“Splunking” Your z/OS Mainframe Introducing Syncsort Ironstream®

Ed Hallock

Director of Product Management, Syncsort Inc.

.conf2016

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.

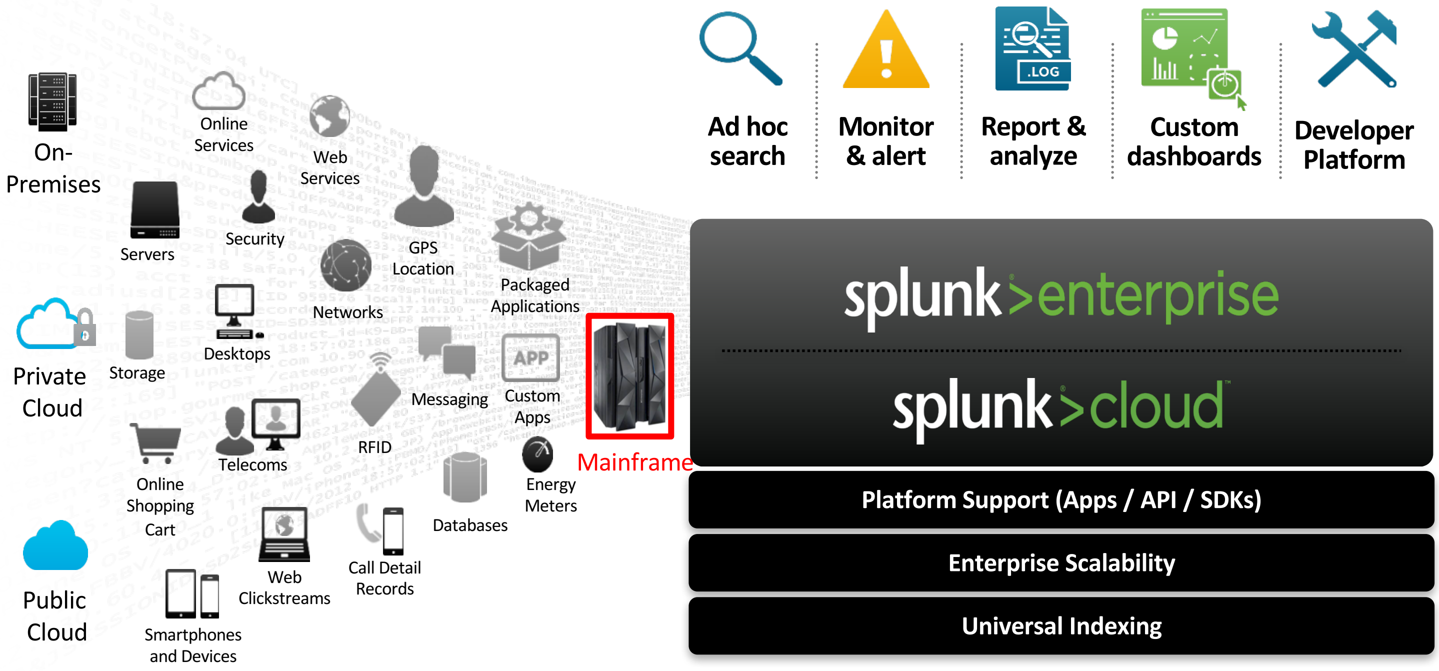
Agenda

- Why “Splunk” Your z/OS Mainframe?
- Challenges with Getting Mainframe Data into Splunk
- Ironstream®: Getting z/OS Mainframe Operational & Security Data Into Splunk
- Ironstream Sample Applications for Operational Analytics and Application Monitoring
- Ironstream for z/OS Security and Integration with Splunk Enterprise Security (ES)
- Ironstream Integration with Splunk IT Service Intelligence (ITSI)
- Conclusion

"Splunking" Your Mainframe Data Into The Industry-Leading Platform For Machine Data

Machine Data: Any Location, Type, Volume

Answer Any Question



On-Premises

Online Services

Web Services

Servers

Security

GPS Location

Packaged Applications

Networks

Private Cloud

Storage

Desktops

Messaging

Custom Apps

Mainframe

RFID

Telecoms

Online Shopping Cart

Energy Meters

Databases

Public Cloud

Web Clickstreams

Call Detail Records

Smartphones and Devices

Ad hoc search

Monitor & alert

Report & analyze

Custom dashboards

Developer Platform

splunk>enterprise

splunk>cloud

Platform Support (Apps / API / SDKs)

Enterprise Scalability

Universal Indexing

Why Splunk Your Mainframe?
Because Mainframes Still Host the Most Critical Applications

71%
Fortune 500

2.5 Billion
Bus. Transactions / day / per MF

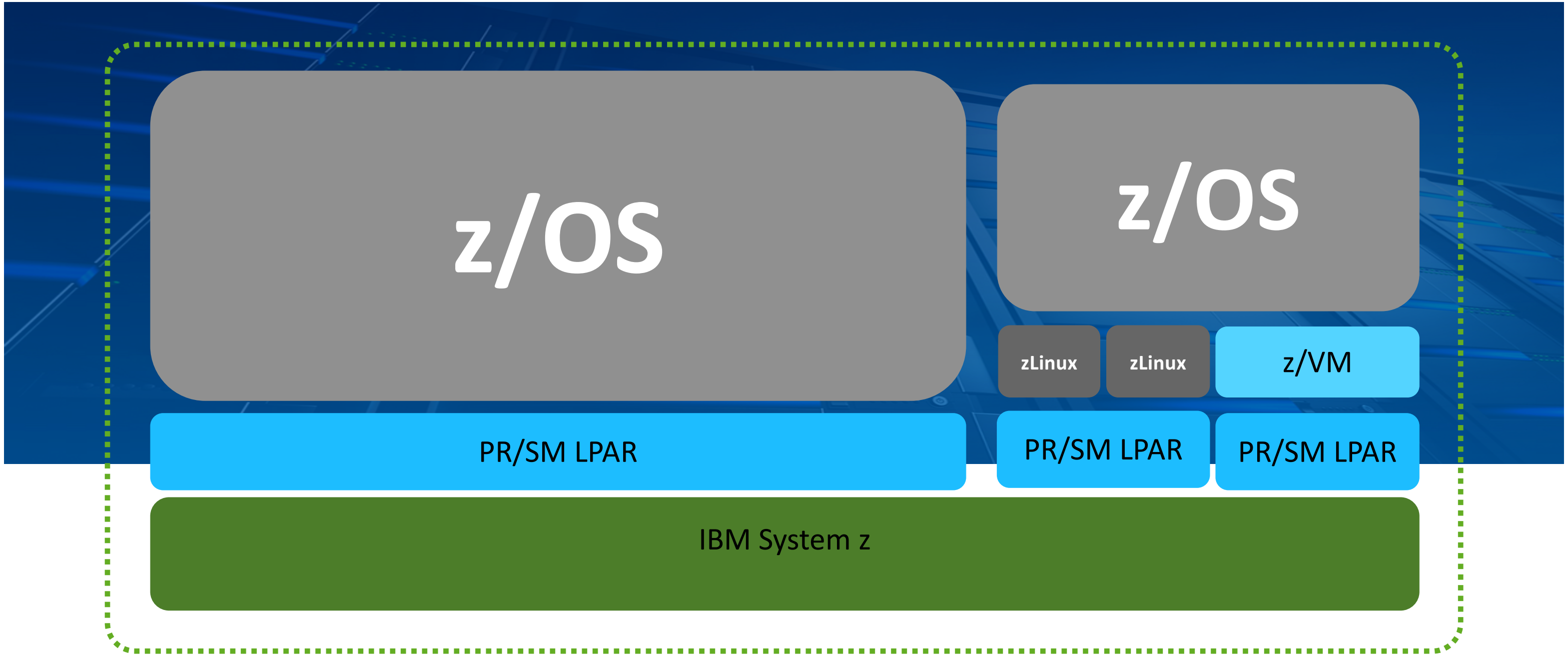
92 Top World Banks

10 of World's Top Insurers

23 of Top 25 US Retailers

Source: IBM

IBM System z and z/OS 101

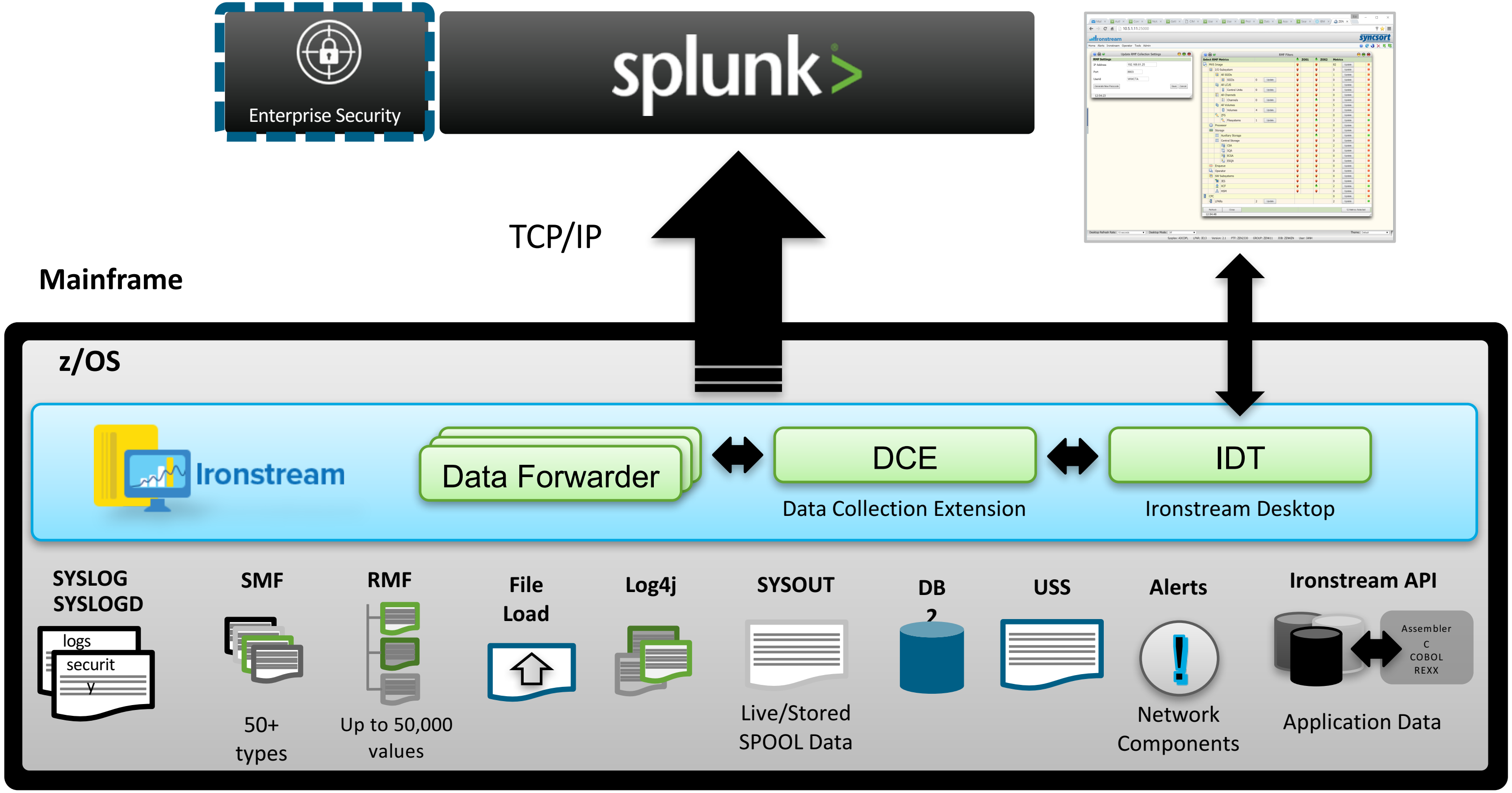


*Note - z/Linux is NOT z/OS

Challenges with Getting Mainframe Data Into Splunk

- Integration
  - Data Conversion: EBCDIC to ASCII; Binary to readable
  - Complex mainframe data structures: SMF Data
- Security
  - Hosts mission critical sensitive data making it difficult to access
- Cost
  - Processing on the mainframe costs CPU cycles (MIPS) – including data transmission (TCP, FTP, etc.)
  - Cannot interfere with system throughput
- Operational
  - Log file migration can be complex
  - Tracking delta from log files difficult, if not possible
  - Getting data in real time/near real time is complex

Ironstream: Getting z/OS Mainframe Operational & Security Data Into Splunk



Enterprise Security

splunk>

TCP/IP

Mainframe

z/OS

Ironstream

Data Forwarder

DCE

Data Collection Extension

IDT

Ironstream Desktop

SYSLOG
SYSLOGD

logs
securit
y

SMF

50+
types

RMF

Up to 50,000
values

File
Load

Log4j

SYSOUT

Live/Stored
SPOOL Data

DB
2

USS

Alerts

Network
Components

Ironstream API

Assembler
C
COBOL
REXX

Application Data

Ironstream Architectural Considerations

Ultra Light Weight

- Minimal MIPS impact even for billions of SMF records

Non-intrusive

- Collect data from critical system
- Zero impact to throughput

Fast

- Collect data in real time

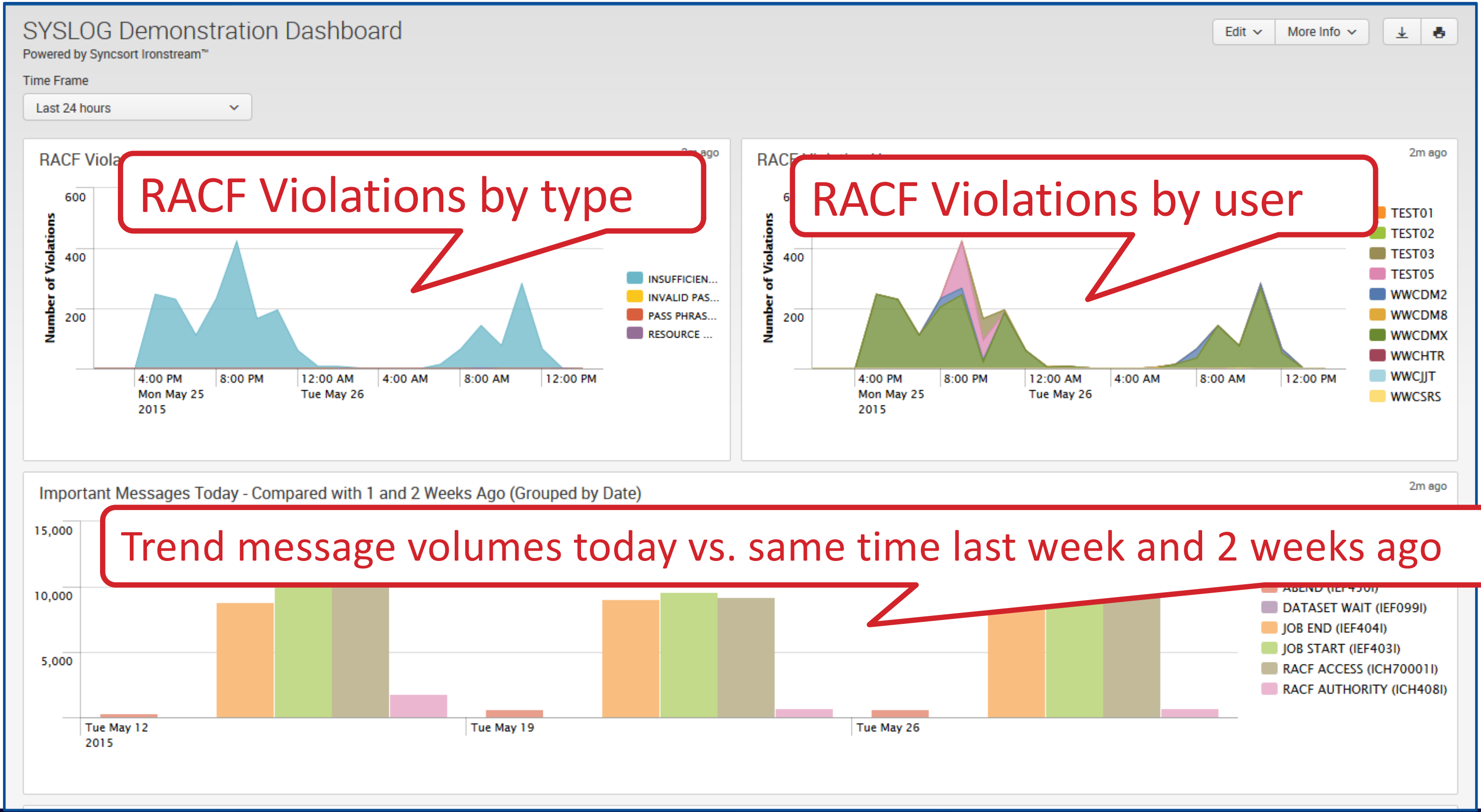
Secure and Reliable

- Error recovery
- Security
- Load balancing

Sample Mainframe Log Data That Can Be "Splunked"

	Mainframe Application	Related Mainframe Logs
Operational Analytics	Operator logs for DB2, CICS, IMS, etc	Syslog
Application Monitoring	DB2 Accounting Records	SMF Type 101
	CICS Accounting Records	SMF Type 110
	WebSphere	Log4j
	Job / Step Accounting Records	SMF Type 30
Security & Compliance	RACF	SMF Type 80
	Intrusion Detection	SyslogD

Operational Analytics: RACF Violations and Message Trends
Data Source: SYSLOG



SYSLOG Demonstration Dashboard

Powered by Syncsort Ironstream™

Time Frame

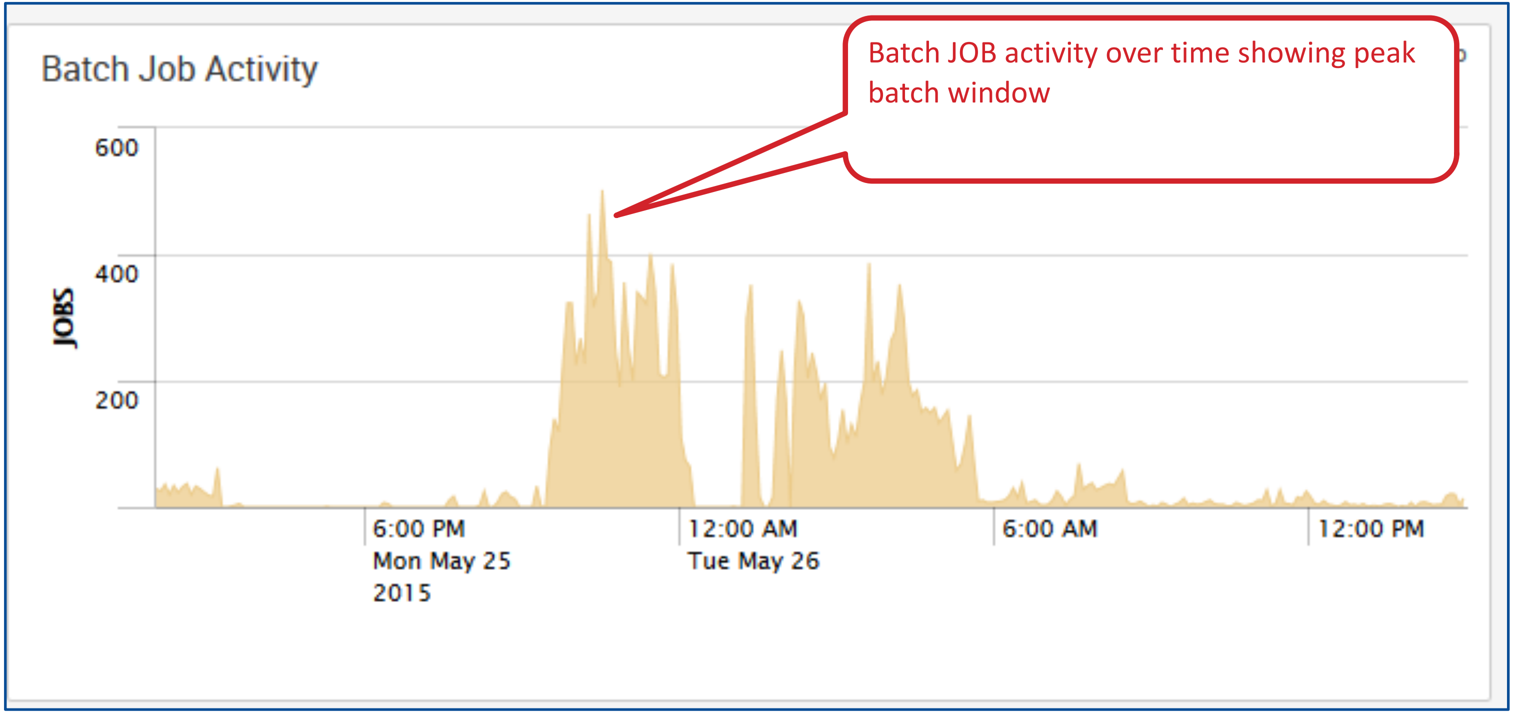
Last 24 hours

RACF Violations by type

RACF Violations by user

Trend message volumes today vs. same time last week and 2 weeks ago

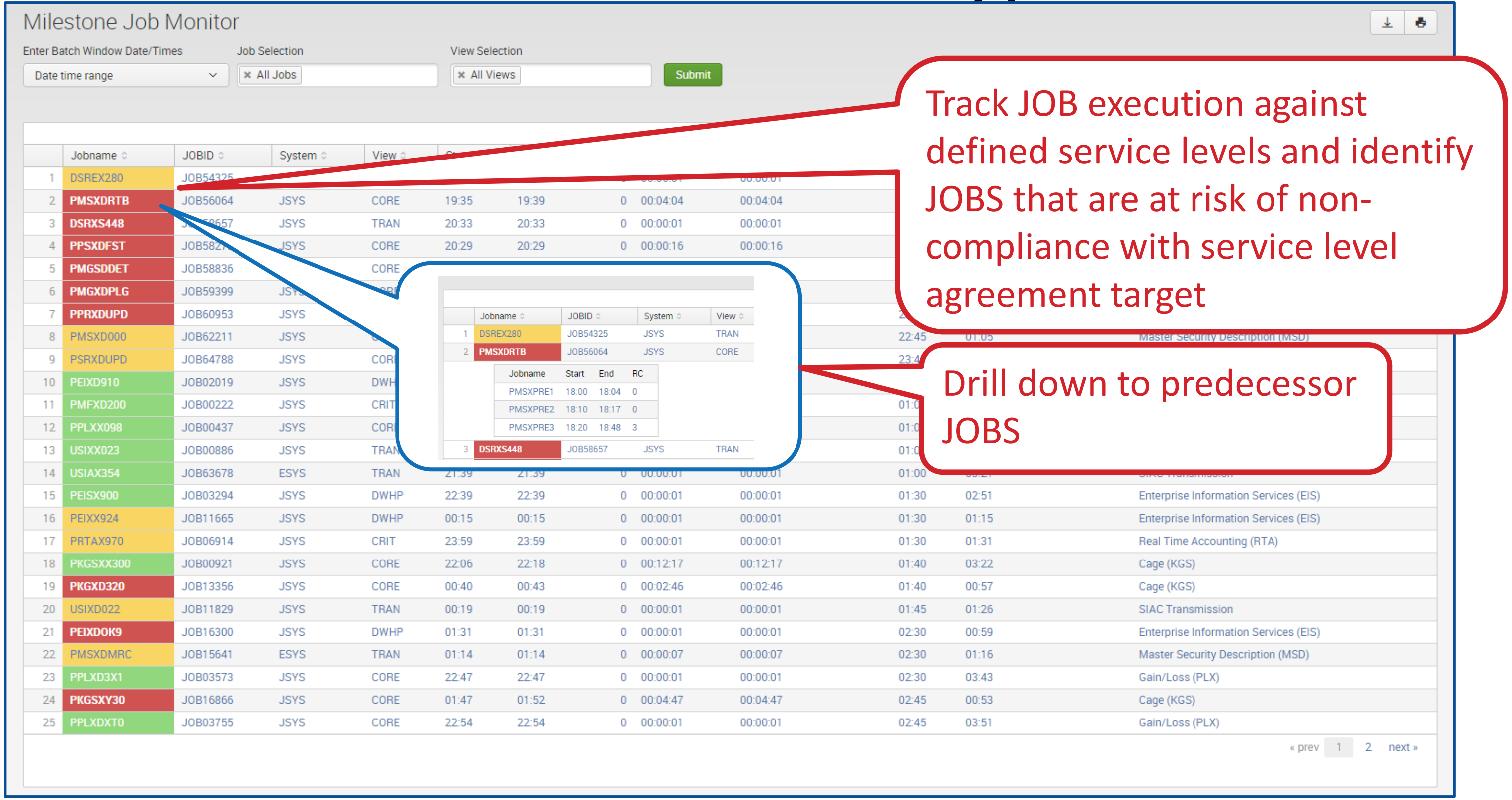
Operational Analytics: Batch Job Activity Data Source: SYSLOG



Batch JOB activity over time showing peak batch window

Operational Analytics: Job Monitor for SLA Tracking

Data Source: SMF Type 30



Milestone Job Monitor

Enter Batch Window Date/Times: Date time range

Job Selection: × All Jobs

View Selection: × All Views

	Jobname	JOBID	System	View	St							
1	DSREX280	JOB54325					0	00:00:01	00:00:01			
2	PMSXDRTB	JOB56064	JSYS	CORE	19:35	19:39	0	00:04:04	00:04:04			
3	DSRXS448	JOB58657	JSYS	TRAN	20:33	20:33	0	00:00:01	00:00:01			
4	PPSXDFST	JOB582	JSYS	CORE	20:29	20:29	0	00:00:16	00:00:16			
5	PMGSDDET	JOB58836		CORE								
6	PMGXDPLG	JOB59399	JSYS									
7	PPRXDUPD	JOB60953	JSYS									
8	PMSXD000	JOB62211	JSYS							22:45	01:05	Master Security Description (MSD)
9	PSRXDUPD	JOB64788	JSYS	CORE						23:4		
10	PEIXD910	JOB02019	JSYS	DWH								
11	PMFXD200	JOB00222	JSYS	CRIT						01:0		
12	PPLXX098	JOB00437	JSYS	CORE						01:0		
13	USIXX023	JOB00886	JSYS	TRAN						01:0		
14	USIAX354	JOB63678	ESYS	TRAN	21:39	21:39	0	00:00:01	00:00:01	01:00	03:21	SIAC Transmission
15	PEISX900	JOB03294	JSYS	DWHP	22:39	22:39	0	00:00:01	00:00:01	01:30	02:51	Enterprise Information Services (EIS)
16	PEIXX924	JOB11665	JSYS	DWHP	00:15	00:15	0	00:00:01	00:00:01	01:30	01:15	Enterprise Information Services (EIS)
17	PRTAX970	JOB06914	JSYS	CRIT	23:59	23:59	0	00:00:01	00:00:01	01:30	01:31	Real Time Accounting (RTA)
18	PKGSXX300	JOB00921	JSYS	CORE	22:06	22:18	0	00:12:17	00:12:17	01:40	03:22	Cage (KGS)
19	PKGXD320	JOB13356	JSYS	CORE	00:40	00:43	0	00:02:46	00:02:46	01:40	00:57	Cage (KGS)
20	USIXD022	JOB11829	JSYS	TRAN	00:19	00:19	0	00:00:01	00:00:01	01:45	01:26	SIAC Transmission
21	PEIXDOK9	JOB16300	JSYS	DWHP	01:31	01:31	0	00:00:01	00:00:01	02:30	00:59	Enterprise Information Services (EIS)
22	PMSXDMRC	JOB15641	ESYS	TRAN	01:14	01:14	0	00:00:07	00:00:07	02:30	01:16	Master Security Description (MSD)
23	PPLXD3X1	JOB03573	JSYS	CORE	22:47	22:47	0	00:00:01	00:00:01	02:30	03:43	Gain/Loss (PLX)
24	PKGSXY30	JOB16866	JSYS	CORE	01:47	01:52	0	00:04:47	00:04:47	02:45	00:53	Cage (KGS)
25	PPLXDXT0	JOB03755	JSYS	CORE	22:54	22:54	0	00:00:01	00:00:01	02:45	03:51	Gain/Loss (PLX)

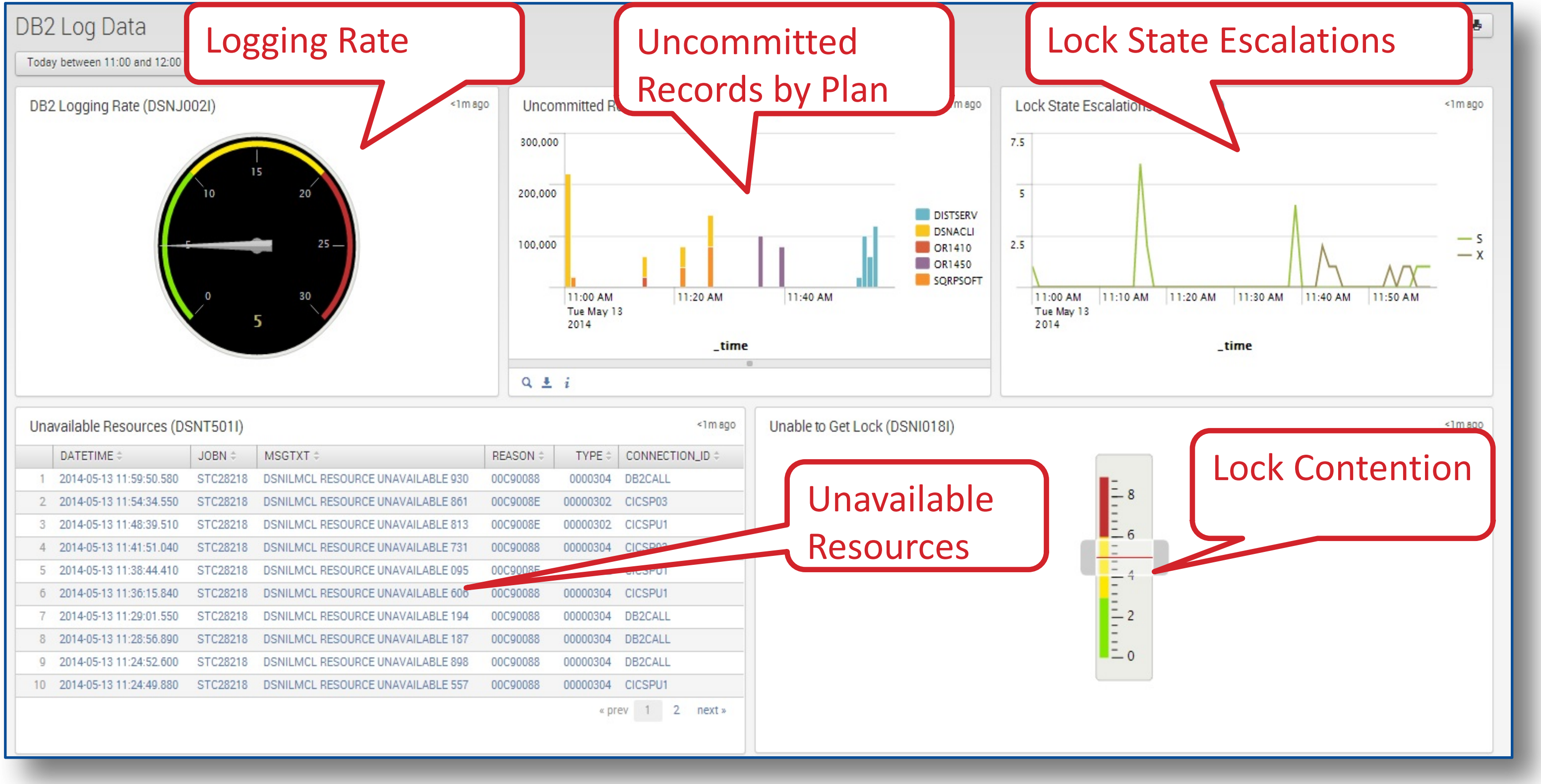
	Jobname	JOBID	System	View
1	DSREX280	JOB54325	JSYS	TRAN
2	PMSXDRTB	JOB56064	JSYS	CORE
3	DSRXS448	JOB58657	JSYS	TRAN

Jobname	Start	End	RC
PMSXPRE1	18:00	18:04	0
PMSXPRE2	18:10	18:17	0
PMSXPRE3	18:20	18:48	3

Track JOB execution against defined service levels and identify JOBS that are at risk of non-compliance with service level agreement target

Drill down to predecessor JOBS

Application Monitoring: DB2 Performance
Data Source: SMF Type 100, 101, 102



Logging Rate

Uncommitted Records by Plan

Lock State Escalations

Unavailable Resources (DSNT501I)

<1m ago

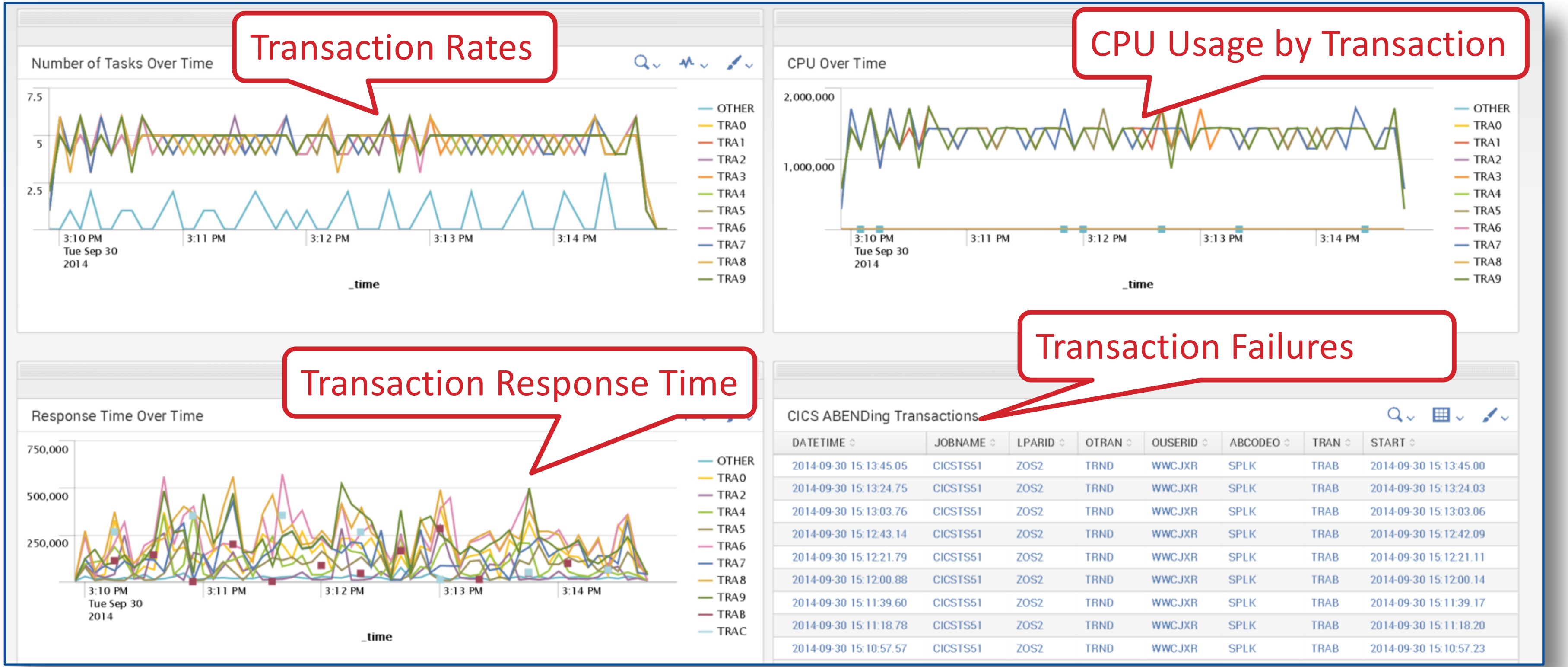
	DATETIME	JOBN	MSGTXT	REASON	TYPE	CONNECTION_ID
1	2014-05-13 11:59:50.580	STC28218	DSNILMCL RESOURCE UNAVAILABLE 930	00C90088	0000304	DB2CALL
2	2014-05-13 11:54:34.550	STC28218	DSNILMCL RESOURCE UNAVAILABLE 861	00C9008E	00000302	CICSP03
3	2014-05-13 11:48:39.510	STC28218	DSNILMCL RESOURCE UNAVAILABLE 813	00C9008E	00000302	CICSPU1
4	2014-05-13 11:41:51.040	STC28218	DSNILMCL RESOURCE UNAVAILABLE 731	00C90088	00000304	CICSP03
5	2014-05-13 11:38:44.410	STC28218	DSNILMCL RESOURCE UNAVAILABLE 095	00C9008E	[illegible]	CICSPU1
6	2014-05-13 11:36:15.840	STC28218	DSNILMCL RESOURCE UNAVAILABLE 606	00C90088	00000304	CICSPU1
7	2014-05-13 11:29:01.550	STC28218	DSNILMCL RESOURCE UNAVAILABLE 194	00C90088	00000304	DB2CALL
8	2014-05-13 11:28:56.890	STC28218	DSNILMCL RESOURCE UNAVAILABLE 187	00C90088	00000304	DB2CALL
9	2014-05-13 11:24:52.600	STC28218	DSNILMCL RESOURCE UNAVAILABLE 898	00C90088	00000304	DB2CALL
10	2014-05-13 11:24:49.880	STC28218	DSNILMCL RESOURCE UNAVAILABLE 557	00C90088	00000304	CICSPU1

« prev 1 2 next »

Unavailable Resources

Lock Contention

Application Monitoring: CICS Transaction Analysis
Data Source: SMF Type 110



Transaction Rates

CPU Usage by Transaction

Transaction Response Time

Transaction Failures

CICS ABENDing Transactions

DATETIME	JOBNAME	LPARID	OTRAN	OUSERID	ABCODEO	TRAN	START
2014-09-30 15:13:45.05	CICSTS51	ZOS2	TRND	WWCJXR	SPLK	TRAB	2014-09-30 15:13:45.00
2014-09-30 15:13:24.75	CICSTS51	ZOS2	TRND	WWCJXR	SPLK	TRAB	2014-09-30 15:13:24.03
2014-09-30 15:13:03.76	CICSTS51	ZOS2	TRND	WWCJXR	SPLK	TRAB	2014-09-30 15:13:03.06
2014-09-30 15:12:43.14	CICSTS51	ZOS2	TRND	WWCJXR	SPLK	TRAB	2014-09-30 15:12:42.09
2014-09-30 15:12:21.79	CICSTS51	ZOS2	TRND	WWCJXR	SPLK	TRAB	2014-09-30 15:12:21.11
2014-09-30 15:12:00.88	CICSTS51	ZOS2	TRND	WWCJXR	SPLK	TRAB	2014-09-30 15:12:00.14
2014-09-30 15:11:39.60	CICSTS51	ZOS2	TRND	WWCJXR	SPLK	TRAB	2014-09-30 15:11:39.17
2014-09-30 15:11:18.78	CICSTS51	ZOS2	TRND	WWCJXR	SPLK	TRAB	2014-09-30 15:11:18.20
2014-09-30 15:10:57.57	CICSTS51	ZOS2	TRND	WWCJXR	SPLK	TRAB	2014-09-30 15:10:57.23

Ironstream z/OS Security & Splunk Enterprise Security

.conf2016

splunk>

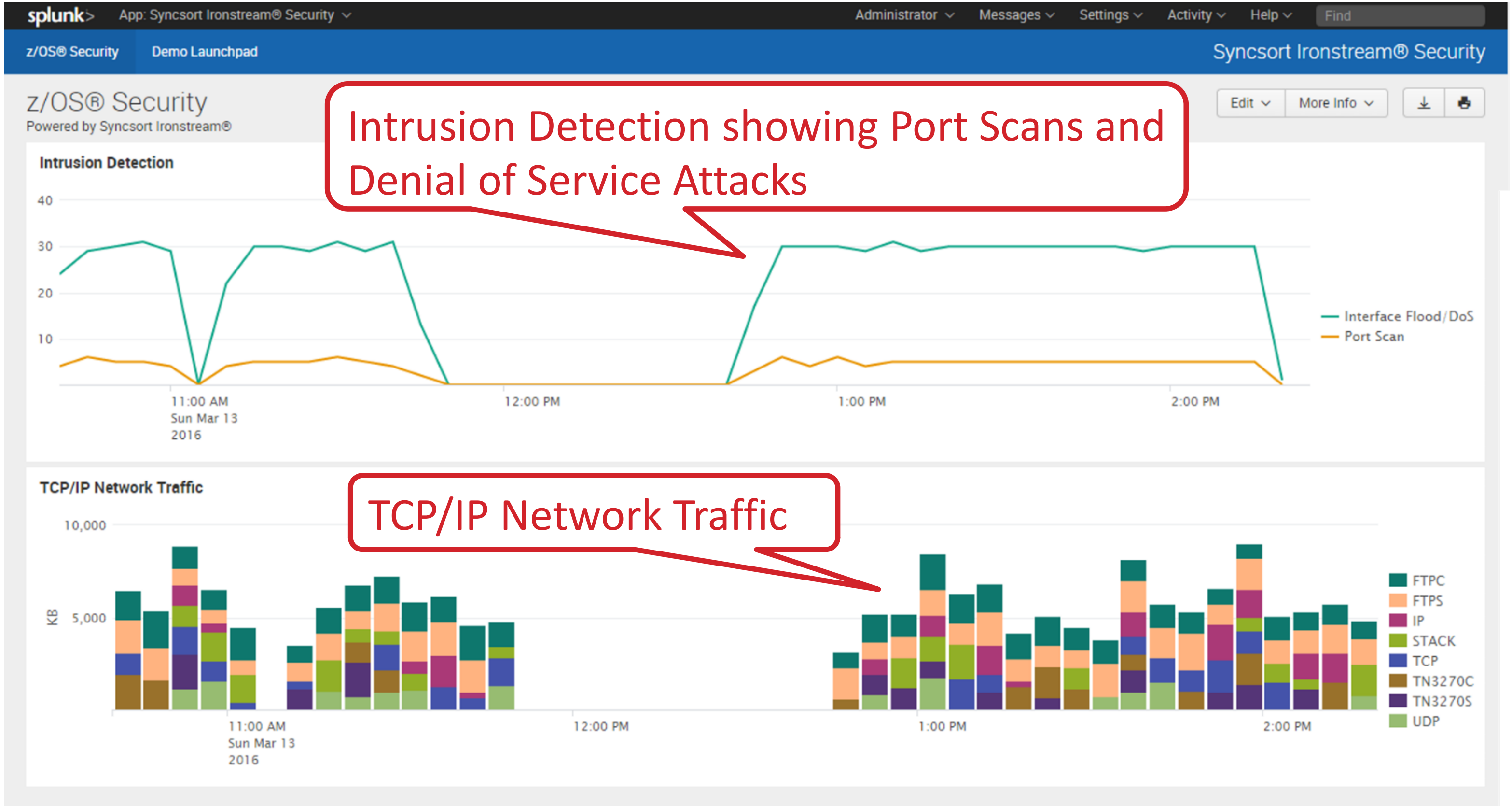
Critical z/OS Security Data Sources Collected via Ironstream

- Intrusion Detection (port scans, floods/DoS attacks, malformed data packets)
  - z/OS Traffic Regulation Management Daemon (TRMD)
  - SYSLOGD
  - Network Management Component
- TSO logon tracking
  - SMF30
- TSO account change activity
  - SMF80
- FTP authentications
  - SYSLOGD
  - Network Management Component
- FTP file change analysis
  - SMF119
- IP traffic analysis
  - SMF119
- Network events
  - Network Management Component

Ironstream z/OS Security App

- All data sources collected by Ironstream are exposed in an application focused on z/OS security only
- This app shows z/OS mainframe security data and is NOT an enterprise-wide integrated view

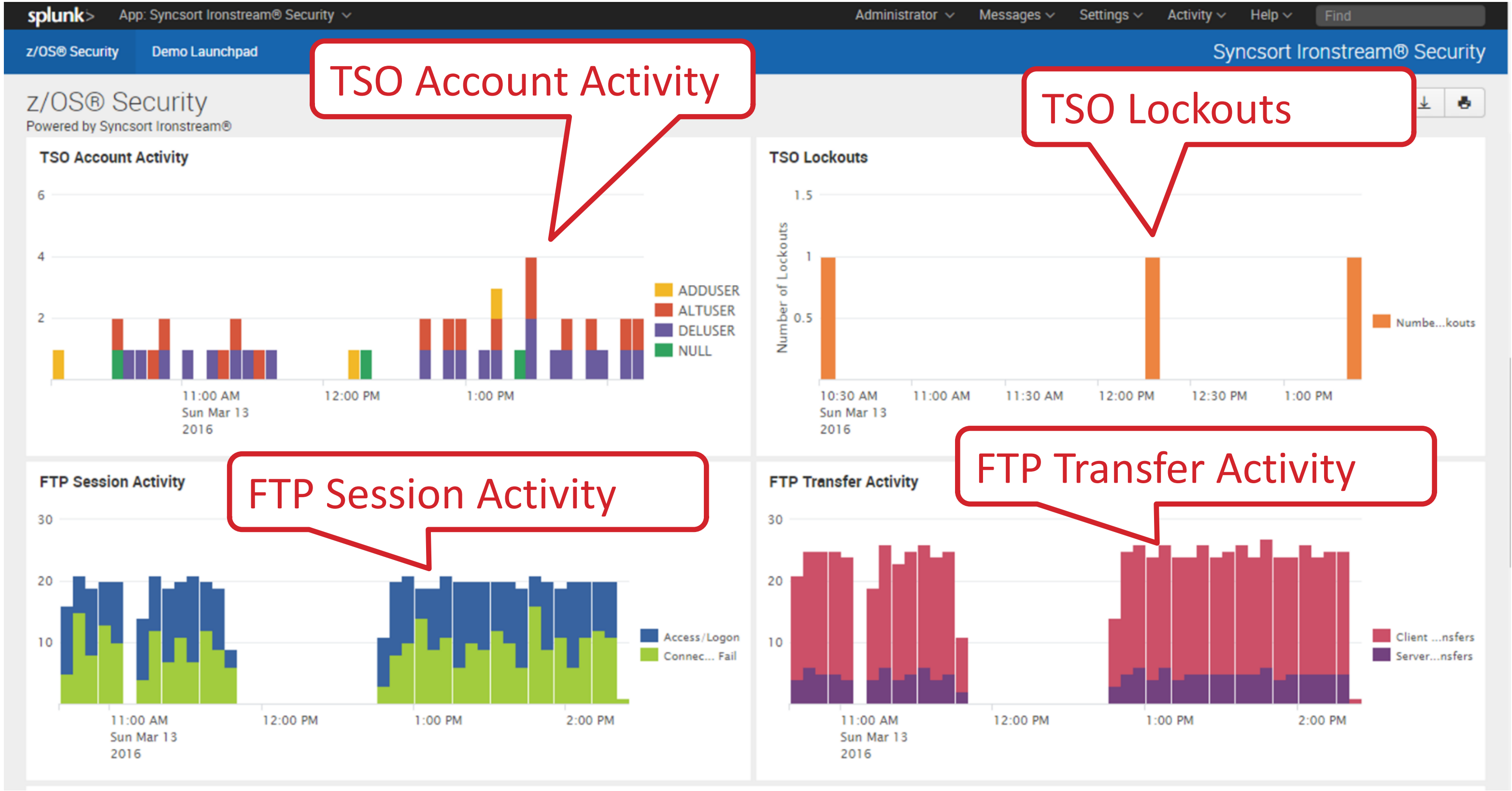
z/OS Security Dashboard



Intrusion Detection showing Port Scans and Denial of Service Attacks

TCP/IP Network Traffic

z/OS Security Dashboard



TSO Account Activity

TSO Lockouts

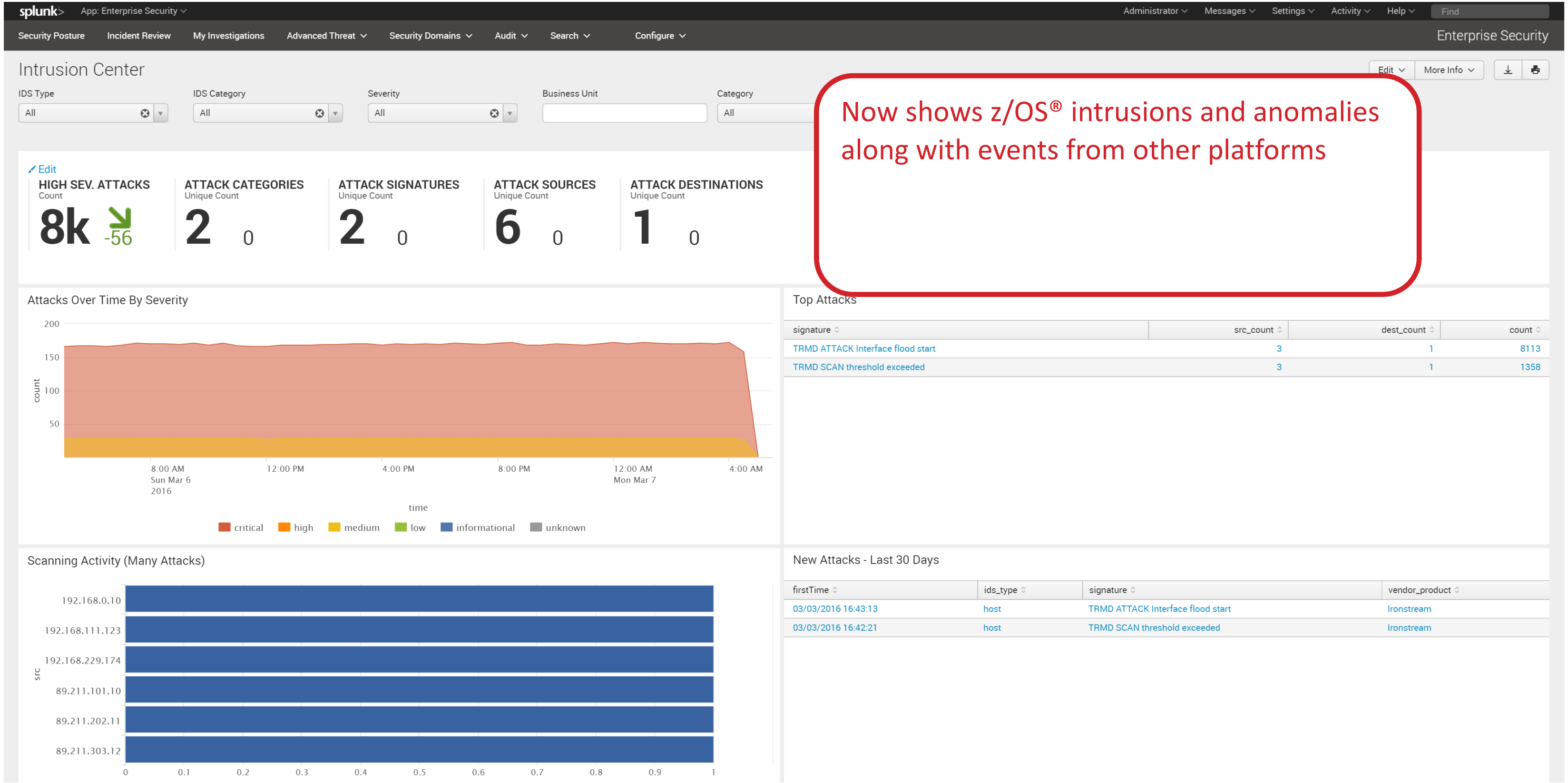
FTP Session Activity

FTP Transfer Activity

Ironstream + Splunk Enterprise Security App

- All collected data sources can also be mapped to Splunk CIM for Enterprise Security and automatically exposed in ES dashboards along with security information from other platforms
  - Requires the Ironstream TA for Splunk Enterprise Security to be installed
  - Provides an enterprise-wide, integrated view of security across all platforms via ES dashboards provided by Splunk

Sample Intrusion Center Dashboard With Splunk Enterprise Security™



Intrusion Center

IDS Type	IDS Category	Severity	Business Unit	Category
All	All	All		All

✎ Edit

HIGH SEV. ATTACKS Count	ATTACK CATEGORIES Unique Count	ATTACK SIGNATURES Unique Count	ATTACK SOURCES Unique Count	ATTACK DESTINATIONS Unique Count
8k ↘ -56	2 0	2 0	6 0	1 0

Top Attacks

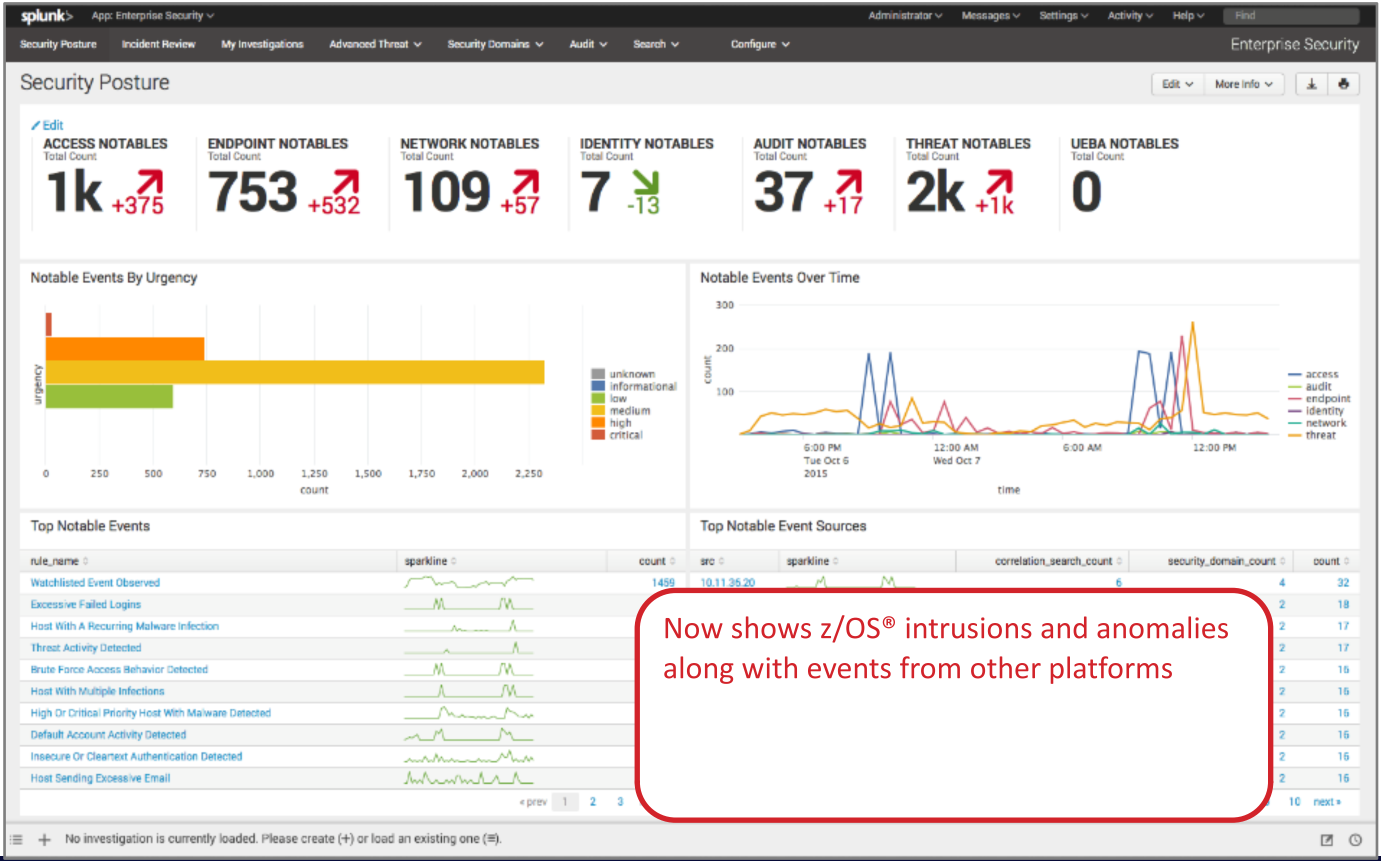
signature	src_count	dest_count	count
TRMD ATTACK Interface flood start	3	1	8113
TRMD SCAN threshold exceeded	3	1	1358

New Attacks - Last 30 Days

firstTime	ids_type	signature	vendor_product
03/03/2016 16:43:13	host	TRMD ATTACK Interface flood start	Ironstream
03/03/2016 16:42:21	host	TRMD SCAN threshold exceeded	Ironstream

Now shows z/OS® intrusions and anomalies along with events from other platforms

Sample Security Posture Dashboard With Splunk Enterprise Security™



Security Posture

Edit

ACCESS NOTABLES Total Count	ENDPOINT NOTABLES Total Count	NETWORK NOTABLES Total Count	IDENTITY NOTABLES Total Count	AUDIT NOTABLES Total Count	THREAT NOTABLES Total Count	UEBA NOTABLES Total Count
1k +375	753 +532	109 +57	7 -13	37 +17	2k +1k	0

Top Notable Events

rule_name	sparkline	count
Watchlisted Event Observed		1459
Excessive Failed Logins		
Host With A Recurring Malware Infection		
Threat Activity Detected		
Brute Force Access Behavior Detected		
Host With Multiple Infections		
High Or Critical Priority Host With Malware Detected		
Default Account Activity Detected		
Insecure Or Cleartext Authentication Detected		
Host Sending Excessive Email		

« prev 1 2 3

Top Notable Event Sources

src	sparkline	correlation_search_count	security_domain_count	count
10.11.36.20		6	4	32
			2	18
			2	17
			2	17
			2	16
			2	16
			2	16
			2	16
			2	16
			2	16

10 next »

No investigation is currently loaded. Please create (+) or load an existing one (≡).

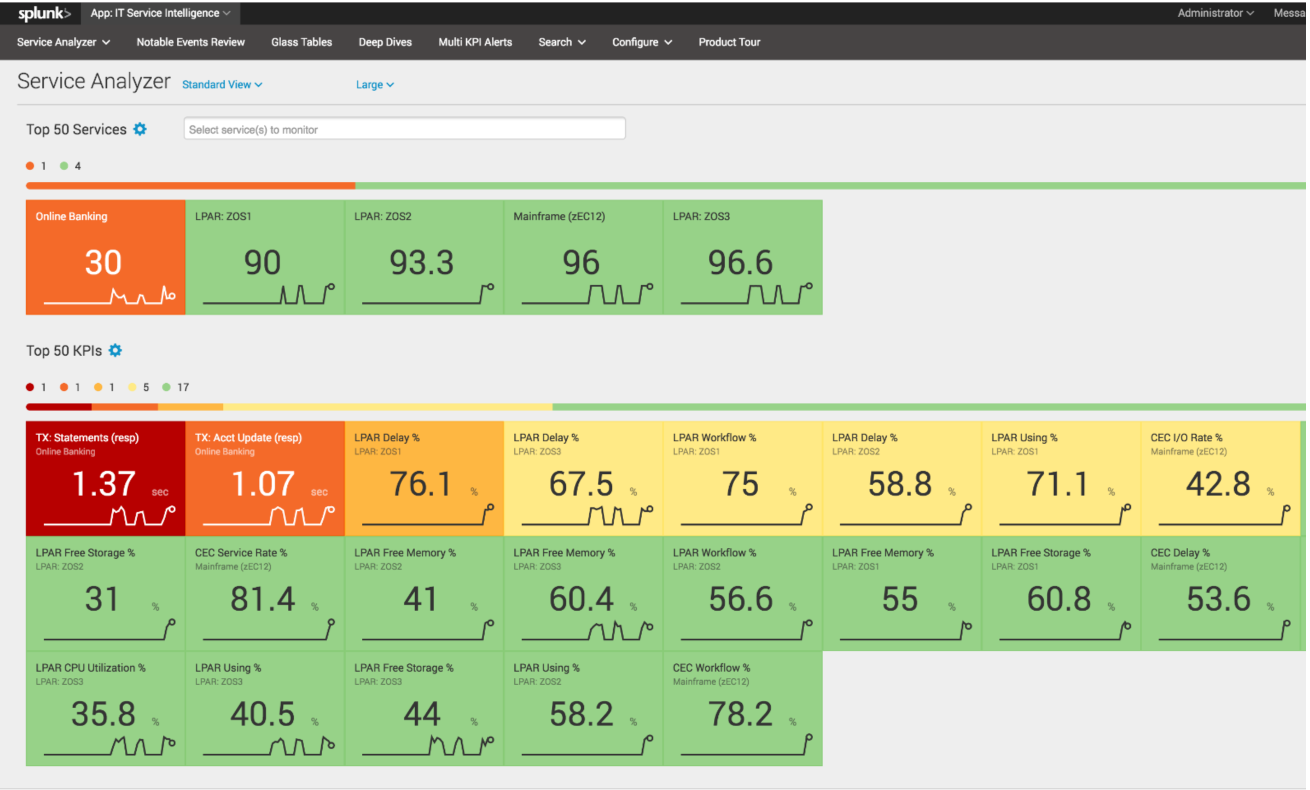
Now shows z/OS® intrusions and anomalies along with events from other platforms

Ironstream Integration with ITSI

.conf2016

splunk>

Ironstream Integration with ITSI



Service Analyzer

Top 50 Services

● 1 ● 4

Online Banking	LPAR: ZOS1	LPAR: ZOS2	Mainframe (zEC12)	LPAR: ZOS3
30	90	93.3	96	96.6

Top 50 KPIs

● 1 ● 1 ● 1 ● 5 ● 17

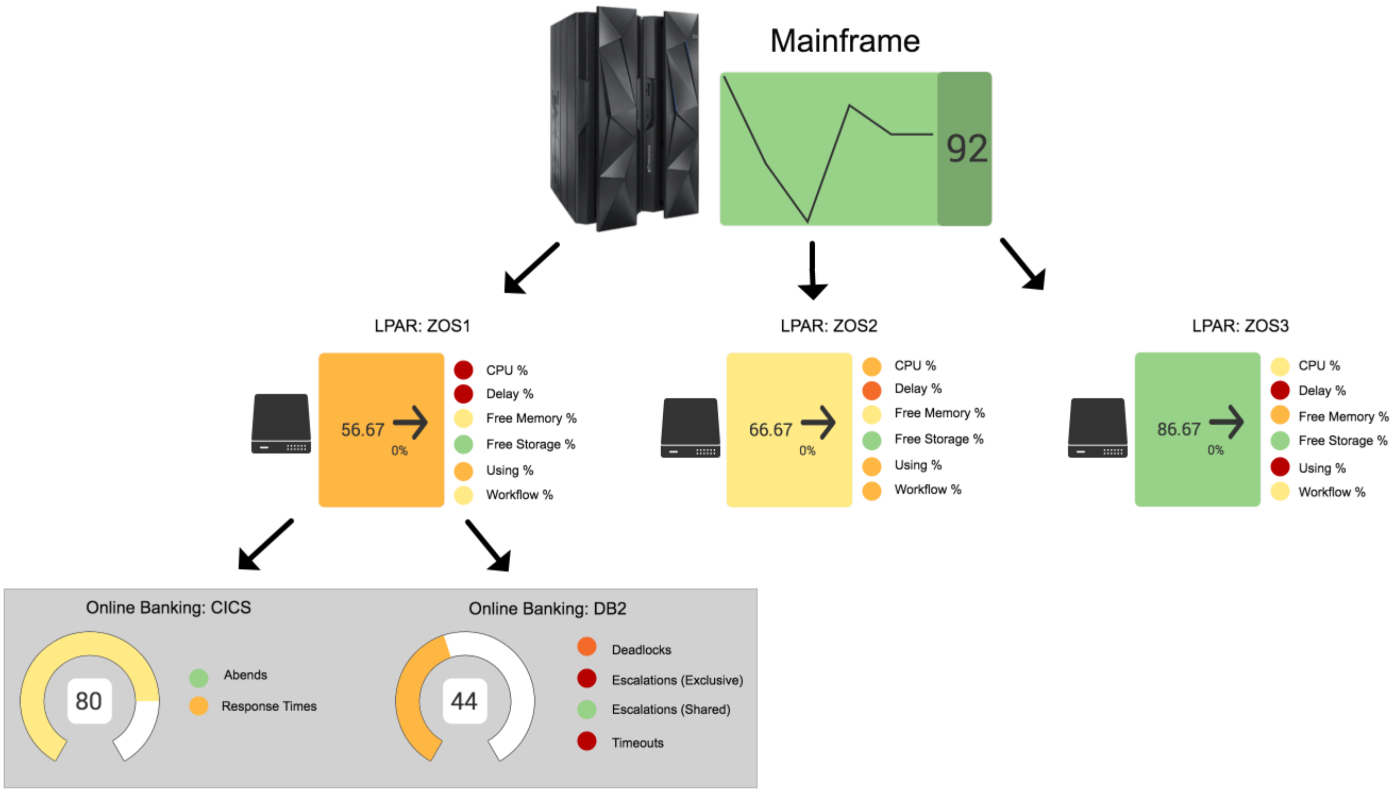
TX: Statements (resp) Online Banking 1.37 sec	TX: Acct Update (resp) Online Banking 1.07 sec	LPAR Delay % LPAR: ZOS1 76.1 %	LPAR Delay % LPAR: ZOS3 67.5 %	LPAR Workflow % LPAR: ZOS1 75 %	LPAR Delay % LPAR: ZOS2 58.8 %	LPAR Using % LPAR: ZOS1 71.1 %	CEC I/O Rate % Mainframe (zEC12) 42.8 %
LPAR Free Storage % LPAR: ZOS2 31 %	CEC Service Rate % Mainframe (zEC12) 81.4 %	LPAR Free Memory % LPAR: ZOS2 41 %	LPAR Free Memory % LPAR: ZOS3 60.4 %	LPAR Workflow % LPAR: ZOS2 56.6 %	LPAR Free Memory % LPAR: ZOS1 55 %	LPAR Free Storage % LPAR: ZOS1 60.8 %	CEC Delay % Mainframe (zEC12) 53.6 %
LPAR CPU Utilization % LPAR: ZOS3 35.8 %	LPAR Using % LPAR: ZOS3 40.5 %	LPAR Free Storage % LPAR: ZOS3 44 %	LPAR Using % LPAR: ZOS2 58.2 %	CEC Workflow % Mainframe (zEC12) 78.2 %			

KPIs provided for mainframe systems in Service Analyzer

- CEC (Central Electronic Complex), i.e. “the box”
- LPARs (logical partitions)
- Critical services

Glass Tables for visualization

Ironstream Integration with ITSI



Mainframe

92

LPAR: ZOS1

56.67

0%

CPU %

Delay %

Free Memory %

Free Storage %

Using %

Workflow %

LPAR: ZOS2

66.67

0%

CPU %

Delay %

Free Memory %

Free Storage %

Using %

Workflow %

LPAR: ZOS3

86.67

0%

CPU %

Delay %

Free Memory %

Free Storage %

Using %

Workflow %

Online Banking: CICS

80

Abends

Response Times

Online Banking: DB2

44

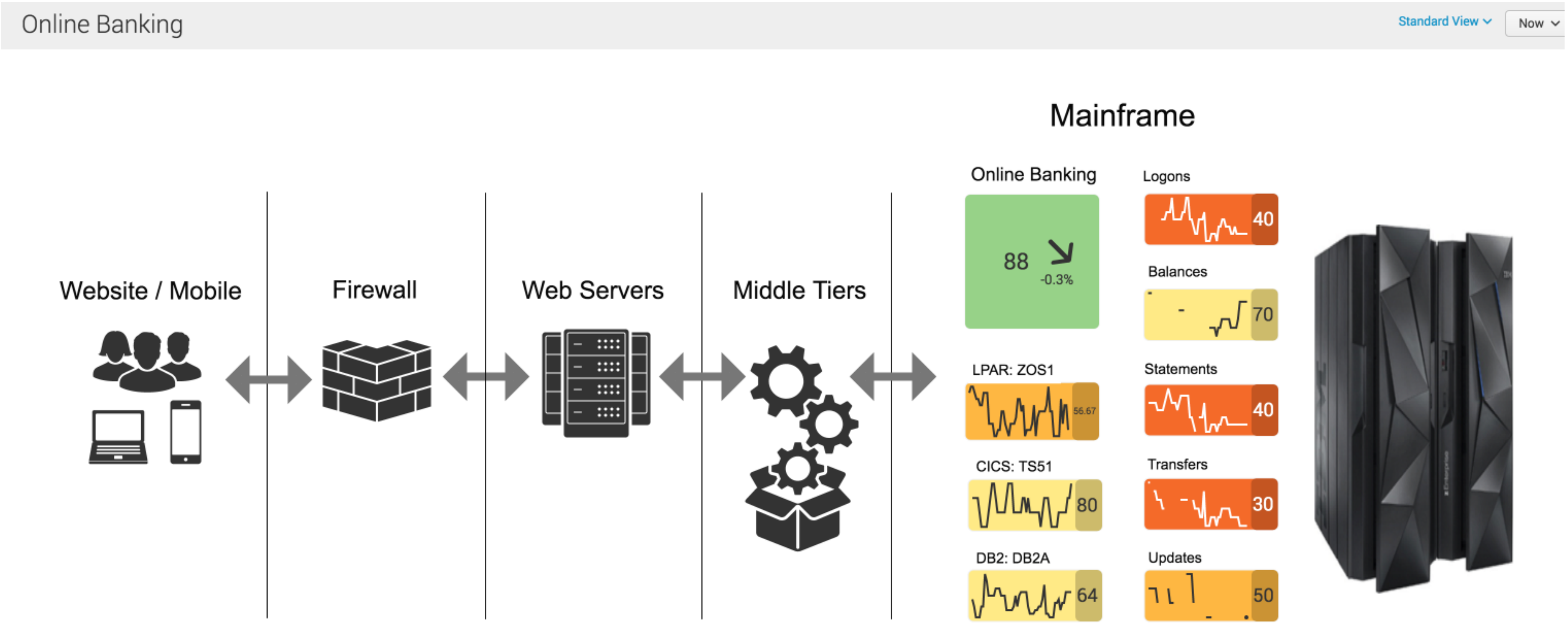
Deadlocks

Escalations (Exclusive)

Escalations (Shared)

Timeouts

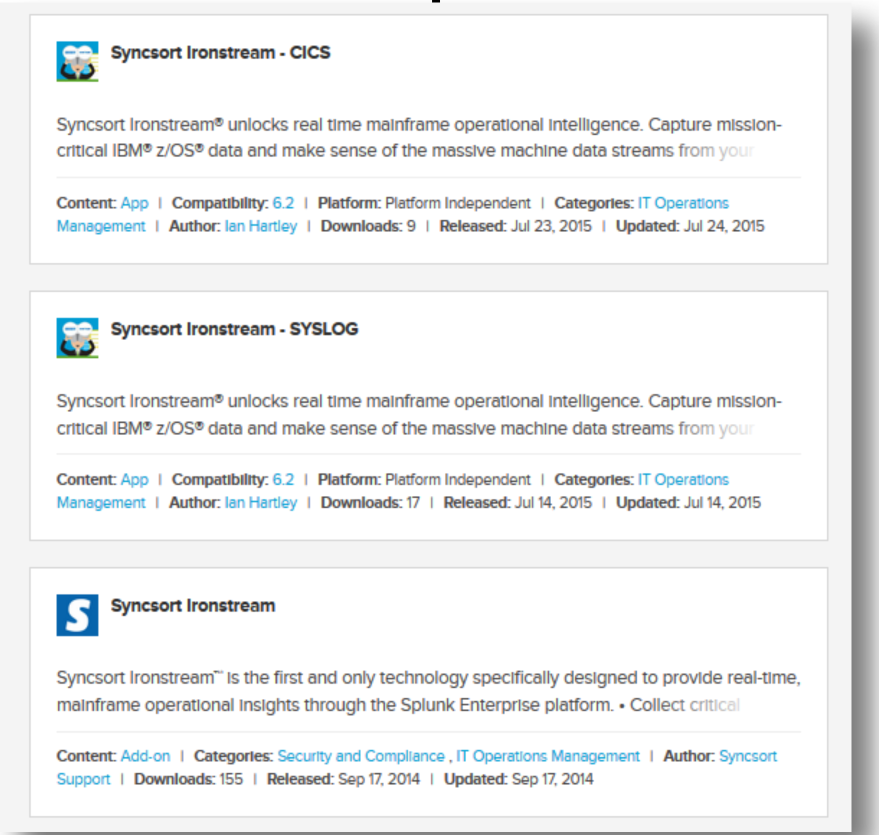
Ironstream Integration with ITSI



Ironstream Apps Are On splunkbase

https://splunkbase.splunk.com/

→ Search Syncsort



Syncsort Ironstream - CICS

Syncsort Ironstream® unlocks real time mainframe operational intelligence. Capture mission-critical IBM® z/OS® data and make sense of the massive machine data streams from your

Content: App | **Compatibility:** 6.2 | **Platform:** Platform Independent | **Categories:** IT Operations Management | **Author:** Ian Hartley | **Downloads:** 9 | **Released:** Jul 23, 2015 | **Updated:** Jul 24, 2015

Syncsort Ironstream - SYSLOG

Syncsort Ironstream® unlocks real time mainframe operational intelligence. Capture mission-critical IBM® z/OS® data and make sense of the massive machine data streams from your

Content: App | **Compatibility:** 6.2 | **Platform:** Platform Independent | **Categories:** IT Operations Management | **Author:** Ian Hartley | **Downloads:** 17 | **Released:** Jul 14, 2015 | **Updated:** Jul 14, 2015

Syncsort Ironstream

Syncsort Ironstream™ is the first and only technology specifically designed to provide real-time, mainframe operational insights through the Splunk Enterprise platform. • Collect critical

Content: Add-on | **Categories:** Security and Compliance , IT Operations Management | **Author:** Syncsort Support | **Downloads:** 155 | **Released:** Sep 17, 2014 | **Updated:** Sep 17, 2014

Splunk Your z/OS Mainframe and Get a 360-degree View of Your Entire IT Infrastructure

- Intrusion Detection (port scans, floods/DoS attacks, malformed data packets)
  - z/OS Traffic Regulation Management Daemon (TRMD)
  - SYSLOGD
  - Network Management Component
- TSO logon tracking
  - SMF30
- TSO account change activity
  - SMF80
- FTP authentications
  - SYSLOGD
  - Network Management Component
- FTP file change analysis
  - SMF119
- IP traffic analysis
  - SMF119
- Network events
  - Network Management Component

Syncsort Heritage

- Syncsort provides fast, secure, enterprise-grade software spanning “Big Iron to Big Data”
- 50% of all mainframes run Syncsort software
- Real-time MF Log data to Splunk - Ironstream
- DB2 transparency migration solutions
- Real-time network management and security software

- Fastest sort technology in the market
  - *Most trusted 3rd party mainframe software*
- Over 45 years of innovation:
  - *25+ issued & pending patents*
- Large global customer base
  - *12,000+ deployments in 85 countries and serving 87 of the Fortune 100*
  - *1,500 mainframe customers*

Our customers realize ROI and get the best customer service in the world, every day!

BARCLAYS CAPITAL · THOMSON REUTERS · millennialmedia The Mobile Advertising Platform · comScore · globalpayments · HSBC · Sprint

BBVA Compass · NYSE Euronext · JPMorganChase · Nationwide On Your Side · HCA Hospital Corporation of America · BBVA · INTESA SANPAOLO · verizonwireless

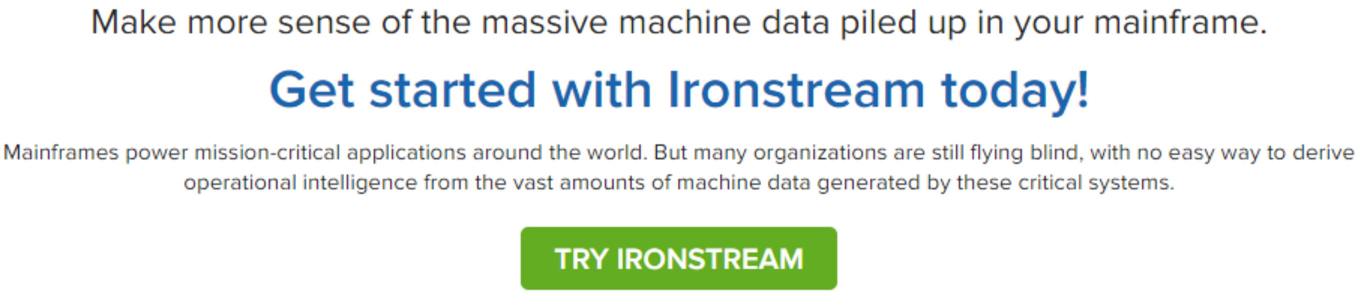
Overstock.com · metroPCS · shopzilla · Sabadell · BNP PARIBAS · LCL Le Crédit Lyonnais · MONTE DEI PASCHI DI SIENA BANCA DAL 1472

Key Partners

cloudera Ask Bigger Questions · Hortonworks · bmcsoftware · IBM · hp VERTICA · Cognizant · Greenplum · splunk> · DELL · tableau software

What Now?

Come visit us our booth!
Get Ironstream® for SYSLOG for free



Make more sense of the massive machine data piled up in your mainframe.

Get started with Ironstream today!

Mainframes power mission-critical applications around the world. But many organizations are still flying blind, with no easy way to derive operational intelligence from the vast amounts of machine data generated by these critical systems.

http://www.syncsort.com/en/TestDrive/Ironstream-Starter-Edition

CONTACT

INFO@SYNCSORT.COM

THANK YOU

syncsort

.conf2016

splunk>