Splunking IBM i Data

Chip Sutton
Director, Software Development - Syncsort

Brian Brake
Senior Splunk Engineer – Cox Automotive

splunk> .conf19

Splunking IBM i Data

Chip Sutton
Director, Software Development - Syncsort

Brian Brake
Senior Splunk Engineer – Cox Automotive

Topical Questions

Why Should I Add IBM i data to Splunk?

What kind of IBM i data can I collect?

How do I get IBM i data into Splunk and how much time to implement?

What can I do with this data after it is Splunk?

How do I incorporate this into my day-to-day operations workflow?

Who is familiar with…

AS/400

System I

IBM i

iSeries

Power System

If you are familiar with one or more names…

Chances are you have one or more in your infrastructure

These systems run the IBM i Operating system, previously called

- OS/400
- I5/OS

Splunk is a great Enterprise Tool for …

- Applications
- Operating Systems
- Databases
- Performance Metrics
- Network statistics
- Security data/events
- And much more

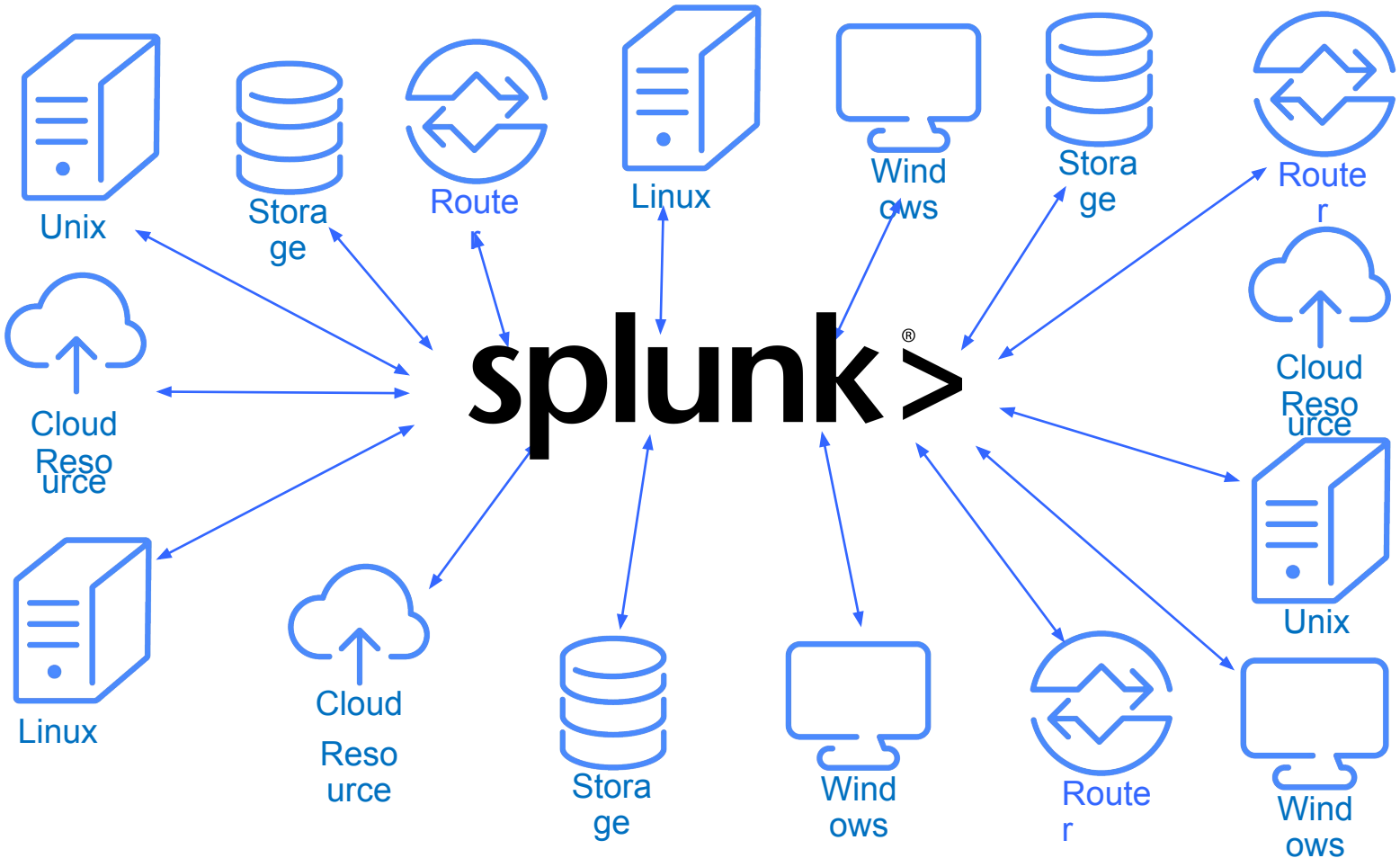
For all of your systems……except?

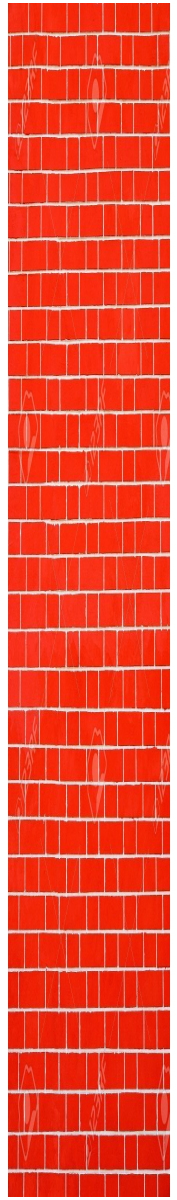
The IBM i Systems

I thought IBM i Systems were dying like the mainframe….

- Over **100,000** companies still use IBM i to power mission critical applications
- Banks, health care, manufacturing, retail, automotive and others
- Over 1/3 of these companies are running 75%+ workload on IBM i based on surveys
- IBM i provides the backbone of many critical enterprise business applications

Your Splunk Today…..

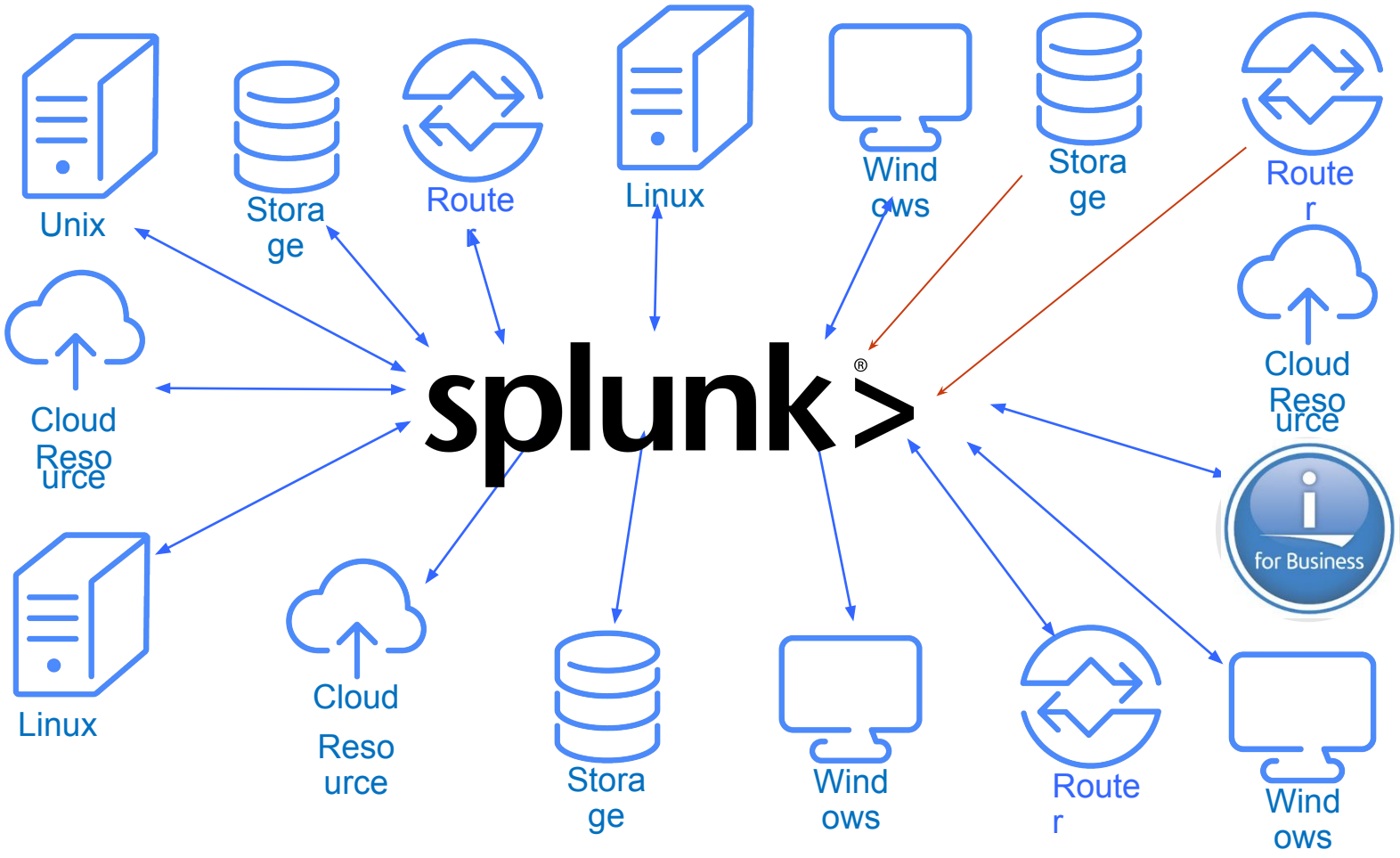




No visibility into mission-critical IBM i environments

splunk> .conf19

Your Splunk Tomorrow…..



What types of IBM i data can be collected ?

Message Queue data

- Similar to SYSLOG or Windows Event Logs
- Important event data about operating system, hardware and applications

System history log

- Capture messages not sent to other message queues

Security Audit Journal Data

- System wide auditing
- Auditing for specific objects (for example files)
- Auditing for specific users

System Performance Data

- System level performance summary data
- Detailed performance data from IBM Collection Services

Application Journal Events

- Object changes, for example database changes (before/after)

System Job Accounting Journal Events

- Capture information Job information, processing time, transaction counts, elapsed time, DB counts

But Splunk doesn't have an IBM i forwarding agent

Syncsort's Ironstream for Splunk product bridges this gap

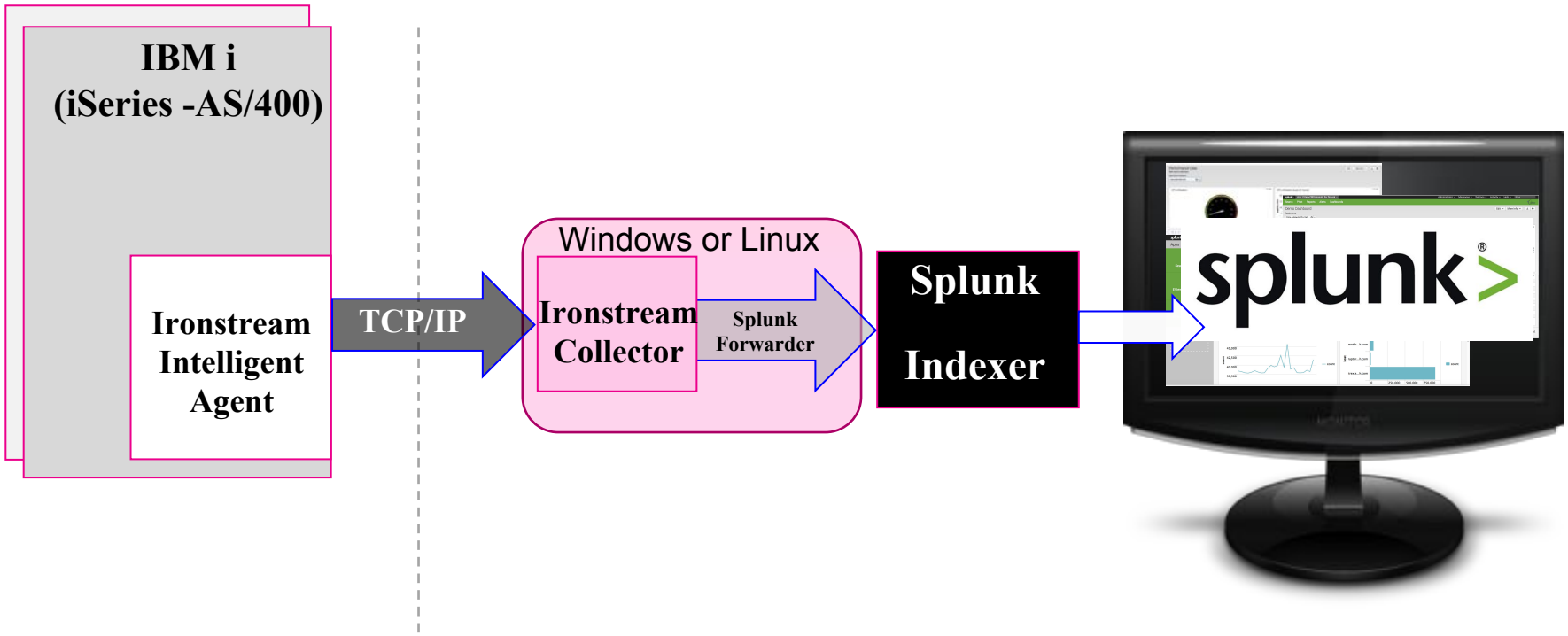
- Syncsort introduced the Ironstream for Splunk for IBM z/OS sytems years ago
- With the acquisition of EView Technology, Syncsort has added IBM i capability for Splunk

Allows you to build on your existing Splunk implementation to include IBM i system data

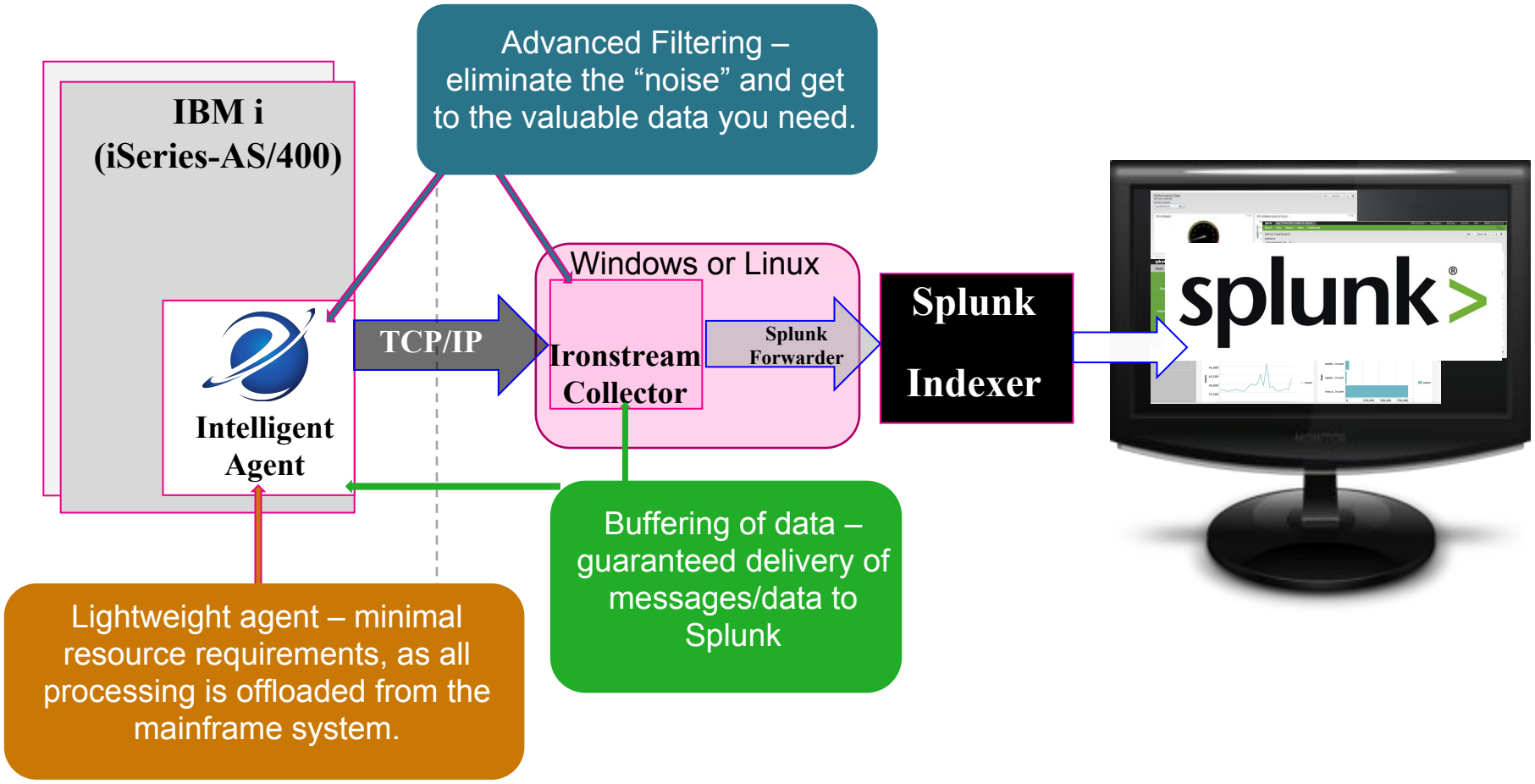
Low Overhead – designed to use minimal resource on the IBM i system

Filtering to give you control over what data you forward to Splunk

How does the integration work?



Integration Continued



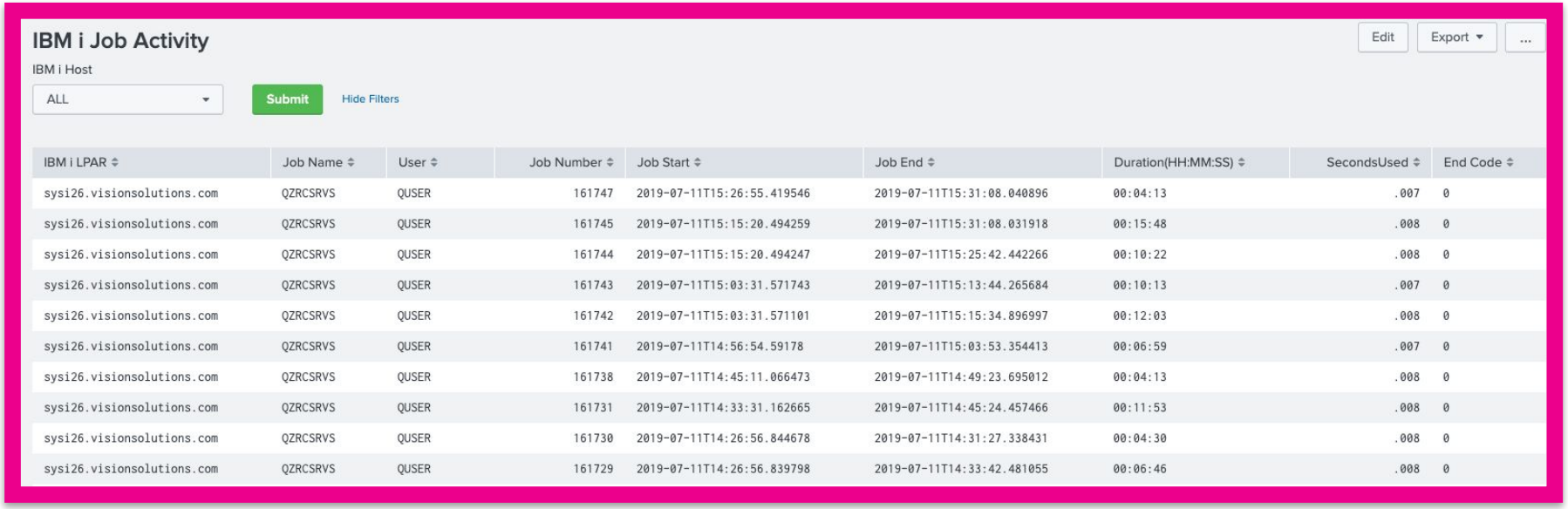
How might I use Message Queue or History Data

High-light critical events

Look at trends, for example application errors

Proactive analysis

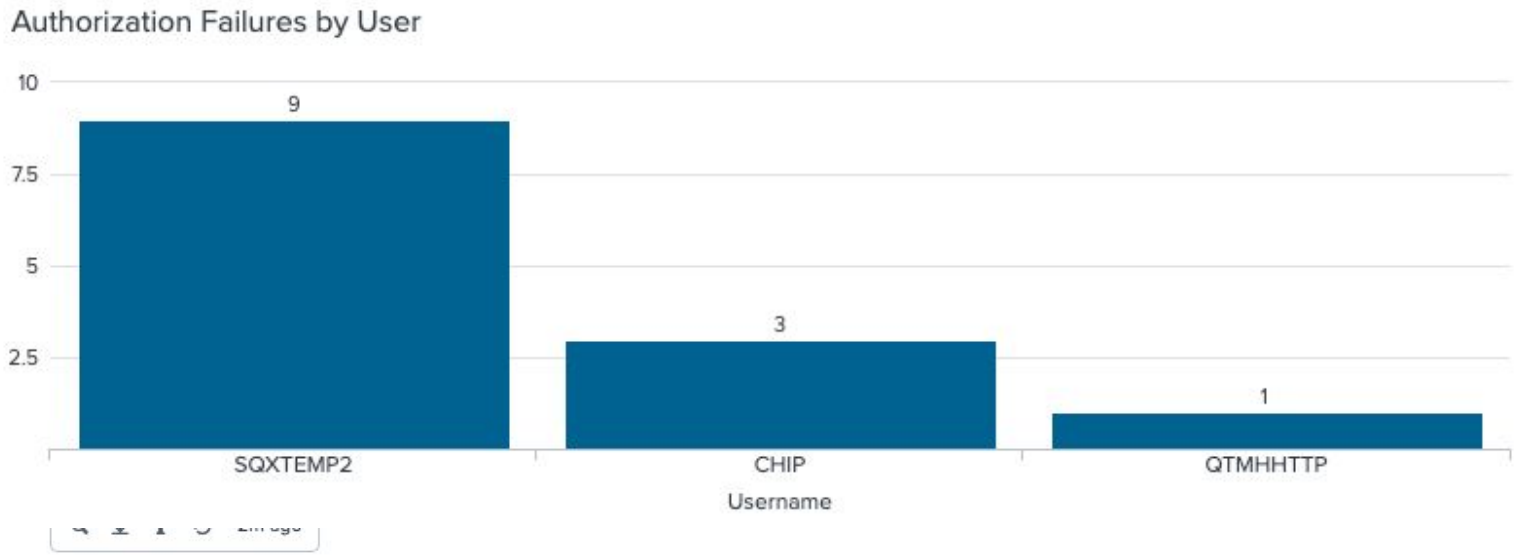
- Long running jobs
- Non fatal hardware errors
- Application issues



IBM i LPAR	Job Name	User	Job Number	Job Start	Job End	Duration(HH:MM:SS)	SecondsUsed	End Code
sysi26.visionsolutions.com	QZRCSRVS	QUSER	161747	2019-07-11T15:26:55.419546	2019-07-11T15:31:08.040896	00:04:13	.007	0
sysi26.visionsolutions.com	QZRCSRVS	QUSER	161745	2019-07-11T15:15:20.494259	2019-07-11T15:31:08.031918	00:15:48	.008	0
sysi26.visionsolutions.com	QZRCSRVS	QUSER	161744	2019-07-11T15:15:20.494247	2019-07-11T15:25:42.442266	00:10:22	.008	0
sysi26.visionsolutions.com	QZRCSRVS	QUSER	161743	2019-07-11T15:03:31.571743	2019-07-11T15:13:44.265684	00:10:13	.007	0
sysi26.visionsolutions.com	QZRCSRVS	QUSER	161742	2019-07-11T15:03:31.571101	2019-07-11T15:15:34.896997	00:12:03	.008	0
sysi26.visionsolutions.com	QZRCSRVS	QUSER	161741	2019-07-11T14:56:54.59178	2019-07-11T15:03:53.354413	00:06:59	.007	0
sysi26.visionsolutions.com	QZRCSRVS	QUSER	161738	2019-07-11T14:45:11.066473	2019-07-11T14:49:23.695012	00:04:13	.008	0
sysi26.visionsolutions.com	QZRCSRVS	QUSER	161731	2019-07-11T14:33:31.162665	2019-07-11T14:45:24.457466	00:11:53	.008	0
sysi26.visionsolutions.com	QZRCSRVS	QUSER	161730	2019-07-11T14:26:56.844678	2019-07-11T14:31:27.338431	00:04:30	.008	0
sysi26.visionsolutions.com	QZRCSRVS	QUSER	161729	2019-07-11T14:26:56.839798	2019-07-11T14:33:42.481055	00:06:46	.008	0

Security is important – what about examples?

- Authorization Failures
- Login attempts
- Creating or deleting objects
- User profile events – special authorities
- System Value changes
- Changes to sensitive files



Authorization Failures

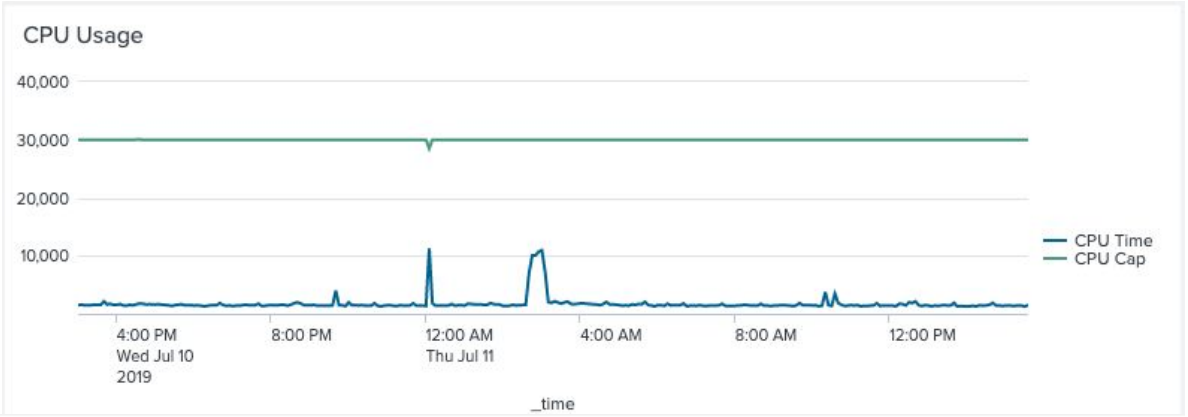
_time	User	Object Name	Object Library	Jobname	JobNumber	Program	ProgramLib	RemoteAddress	host
2019-07-11 10:33:57.567	SQXTEMP2	NETAP	REPTEST	AUDAP1	161638	QCMD	QSYS		sysi26.visionsolutions.com
2019-07-11 10:33:57.437	SQXTEMP2			AUDAF1	161633	NETAF	REPTEST		sysi26.visionsolutions.com
2019-07-11 10:33:57.425	SQXTEMP2			AUDAF1	161633	NETAF	REPTEST		sysi26.visionsolutions.com
2019-07-11 10:33:57.421	SQXTEMP2			AUDAF1	161633	NETAF	REPTEST		sysi26.visionsolutions.com
2019-07-11 10:33:57.413	SQXTEMP2	CHGUSRPRF	*N	AUDAF1	161633	NETAF	REPTEST		sysi26.visionsolutions.com
2019-07-11 10:33:57.405	SQXTEMP2	QSYS		AUDAF1	161633	NETAF	REPTEST		sysi26.visionsolutions.com
2019-07-11 10:33:57.384	SQXTEMP2	QAUDJRN	QSYS	AUDAF1	161633	NETAF	REPTEST		sysi26.visionsolutions.com
2019-07-11 10:33:57.370	CHIP			QPADEV0007	161594	NETC	REPTEST	10.2.129.105	sysi26.visionsolutions.com
2019-07-11 10:17:56.896	SQXTEMP2	NETAP	REPTEST	AUDAP1	161601	QCMD	QSYS		sysi26.visionsolutions.com
2019-07-11 10:17:56.696	CHIP			QPADEV0007	161594	NETC	REPTEST	10.2.129.105	sysi26.visionsolutions.com

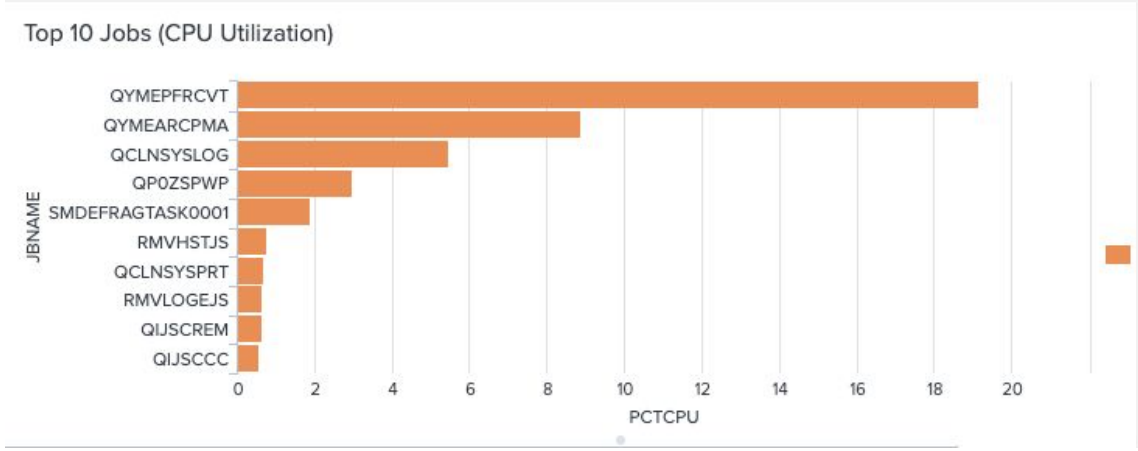
We also need to see performance data…

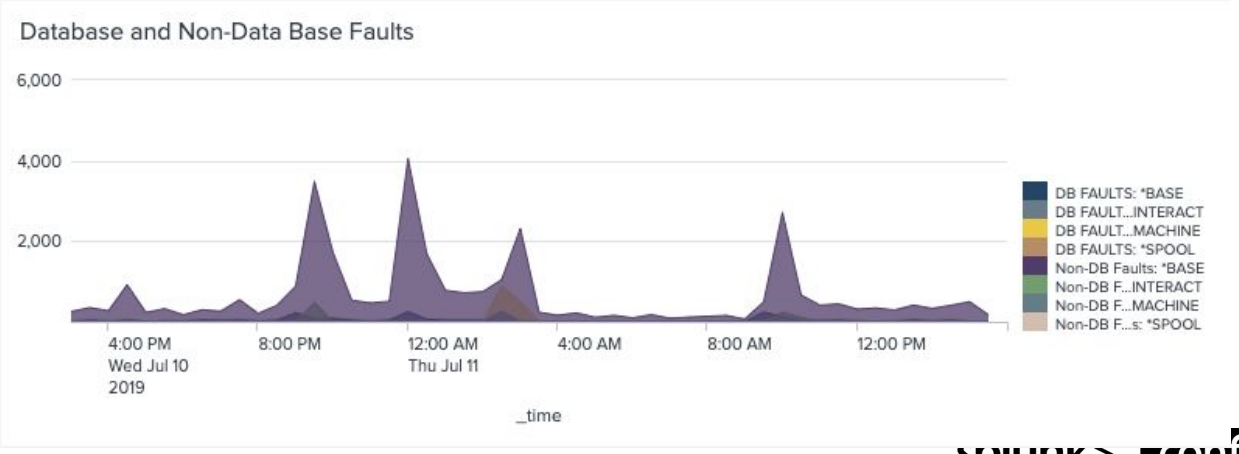
System level summary data

Detailed data from IBM Collection Services from 48 different performance collection files

- CPU
- Disk
- Memory
- Job Performance
- Network Metrics
- More







What are examples of application file monitoring?

- Changes made to files
- Matching before/after field changes
- Anomalies in file field changes
  - Powerful SPL capability to match and note exceptions.


```
index=eview72 JournalName="TESTJRN" ObjectName="PAYROLL"
(EntryType=UP OR EntryType=UB)
| rename SALARY AS "Salary"
| transaction EMPNUM maxspan=30s startswith=(EntryType=UB)
endswith=(EntryType=UP)
| eval befsalary=mvindex(Salary, 0)
| eval aftsalary=mvindex(Salary, 1)
| eval pctchange = round((aftsalary/befsalary*100)-100,0)
| where pctchange > $changepct$
```

Cox Automotive Success Story

splunk> .conf19

Who is Cox Automotive

Cox Automotive is uniquely positioned to transform the way the world buys, sells, owns and uses vehicles. With over 34,000 teammates representing 20+ brands globally.

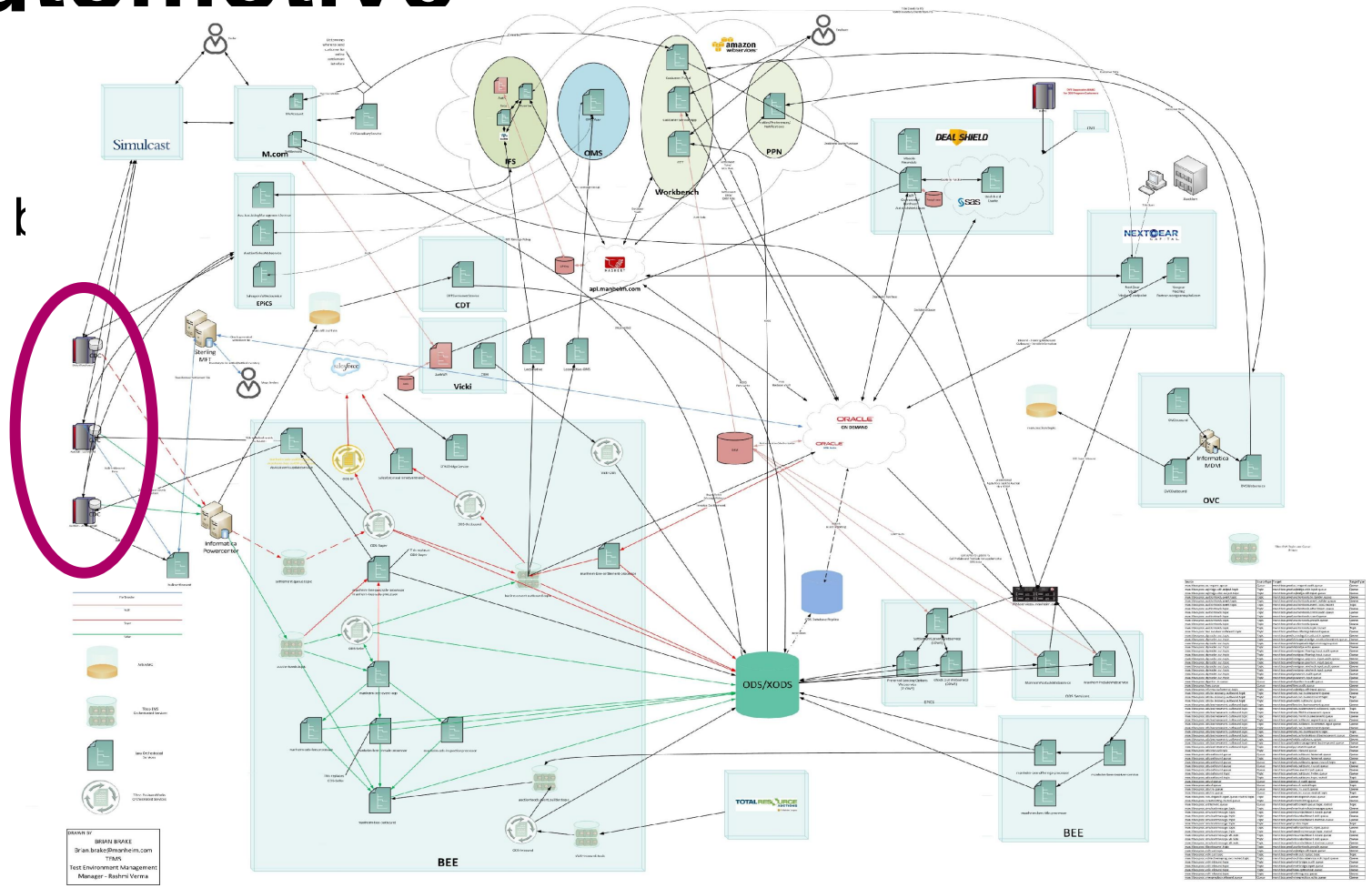
Over 120 IBMi across North America powering Manheim Auctions

Splunk Cloud, IronStream Customer

- Splunk ITSI
- Splunk ES

IBMi and Cox Automotive

- Manheim Auction Vehicles are k
  - Vehicle Check In
  - Reconditioning
  - Condition Reporting
  - Inventory Management
  - Bidding
  - Customer Data



Why IronStream

Move to a more versatile Ops Intelligence Platform

- Simpler Administration
- More control in the hands of the consumer

Integration with IBMi and IT Incident Management/IT Service Intelligence

Cost Savings

How Cox Automotive Uses IronStream

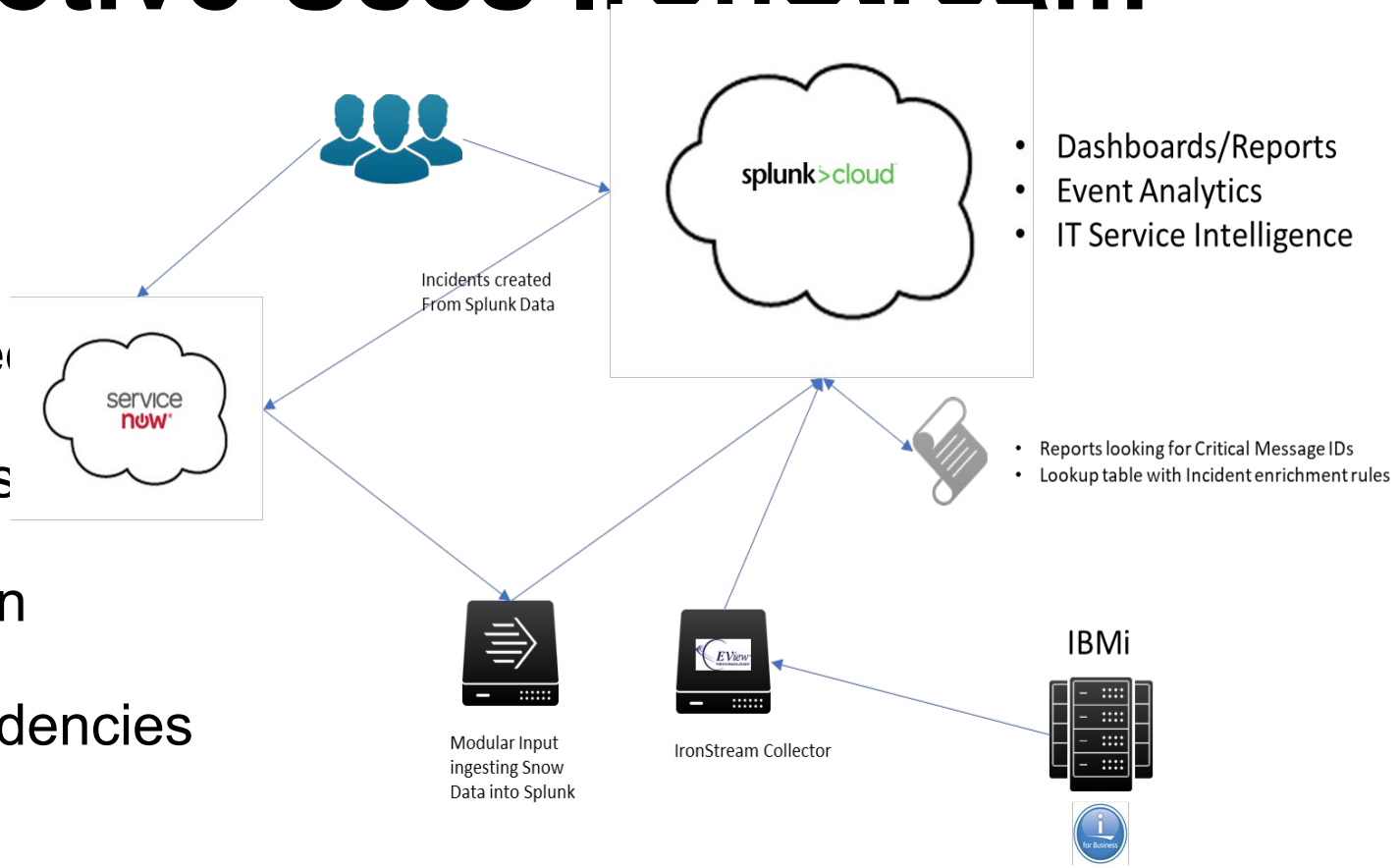
Data Collection Across 120+ IBMi

Data enriched with human knowle

Dashboards/Reports for critical iss

Automated ServiceNow integration

ITSI Services with Auction Dependencies



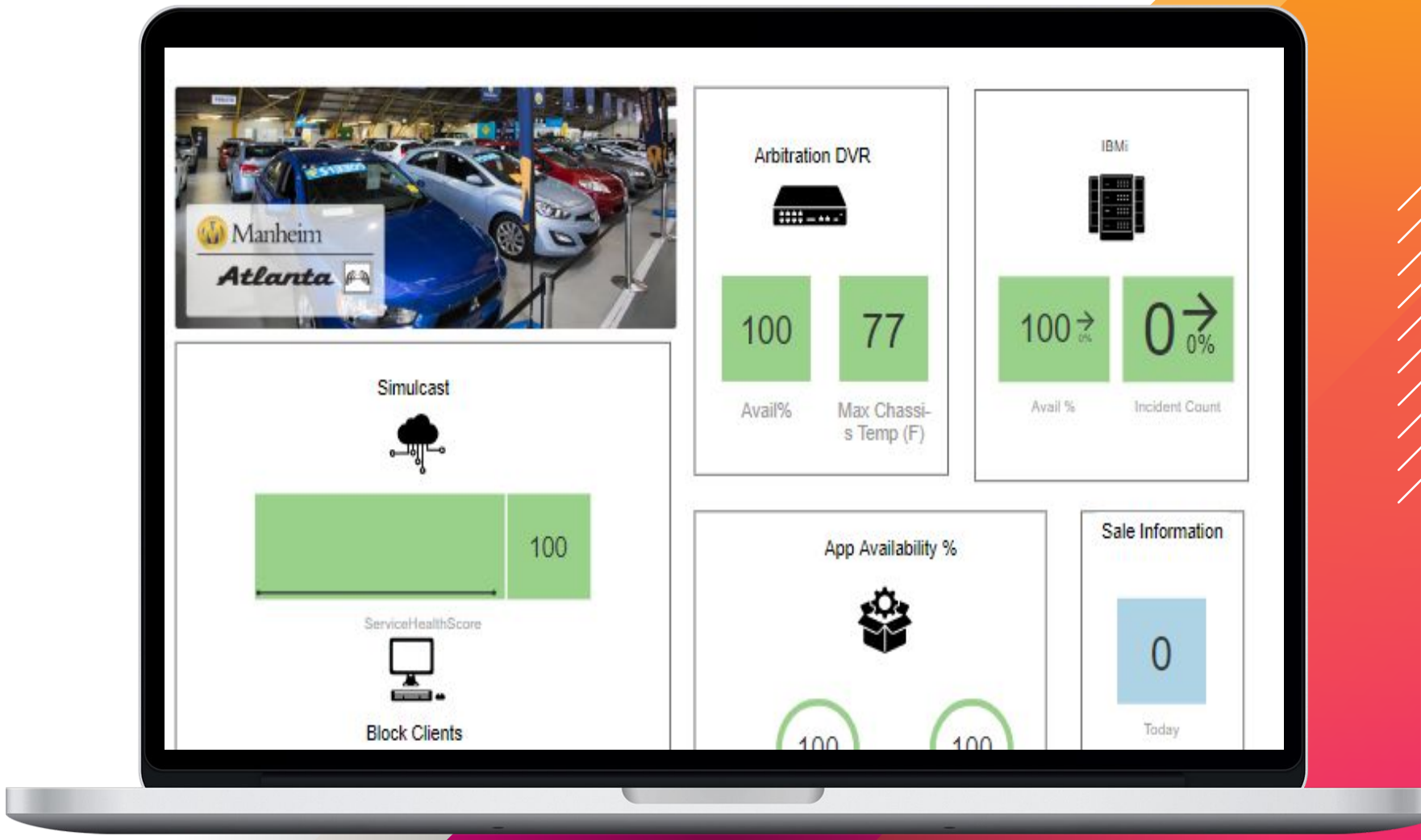
IBMi and Service Intelligence

Seeing the Bigger Picture

Criticality represented in Services

IBMi is no longer a silo

- Correlated with other KPIs and services



The Future

Our work is NEVER done

1. Audit data with Splunk ES
2. Job Level AND System Level Performance
3. Continually Adding KPIs

Q&A

splunk> .conf19

.conf19

splunk>

Thank You !

Go to the .conf19 mobile app to

RATE THIS SESSION