Gaining Insight into Mainframe Log Data through Enhanced z/OS Analytics

Ed Wrazen, Product Management Director
Syncsort Inc

November 2018
Session OH

Agenda

- Introductions
- Syncsort Overview
- State of the Mainframe Survey 2018
- Mainframe Log Data Sources
- Syncsort Ironstream Overview
- Splunk Mainframe Log Analytics
- Summary
- Q&A

Introducing Syncsort

Global leader in Big Iron to Big Data

Big Iron to Big Data is a fast-growing market segment composed of solutions that optimize traditional data systems and deliver mission-critical data from these systems to next-generation analytic environments.

>7,000 customers

84 of the Fortune 100

Customers in >100 countries

Royal Bank of Canada
BARCLAYS CAPITAL
LLOYDS BANKING GROUP
INTESA SANPAOLO
Capital One
REGIONS
Broadridge
HSBC
BBVA Compass
MasterCard
JPMorganChase
BNP PARIBAS
GUARDIAN
PROGRESSIVE
THE HARTFORD
Nationwide On Your Side
CVS/caremark

BOEING
GM FINANCIAL
IHG InterContinental Hotels Group
HCA Hospital Corporation of America
PORSCHE
Volkswagen
KDDI
Sprint
Time Warner Cable
THOMSON REUTERS
CenturyLink
verizon
experian
comScore
LOWE'S
macy's

Headquarters: Pearl River, NY

U.S. LOCATIONS

- Burlington, MA; Irvine, CA; Oakbrook Terrace, IL; Rochester, MN

GLOBAL PRESENCE

- U.K., France, Germany, Netherlands, Israel, Hong Kong & Japan

We build on your legacy… because it works!

Your traditional systems – including mainframes, IBM i servers & data warehouses – adapt and deliver increasing value with each new technology wave

91%

of executives predict long-term viability of the mainframe as the platform continues evolving to meet digital business demands

BMC 12th Annual Mainframe Research Results – Nov. 2017

>100k

companies today use IBM i technology to run significant workloads & power critical business applications

$1.65trillion

invested by enterprise IT to support data warehouse & analytics workloads over the past decade

Wikibon "10-Year Worldwide Enterprise IT Spending 2008-2017"

We help you embrace the next wave

Modern businesses continuously create new streams & sources of data that deliver unique insights when combined with legacy data

CLOUD

- Agility, innovation and time to market
- Increase scalability & reliability
- On-demand investment, pay-as-you-go

IoT & STREAMING DATA

- Increase efficiency
- Reduce costs & risk
- Grow revenue

Advanced Business & Operational Analytics

AI & DATA SCIENCE

- Manage churn, cross sell, analyze risk & fraud
- Predict propensity to purchase
- Anticipate demand, prevent deficiencies

DATA GOVERNANCE

- Meet regulatory compliance
- Understand data context, meaning
- Accuracy, completeness, consistency, relevancy, timeliness, validity of data

Advancing data

Cloud

IoT & Streaming

AI & Data Science

Data Governance

MUST solve for the present & prepare for the future

Control costs & improve performance of legacy systems to help fund new technology investments

Increase security & governance of legacy data systems to prepare to take advantage of new innovations

Combine legacy systems with new data sources to power unique business insights

Optimized access to legacy data reserves is required to achieve the benefits of new tech innovations!

Mainframes and IBM i run the core transactional apps of most enterprises

Mobile & online increasing transaction volumes and workload unpredictability

Enterprises making major investments in Big Data platforms for new insights

State of the Mainframe for 2018

An Annual Survey of IT Professionals

What Every Business Needs to Know About Big Iron in a Big Data World

How is your organization using/ planning to use the mainframe in the next 12 months?

(select all that apply)

50.8% Cutting IT costs by optimizing mainframe resources

21.0% Storing and processing growing volumes of data from mobile devices to support mobile applications

25.0% Connecting/ integrating with on-premise Cloud-based services

13.7% Other

19.4% Providing machine data such as SMF or log data to platforms like Splunk® Enterprise, Hadoop and Spark to get an enterprise-wide view of operational and security intelligence

56.5% Acting as the main hub for business-critical applications

42.7% Running services on the mainframe that can generate revenue for your company

21.0% Providing mainframe application data to a data lake to be integrated and analyzed with other enterprise data sources using Big Data platforms like Hadoop and Spark to support better business decisions

8.9% Storing and processing growing volumes of data from IoT devices

16.9% Connecting/ integrating with off-premise Cloud-based services

Mainframes remain strategic to the business, but optimization is critical

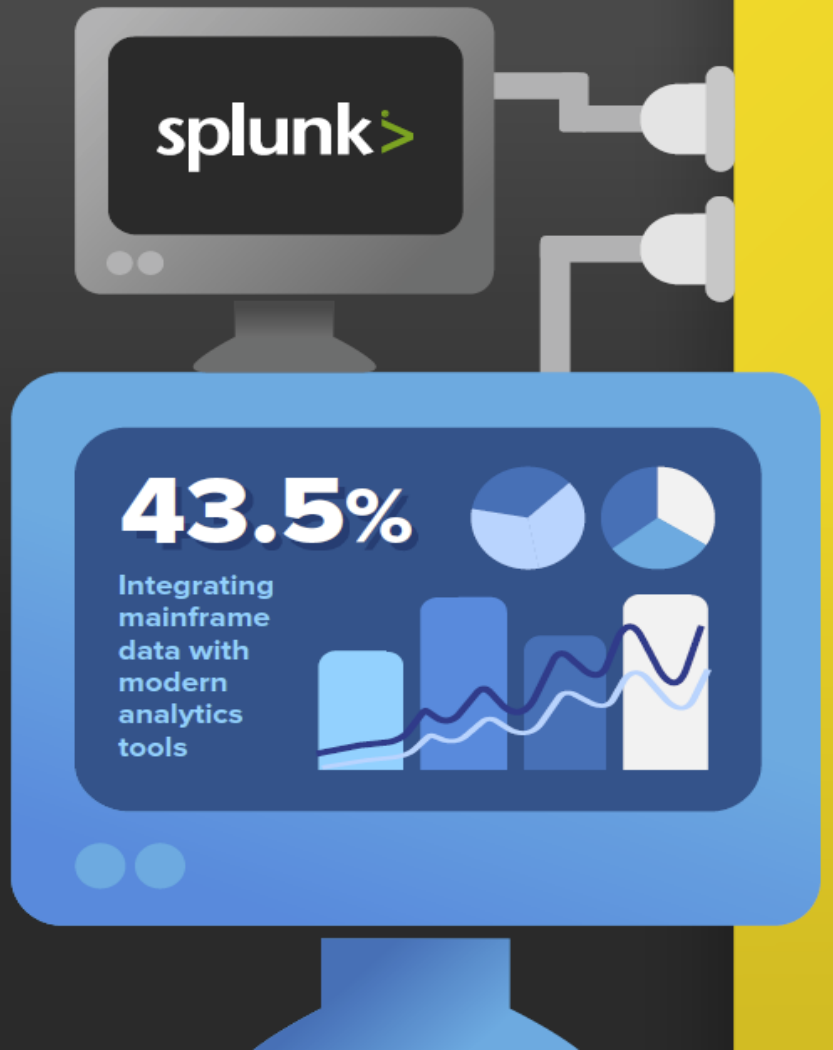
Organizational priorities include zIIP engines for mainframe optimization and mainframe data analytics

What are your priorities for modernizing your mainframe environment in the next 12 months?

(select all that apply)

22.6%

Using tools like Splunk to include mainframe data with other enterprise data for monitoring through a dashboard ("single pane of glass")



50.8%

Leveraging zIIP engines to reduce processing costs

33.9%

Reducing or eliminating technical debt by integrating your mainframe with other IT assets

11.3%

Accessing and integrating mainframe data into Hadoop or Spark data lakes

8.9%

Moving data from IMS to DB2 on IBMz

Meeting security & compliance requirements and SLAs remain critical objectives that will impact mainframes in the next 12 months

Please rank your organization's top objectives that impact your mainframe environment over the next 12 months, with 1 being of high priority/concern and 6 being of least concern/priority

(select all that apply)

	1	2	3	4	5	6
Enhancing IT Operations analytics (ITOA)	12.9%	15.3%	21.0%	11.3%	18.5%	21.0%
Meeting Service Level Agreements (SLAs)	33.1%	21.8%	13.7%	8.9%	11.3%	11.3%
Meeting security and compliance requirements	41.9%	21.0%	13.7%	4.8%	8.1%	10.5%
Consolidation of duplicative systems/functions from consolidation/footprint reduction	15.3%	12.9%	21.8%	16.9%	15.3%	17.7%
Enhanced visibility into delivery of IT services	8.1%	18.5%	24.2%	20.2%	16.1%	12.9%
Expanding use of "big data" analytics and tools	9.7%	12.1%	21.8%	16.9%	16.9%	22.6%

Key points

- **62.9%** Rank meeting security and compliance requirements as the #1 or #2 priority
- **54.9%** Rank meeting Service Level Agreements (SLAs) as the #1 or #2 priority

Analysis of SMF data remains key to understanding mainframe security and compliance

Which of the following are important for security on the mainframe?

(select all that apply)

54.0%
Monitor SMF and log file data

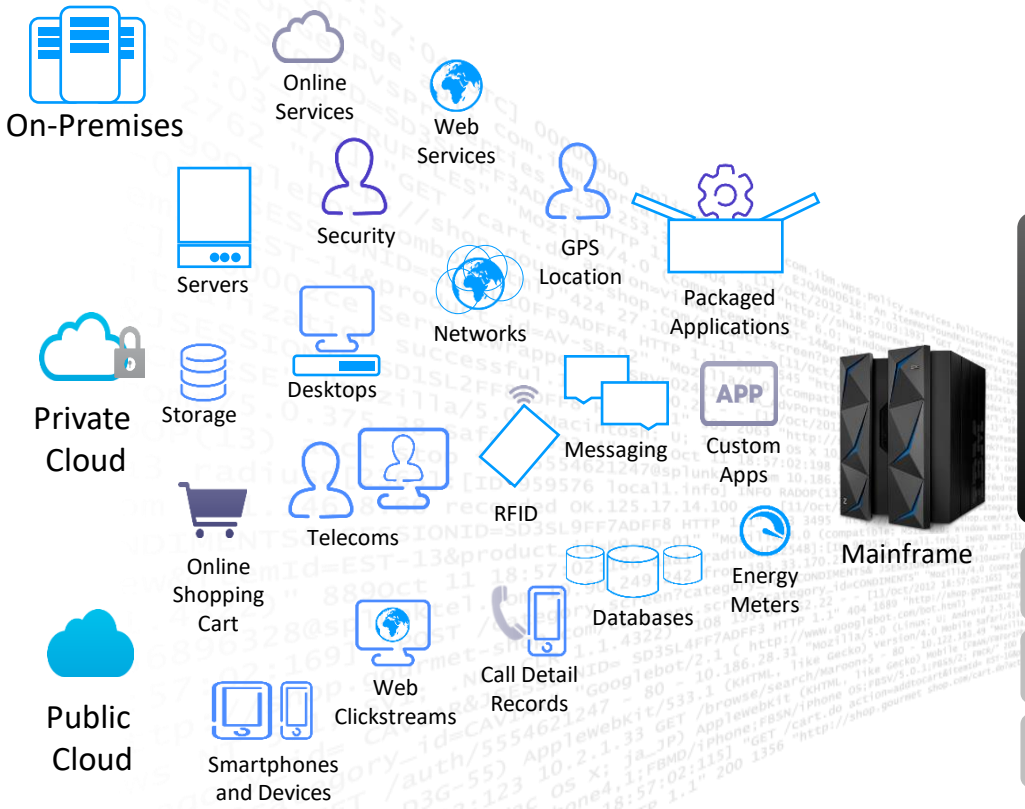
53.2%
Have an audit trail of SMF data

51.6%
Audit and review incident response

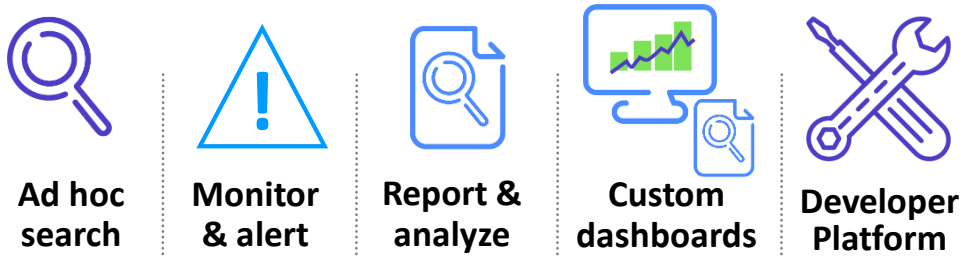
50.8%
Get real-time analysis of security alerts generated by network hardware and applications

Splunk: Industry-Leading Platform For Machine Data

Machine Data: Any Location, Type, Volume



Answer Any Question



splunk>enterprise

splunk>cloud

Platform Support (Apps / API / SDKs)

Enterprise Scalability

Universal Indexing

Machine Data Contains Critical Insights

SOURCES

Mobile app

{"timestamp": "1539680653","connection": "4G", "statusCode": 200, "platform": "Android", "extraData": {"jsessionid": 7888490, "member": "regular"}, "packageName": "com.buttercup. Session ID 'ef1f7539", "requestLength": 301, "url": "/api/buy", "remoteIP": Customer ID "session_id": 58269218 "protocol": "HTTP", "responseLength": 1276, "uuid": "5014e36cad204744aae4df682636a337", "userIdentifier": "freeman" User Name "appVersionName": "4.4", "osVersion": 8.0, "device": "Samsung Galaxy S7", "latency": 171, "carrier": "Orange", "state": "connected"}

Web server

95.74.208.82 - - [16/Oct/2018:12:41:58 +0200] "GET /api/buy?JSESSIONID= 58269218 product=421 HTTP/1.1" 200 352 "-" "Mozilla/5.0 (Android 8.0.0; Mobile; rv:62.0.3) Gecko/62.0.3 Fire Session ID Product ID

Middleware

Order ID

Oct 16 12:41:12.996 wl-01.acme.com Order 569281734 failed for customer 5014e36cad204744aae4df682636a337

Exception follov Customer ID c.extensions.ConnectionDeadSQLException: weblogic.common.resourcepool.ResourceDeadException: Could not create pool connection. The DBMS driver exception was: [BEA][DB2 Driver] Error establishing socket to host and port: EZZ881:1521 Reason: Connection refused

Mainframe

EZZ881I PAGENT POLICY DEFINITIONS CONTAINS ERROR FOR DB2: MQUSER EZZ881:1521

Key Use Cases for Machine Data

Application/System Monitoring

- Bigger picture of what's happening in the environment
- Make better decisions to take control of the IT infrastructure
- Throughput, performance & availability
- Problem Detection & Isolation
- Ensure SLAs Met
- Reduce MTTI, MTTR
- System Health (Splunk ITSI)

Security and Compliance

- Detect and prevent security threats
- Privileged activity
- Ensure compliance
- Ensure audits pass
- Enterprise Security (Splunk ES)

Mainframe Log Data Sources

Data Type	Description
SMF Records & Fields	Provides availability and performance data for z/OS operating systems, applications, web servers, DB2, CICS, and WebSphere MQ sub-systems. SMF provides security and compliance data that can be used for intrusion detection, tracking TSO Logon and account activity, FTP traffic and dataset analysis
IMS Log Records	Provides visibility into IMS system and transaction availability and performance
SYSLOG Messages	Monitor CICS, DB2, IMS, MQ, USS, Websphere Application Server(WAS) and other sub-systems along with JOB activity on z/OS. Monitor RACF, ACF2, and Top Secret activities on z/OS.
SYSLOGD Messages	Enables visibility into network alerts, Linux environments, Open System Adapter (OSA), FTP, IP, and Enterprise Extender (EE).
SYSOUT Data	Enables application outputs to be captured and analyzed from specific JOBs or job types.
Log4J Records	Provides visibility into web application environments for monitoring web application availability and performance
USS file data	Output from applications, as well as critical log data required for IT operational efficiency and security compliance.
RMF III Data	Detect and prevent potential bottlenecks and performance delays by capturing RMF III metrics well before the information is written to SMF.
System State Information	Quick view into z/OS system performance metrics, including 4HRA of MSUs for each LPAR mapped against the CEC defined MSU capacity.

SMF Data: The Most Comprehensive Mainframe Data Source

System Services & Components		SMF Records Logged	Description
CICS: Transaction Processing	→	SMF 110	Transaction Stats & Performance
Db2: Database Systems	→	SMF 100 - 102	Database Stats & Performance
WebSphere AS: Web Application Server	→	SMF 120	Websphere Stats & Performance
WebSphere MQ: Messaging Queueing	→	SMF 115, 116	Message Queueing Stats & Performance
UNIX System Services (USS): Hierarchical File System	→	SMF 92	USS HFS Statistics
RMF: Resource Measurement Facility	→	SMF 70 - 79	Resource Management
RACF/ACF2/Top Secret: Security Systems	→	SMF 80	Access & Authentication
JOBs: Batch Workloads	→	SMF 30	Workload Execution
TCP/IP and FTP: IP & File Transfer Protocol	→	SMF 118, 119	IP & File Transfer Activity
Other Systems Components & Vendor Products	→	Other	Other SMF Record Types

Examples of some SMF records logged by various system components and processes

Market Landscape and Key Concepts: Big Iron to Big Data Analytics Challenges

So many data sources

- Systems Management Facility (SMF)
- IMS
- Syslog
- Sysout
- Log4j web and application logs
- RMF
- USS files and standard datasets
- Db2 & Sequential Files

Volume of data

Millions of log records generated daily

- 9.7TB Average Daily Mainframe Log Data

Format of data

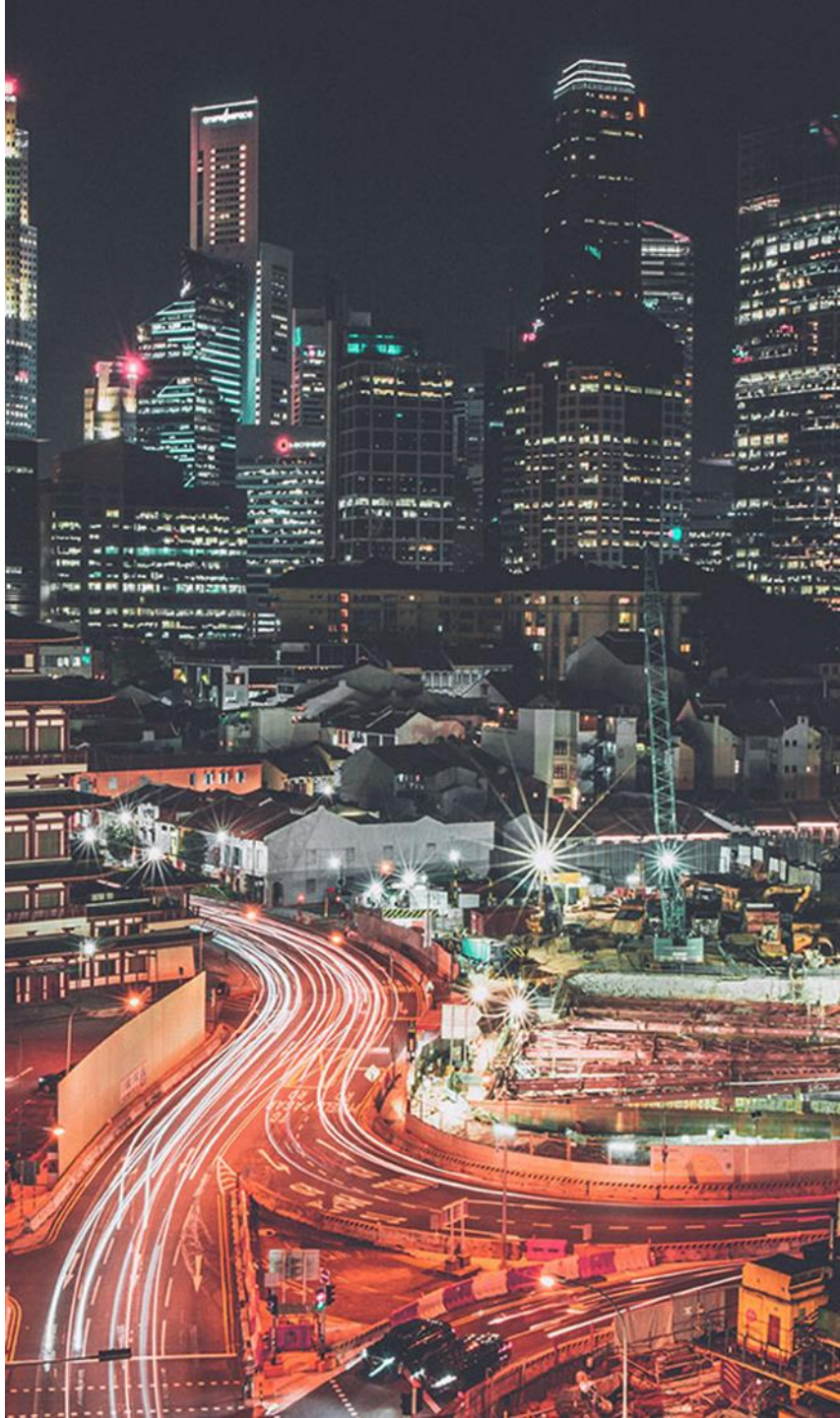
- Multiple formats
- Complex data structures (SMF) with headers, product sections, data sections, variable length and self-describing
- EBCDIC not recognized outside of the mainframe world
- Binary flags and fields

Difficulty to get the information in a timely manner

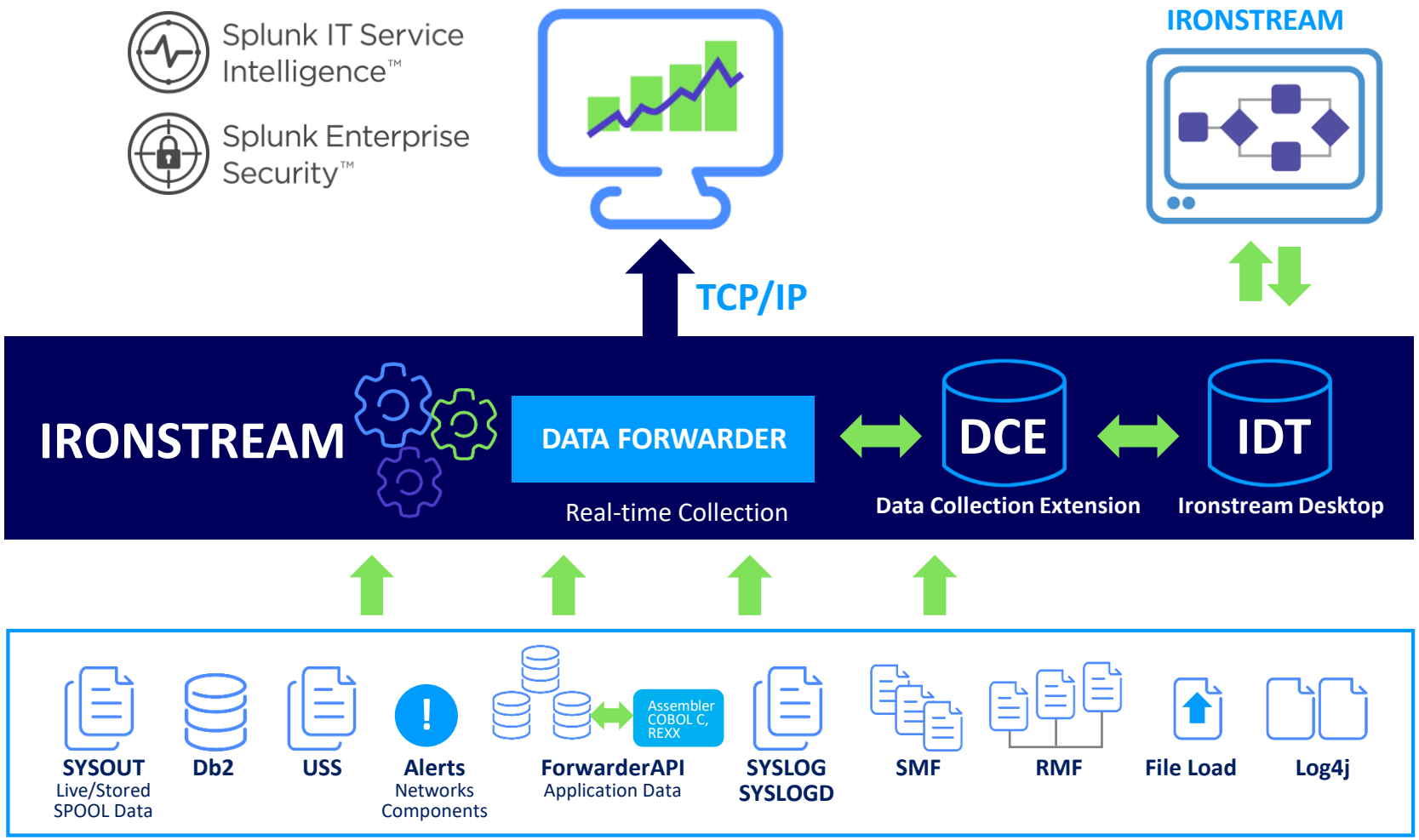
- Not real-time, typically have to wait overnight for an offload
- Typical daily FTP upload/downloads can't get granular

Market Landscape and Key Concepts: What is needed?

- High performance, low-cost, platform for collecting critical system information in real-time
- Normalization of the z/OS data so it can be used off platform analytics engines
- Ability to easily combine information from different data sources and systems across the Enterprise
- Address the SME challenge: use by network managers, security analysts, application analysts, enterprise architects without requiring mainframe access or expertise



Ironstream® for Mainframe Overview



Splunk Analytics for Security and Compliance (SIEM)

Easier to identify unauthorized mainframe access or other **security risks** and ability to meet compliance requirements such as **SOC II**

- **Challenges Addressed**
- Tracking security related issues including password changes, login success and failures, account lock outs, dataset access, FTP activity
- Identify changes in access patterns to detect potential security threats
- Move from post event forensics to real-time monitoring of the security environment
- Fulfillment of mandatory security and compliance audits to meet corporate and regulatory requirements
- Eliminate manual reporting along with the delay required to get the information, by accessing it in real-time

- **Primary Data Sources**
- SMF records used for intrusion detection, tracking TSO Logon and account activity, FTP traffic and dataset analysis.
- SYSLOG messages to monitor RACF, ACF2, and Top Secret activities on z/OS.
- SyslogD and Network Alerts used to monitor security events and activity

Ironstream z/OS Security Specific Data Collection

Intrusion Detection (port scans, floods/DoS attacks, malformed data packets)

- z/OS Traffic Regulation Management Daemon (TRMD) + SYSLOGD + Base network management component

TSO logon tracking

- SMF30

TSO account activity (create, update, delete, lockout)

- SMF80

FTP authentications

- SYSLOGD + Base network management component

FTP change analysis (file create, read, update, delete)

- SMF119

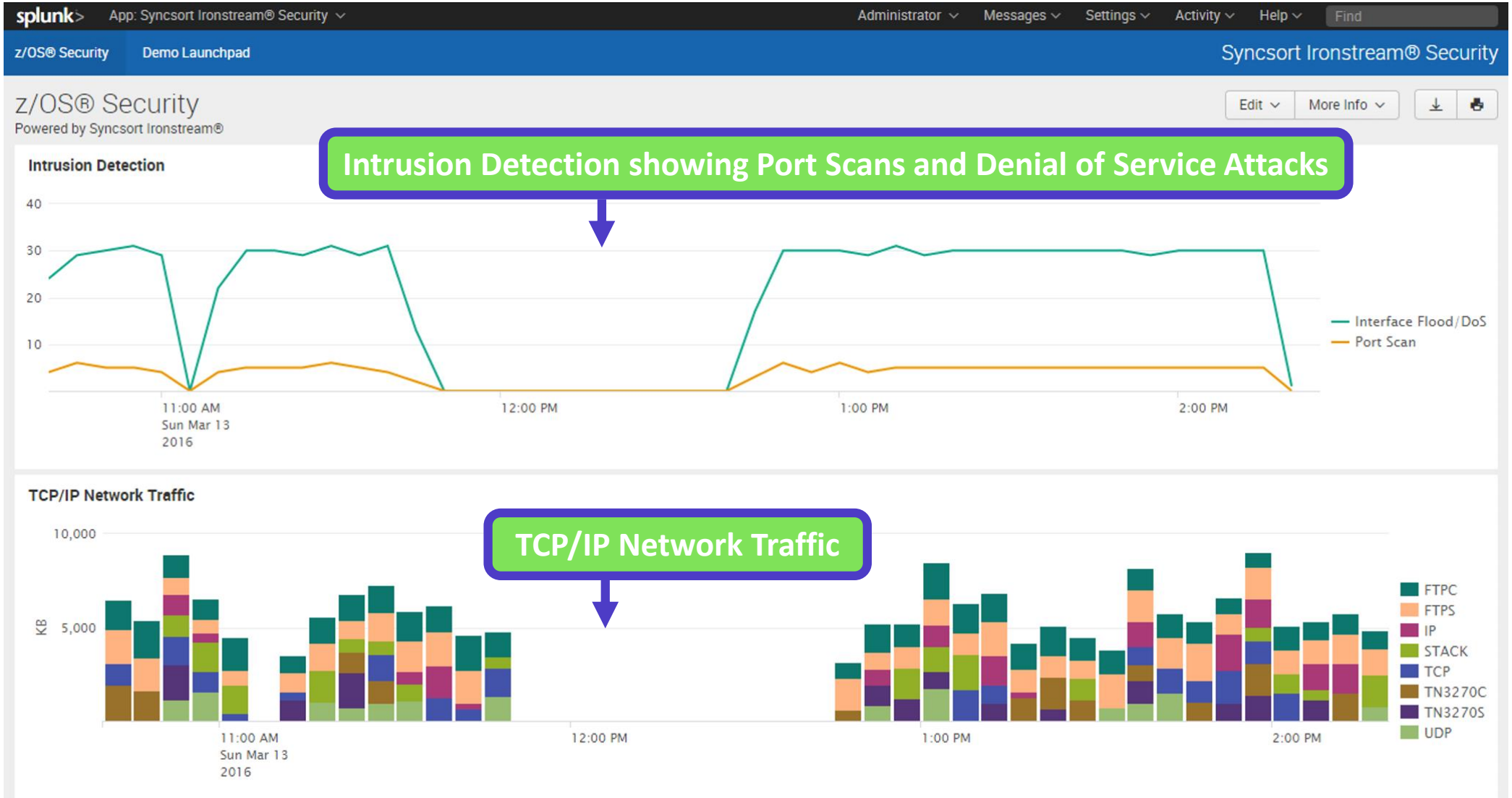
IP traffic analysis

- SMF119

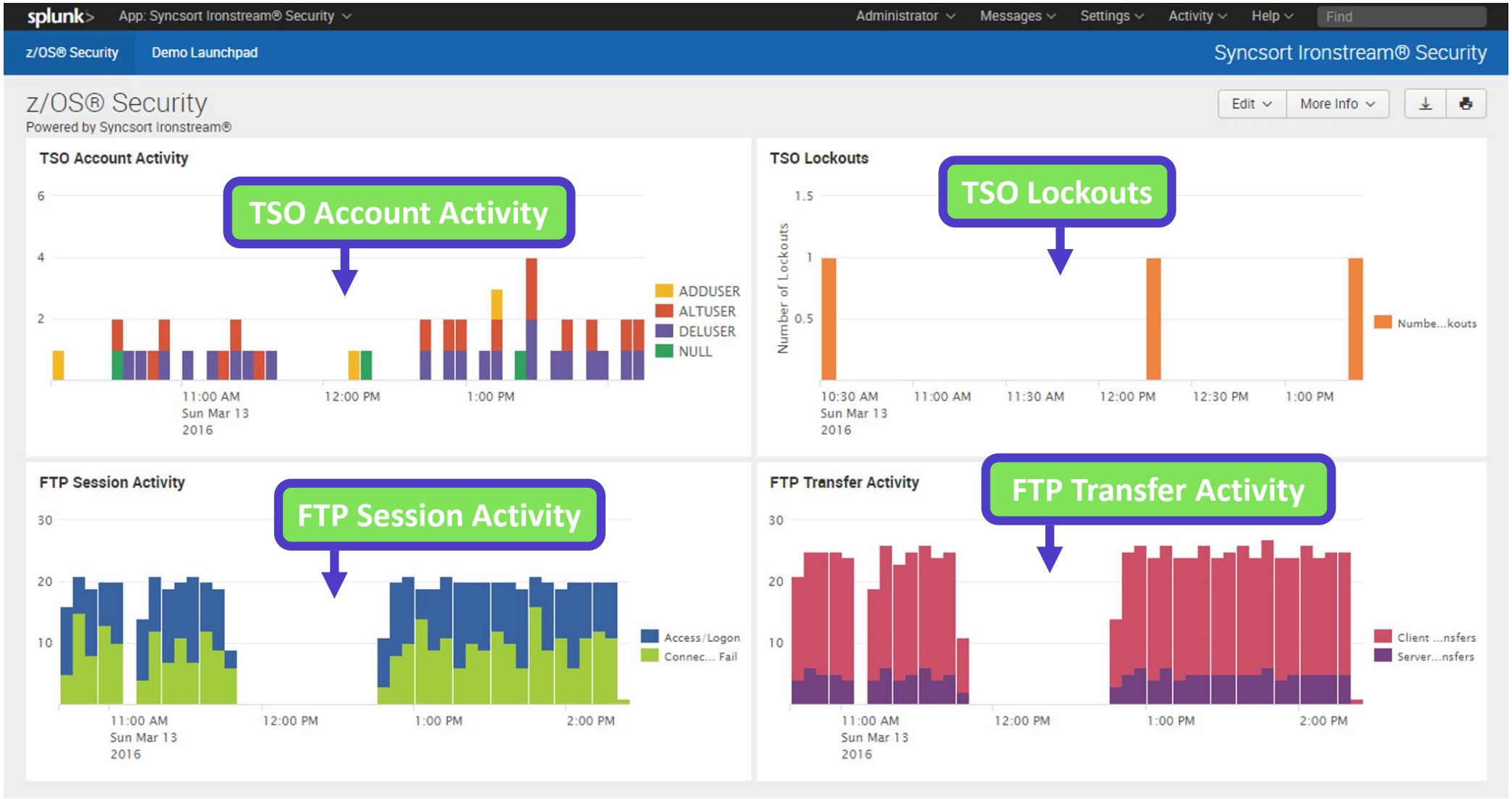
Network + user-defined Events (pre-defined + user-defined)

- Base network management component

z/OS Security Dashboard



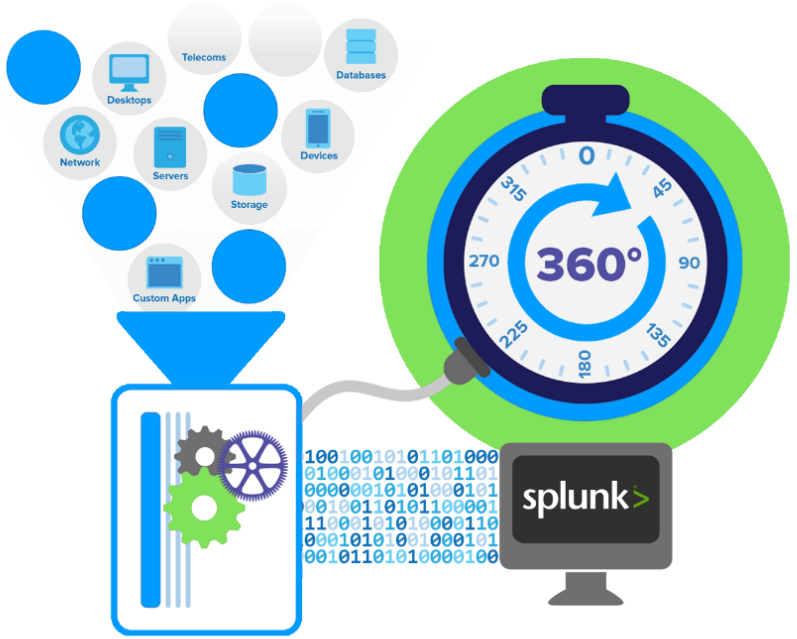
z/OS Security Dashboard



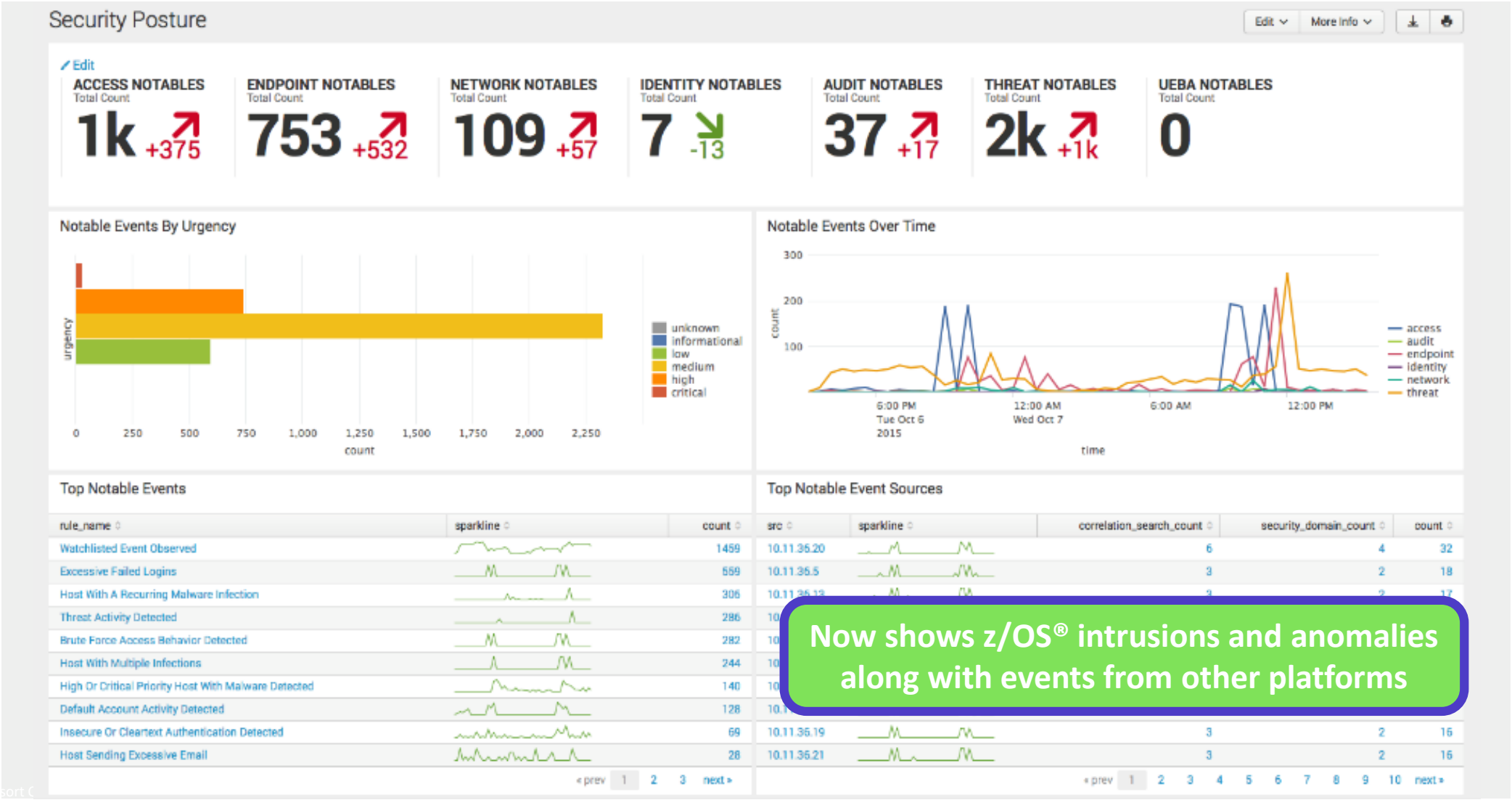
Ironstream z/OS Security & Splunk Enterprise Security

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

- This requires the Ironstream for Splunk Enterprise Security to be installed
- This provides an enterprise-wide, integrated view of security across all platforms via ES dashboards provided by Splunk



Sample: Splunk Enterprise Security™ Security Posture Dashboard



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

Ironstream for IT Operational Analytics (ITOA)

Real-time alerts to identify problems in all key environments like CICS, DB2, IMS, MQ
View latency, transactions per second, exceptions and other valuable data

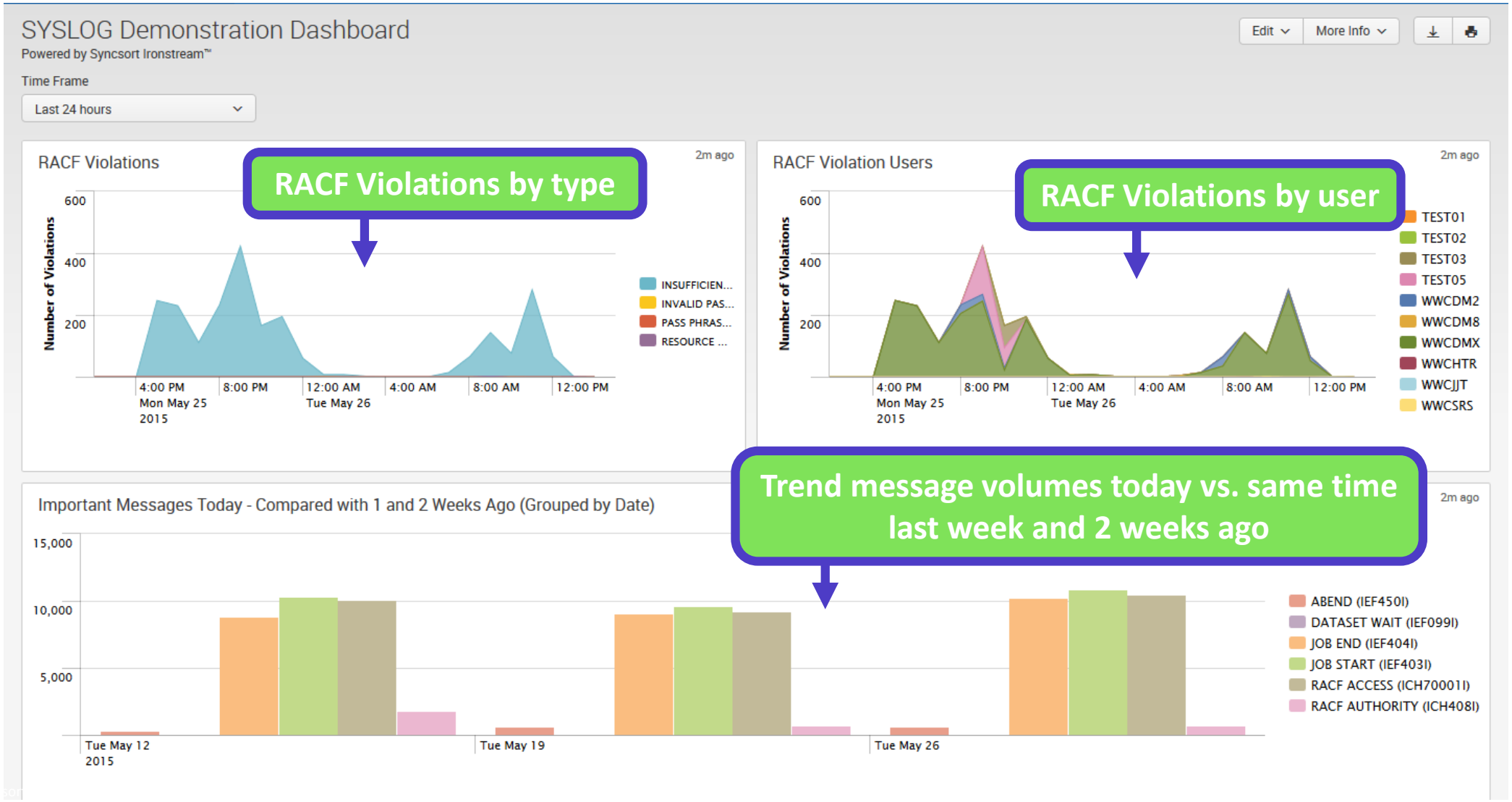
Benefits

- Real-time views of mainframe SMF data to identify real or potential failures earlier
- Correlation of information from different data sources (SYSLOG, Log4J, SMF, RMF) for faster triage and resolution of application issues
- Monitoring of web-application environments with alerting and reporting capabilities to ensure users and customers are receiving the best web experience

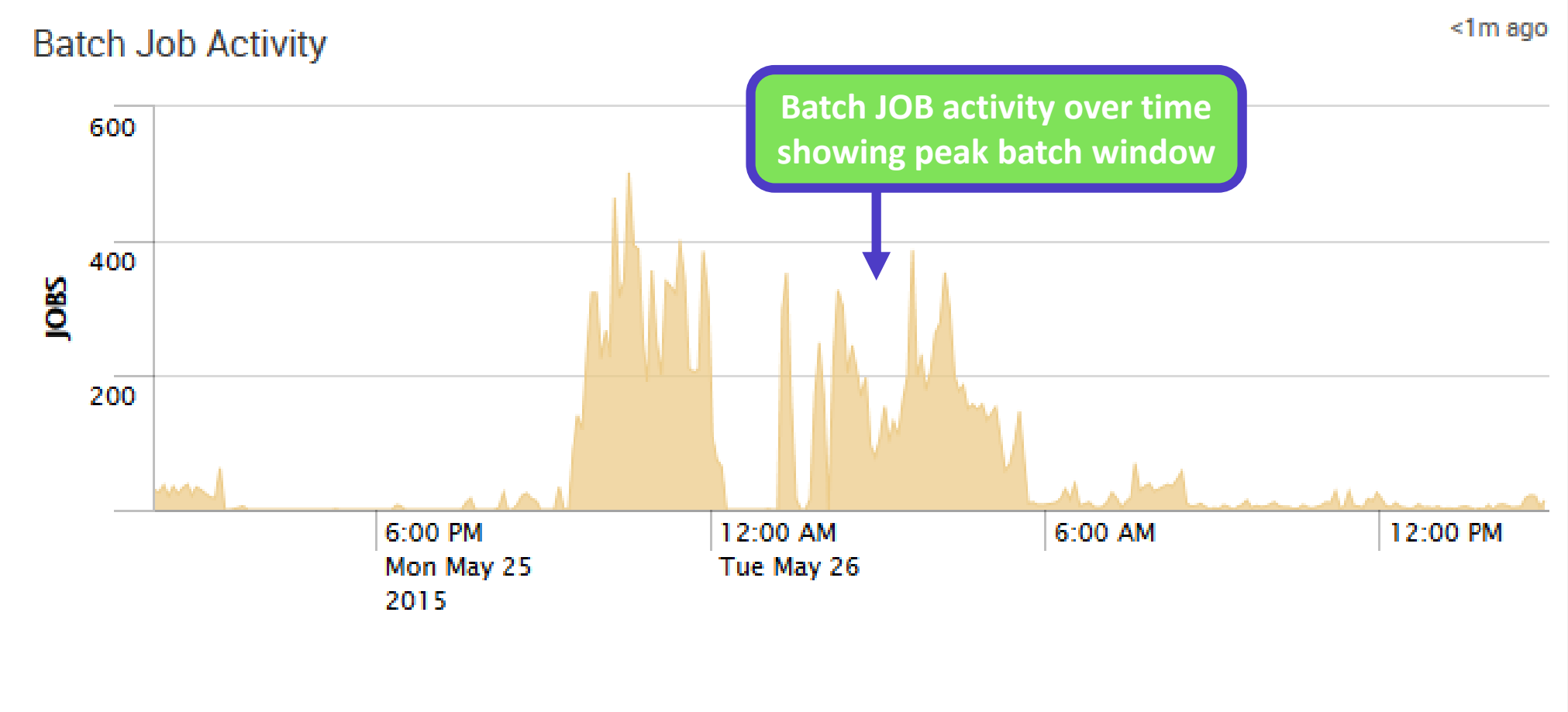
Primary Data Sources

- SMF records for availability and performance data for z/OS operating systems, applications, web servers, DB2, CICS, and WebSphere MQ sub-systems.
- SYSLOG messages to monitor CICS, DB2, IMS, MQ, USS, Websphere Application Server(WAS), JOB activity, and other sub-systems
- Log4J and USS file-based logs used to monitor web-based application activity

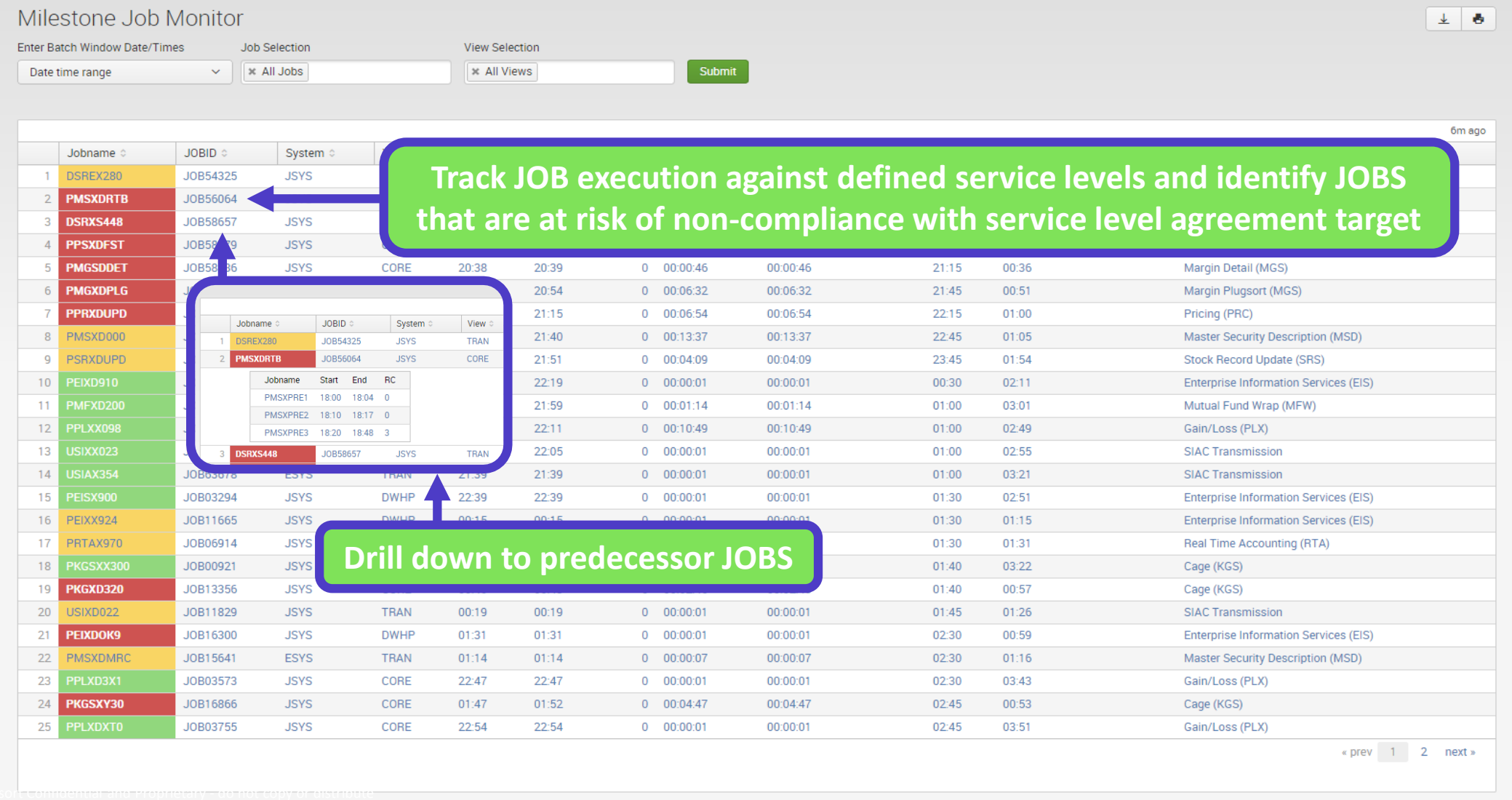
Syslog Dashboard: RACF Violations and Message Trends



Syslog Dashboard: Batch Job Activity



Job Monitor for SLA Tracking: SMF 30



	Jobname	JOBID	System									
1	DSREX280	JOB54325	JSYS									
2	PMSXDRTB	JOB56064										
3	DSRXS448	JOB58657	JSYS									
4	PPSXDFST	JOB58[illegible]79	JSYS									
5	PMGSDDET	JOB58[illegible]36	JSYS	CORE	20:38	20:39	0	00:00:46	00:00:46	21:15	00:36	Margin Detail (MGS)
6	PMGXDPLG	J[illegible]				20:54	0	00:06:32	00:06:32	21:45	00:51	Margin Plugsort (MGS)
7	PPRXDUPD	[illegible]				21:15	0	00:06:54	00:06:54	22:15	01:00	Pricing (PRC)
8	PMSXD000	[illegible]				21:40	0	00:13:37	00:13:37	22:45	01:05	Master Security Description (MSD)
9	PSRXDUPD	[illegible]				21:51	0	00:04:09	00:04:09	23:45	01:54	Stock Record Update (SRS)
10	PEIXD910	[illegible]				22:19	0	00:00:01	00:00:01	00:30	02:11	Enterprise Information Services (EIS)
11	PMFXD200	[illegible]				21:59	0	00:01:14	00:01:14	01:00	03:01	Mutual Fund Wrap (MFW)
12	PPLXX098	[illegible]				22:11	0	00:10:49	00:10:49	01:00	02:49	Gain/Loss (PLX)
13	USIXX023	[illegible]				22:05	0	00:00:01	00:00:01	01:00	02:55	SIAC Transmission
14	USIAX354	JOB[illegible]	[illegible]	[illegible]	[illegible]	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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	01:30	01:15	Enterprise Information Services (EIS)
17	PRTAX970	JOB06914	JSYS							01:30	01:31	Real Time Accounting (RTA)
18	PKGSXX300	JOB00921	JSYS							01:40	03:22	Cage (KGS)
19	PKGXD320	JOB13356	JSYS							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)

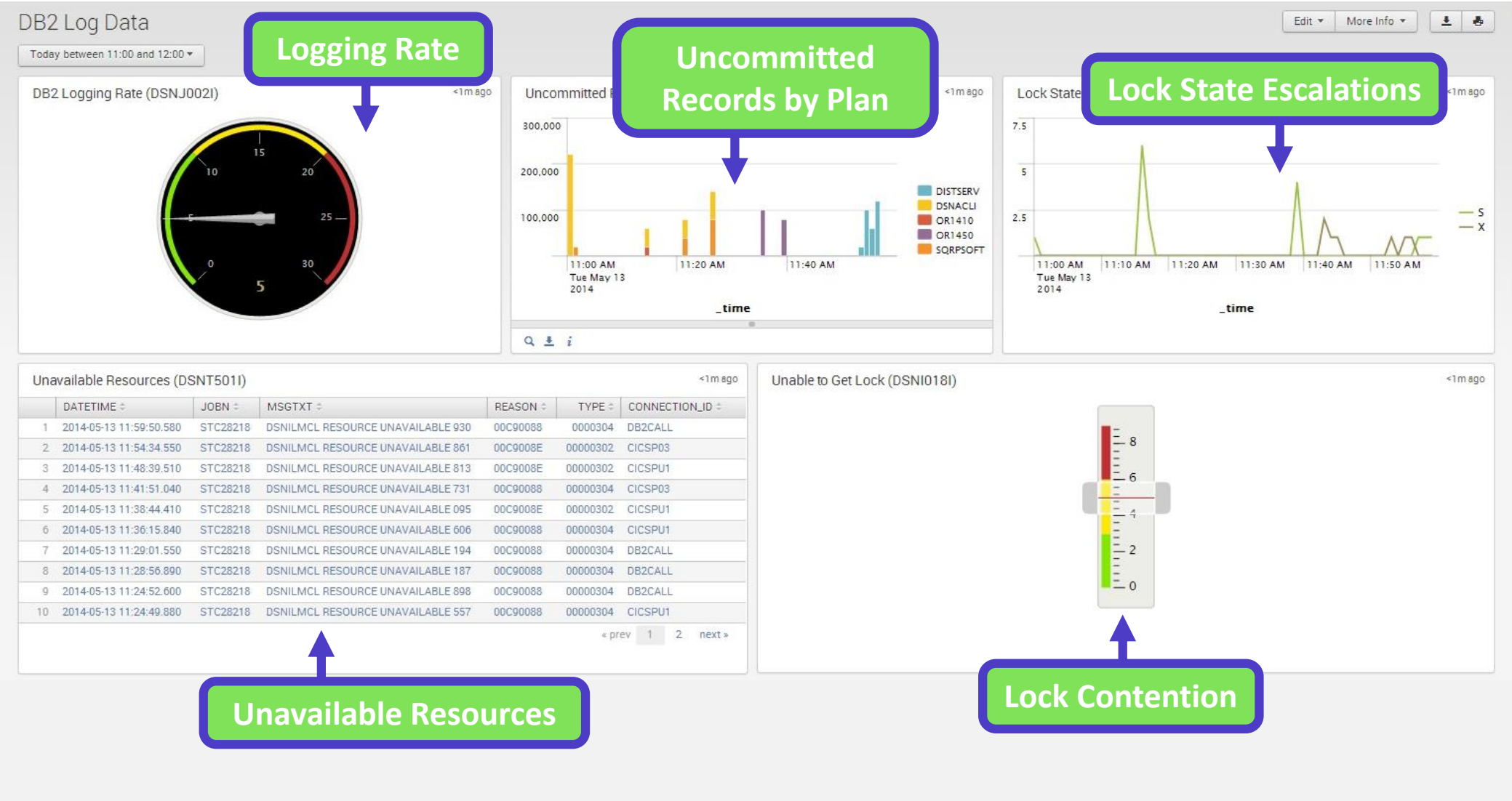
« prev 1 2 next »

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

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

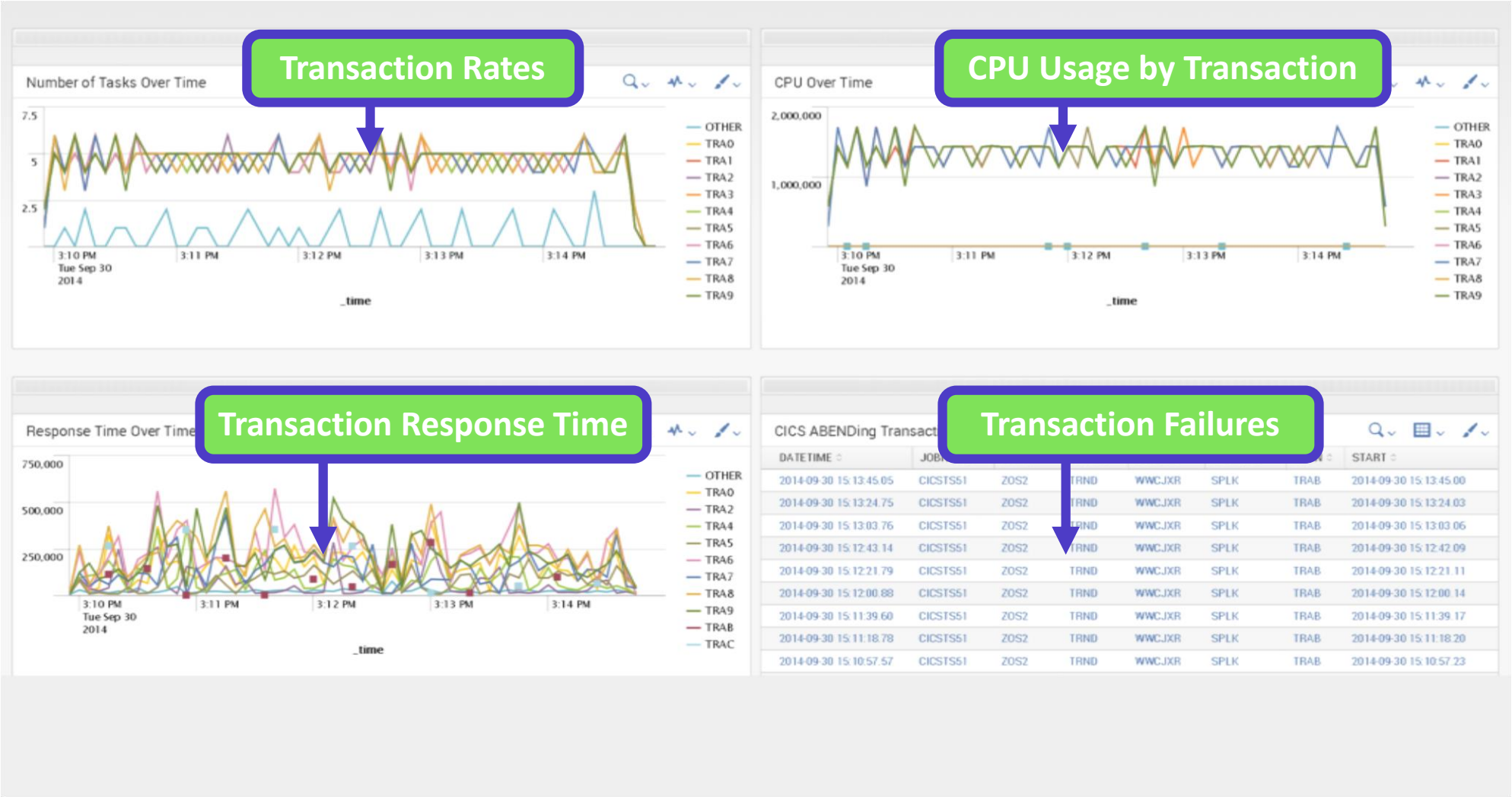
3	DSRXS448	JOB58657	JSYS	TRAN

Db2 Performance Monitoring

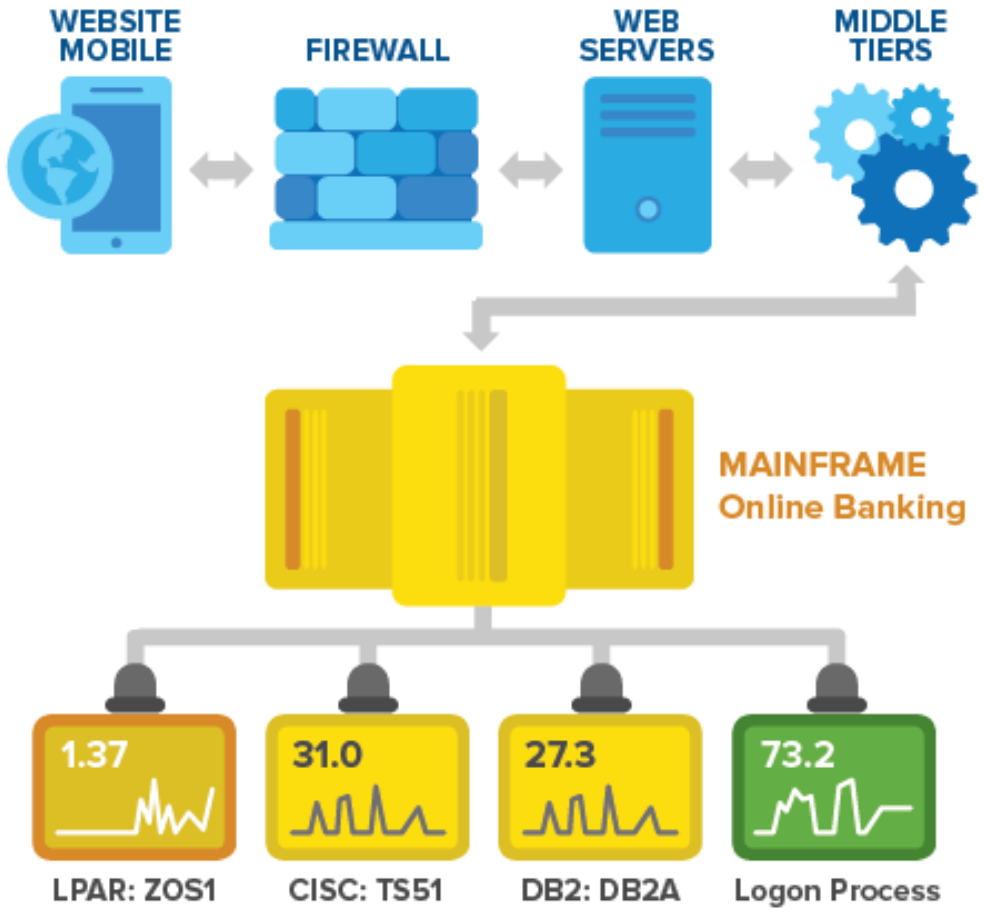


	DATETIME	JOBN	MSGTXT	REASON	TYPE	CONNECTION_ID
1	2014-05-13 11:59:50.580	STC28218	DSNILMCL RESOURCE UNAVAILABLE 930	00C90088	0000304	DB2CALL
2	2014-05-13 11:54:34.550	STC28218	DSNILMCL RESOURCE UNAVAILABLE 861	00C9008E	00000302	CICSP03
3	2014-05-13 11:48:39.510	STC28218	DSNILMCL RESOURCE UNAVAILABLE 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	00000302	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

CICS Transaction Monitoring



Ironstream Mainframe Module for Splunk ITSI

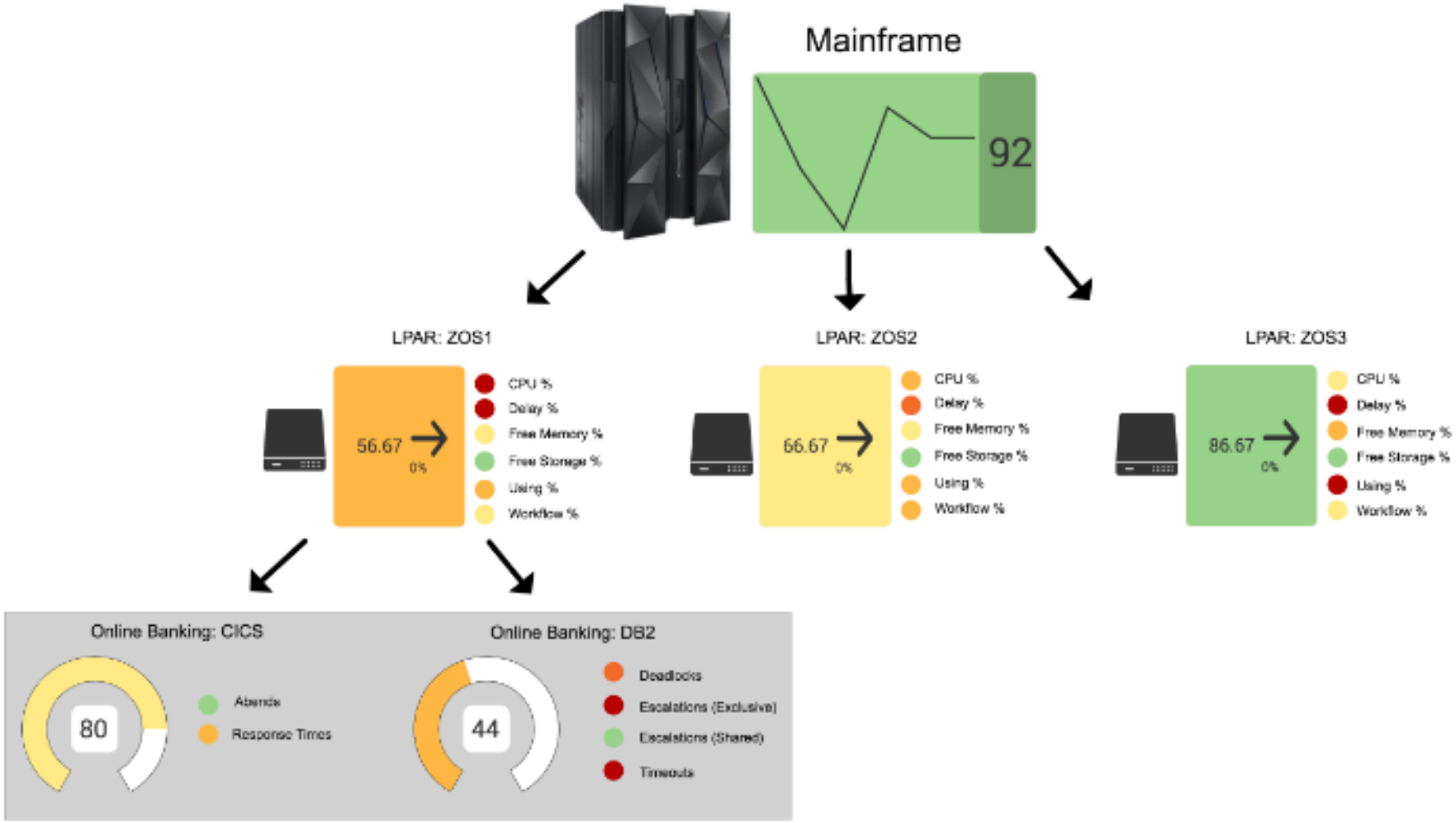


- Splunk IT Service Intelligence (ITSI) premium app delivers unique “service-centric” view of critical internal and customer-facing business services
- Free Ironstream Module enables service visualization, threshold monitoring, drill-down, predictive analytics for services spanning mainframe and distributed systems

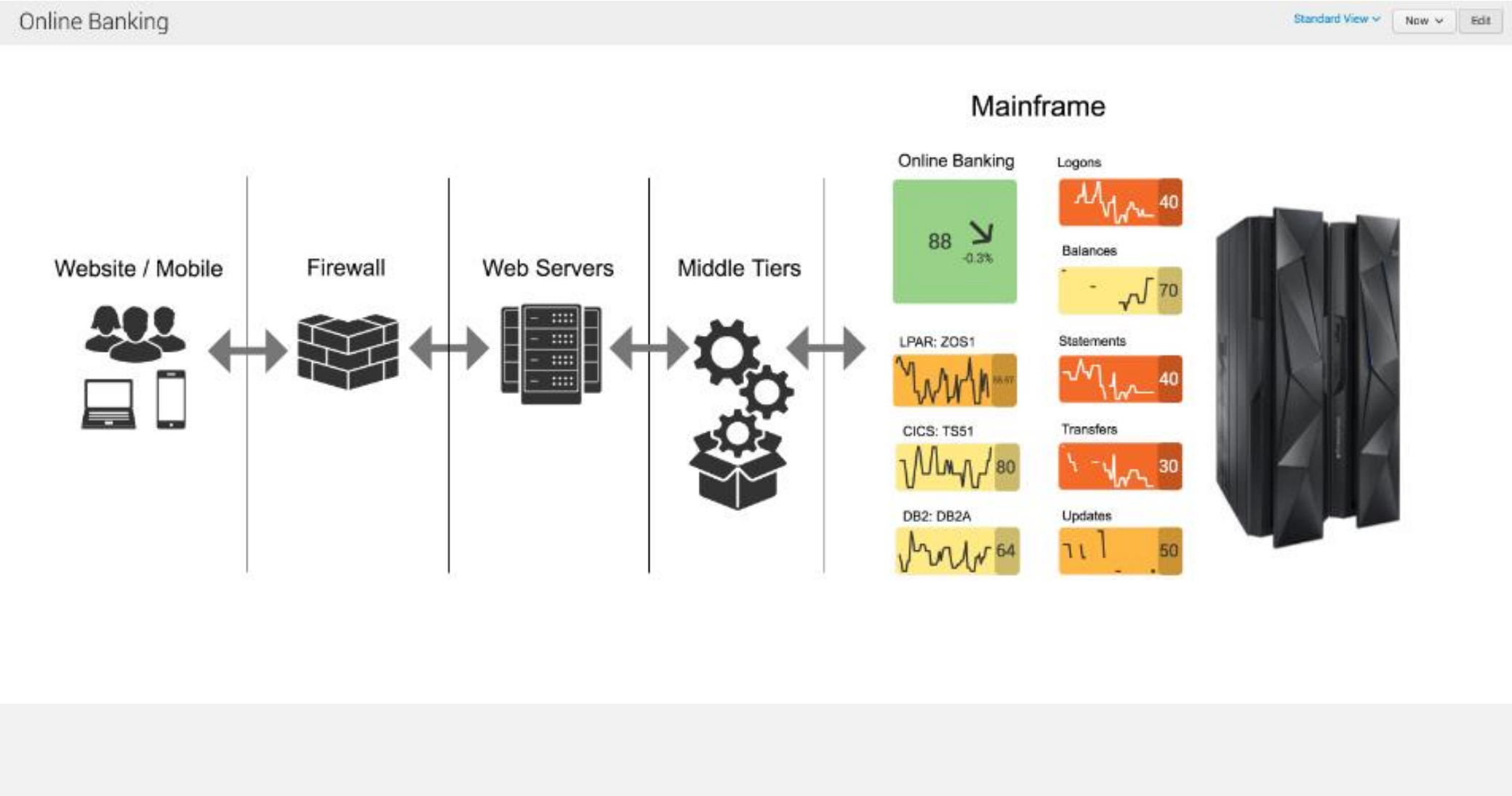
Ironstream Integration with Splunk ITSI

- **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**

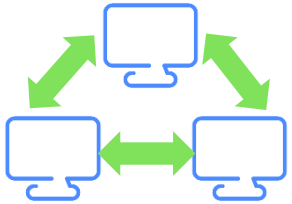
Ironstream ITSI Glass Table for Mainframe



Ironstream ITSI Glass Table for Online Banking Service



Summary: Value Today for Enterprises with an IBM z



Less Complexity

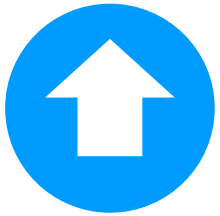
Collect IBM z data; correlate with data from the mainframe and other platforms; no mainframe **expertise required**

Effective Problem-Resolution Management

Real-time views to identify real or potential failures earlier; view related 'surrounding' information to **support triage repair or prevention**

Clearer Security Information

Identify unauthorized access, other **security risks;** prepares and visualizes key data for **compliance audits**



Higher Operational Efficiency

Enhanced event correlation across systems; Staff resolves problems faster; **"do more with less"**

Healthier IT Operations

Real-time alerts identify problems in all key environments View **latency, utilization, exceptions**, etc.

Eliminate Your Mainframe "Blind-Spot"

Splunk + Ironstream = Your 360° Enterprise View

Thank You!

Email: ed.wrazen@syncsort.com
Tel: +44 (0) 118 940 7634

We want your feedback!

- Please submit your feedback online at ….
  - http://conferences.gse.org.uk/2018/feedback/OH

- Paper feedback forms are also available from the Chair person

- This session is OH