determined by the selected category. Adjustments can be made up or down to this priority level if needed but discussed and approved during a use case. Refer to the Use Case SOP for a table of which category aligns with which priority.

SIEM:	Splunk
Zone:	Analytics
PI Objective:	False

Customer Showcase McKesson

- McKesson is leveraging a forked version of the Splunk Kafka Connector with leveraging:
  - Kafka Transforms
  - Kafka Headers
  - Kafka Streams (in POC)
  - Kafka SQL (in POC)
  - https://github.com/vrudenskyi/kafka-connect-splunk

- Custom connectors that McKesson has built and integrated currently:
  - Any layer4 TCP or UDP / network-based
  - HTTPs
  - ICAP
  - Office365
  - AzureMS
  - MSFT IoT HUB
  - SentinelOne



Open Source Repo for Kafka Tools (URL)