



Splunk : Be the Hero!

Ingesting data from your most critical business system

Brant Hubbard | CEO, RHONDOS

Patrick Robinson | Solution Engineer, RHONDOS

Matt Colabrese | Director of Customer Success, RHONDOS

David Clawson | SplunkYoda, Splunk

October 3rd, 2019 | Version 4.1



Agenda

Embrace SAP® Data Chaos

Go from data to business outcomes faster than ever before with Splunk



RHONDOS

▶ The Hero Journey

▶ Security

▶ Supply Chain

▶ Performance

▶ Q&A

Truth #1: Heroes Deliver Massive Return on Investment



Complete visibility to your SAP Supply Chain and related business systems



Monitoring of SAP and its applications for real-time security



Slash MTTR and Root Cause Analysis on SAP and associated systems by 70%



Reduce P1 issues with your SAP & Interrelated systems by 30%



```
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D1SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Opera/9.80 (Win  
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=FI-SW-01" "Opera/9.80 (Win  
ows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.11.18 "GET /oldlink?item_id=EST-26&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=FI-SW-01" "Opera/9.80 (Win  
item_id=EST-16&product_id=RP-LI-02" 468 125.17 14.11.18 "GET /oldlink?item_id=EST-26&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=FI-SW-01" "Opera/9.80 (Win  
do?action=purchase&itemId=EST-6&product_id=FI-SW-01" 468 125.17 14.11.18 "GET /oldlink?item_id=EST-26&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=FI-SW-01" "Opera/9.80 (Win  
buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=FI-SW-01" "Opera/9.80 (Win
```

Truth #2: Heroes Target Projects with Business Impact



Age

47yr

Revenue

\$23B

Fortune 500
Customers

87%

Global Revenue
Touched

77%

Users

12M

Installations

121K

Customers

41K

Countries

120

Partners

1500

Truth #3: Heroes Understand Risk & Reward

SAP® Certified
Integration with SAP S/4HANA®



amazon
web services

Partner
Network

ADVANCED CONSULTING PARTNER

**24X7
Support**

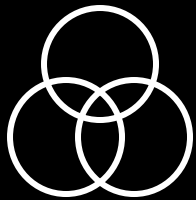
splunk>partner+

Product Investments

4+ years and counting as well release of new
feature pack every 6 months¹

**Splunk Accredited
Implementation Services**

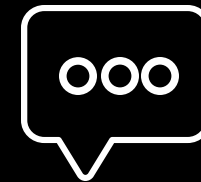
Why is Splunking SAP a 'Hero' Project?



SAP systems are complex, real-time, and mission critical



SAP has limited alerting and visualization



SAP cannot do real-time or historical data correlations

SAP Journey

The DNA required and the areas to focus on

► Hero DNA

- Change Agent
- Collaborative
- Natural leader
- Vision
- Trusted
- Creative
- Business & Technical chops

► SAP Use Cases

- Security
- Supply Chain
- Performance
- Cloud Migration
- IOT
- Phantom
- Compliance
- Monitoring Outsourced SAP SLA's

Security Hero

David Clawson

Principal, Growth
Splunk YODA

SAP Security & Compliance

PowerConnect sends events to Splunk that are named after the T-Code or report typically used to access them. Examples include SM20, SU01, SUIM, SCC4, SMICM, SM04, AL08, RSUSR200, RZ10, STAD, etc

All Security relevant transactions and user activity:

- Geographic view of system usage
- Anomalies in system log, e.g. increased message frequency
- Critical user activity – Role and Permission Changes
- Fraud Detection and Alerting
- Super Admin “Firefighter” ID monitoring
- Password Complexity monitoring

SAP Security Essentials

Edit Export ...

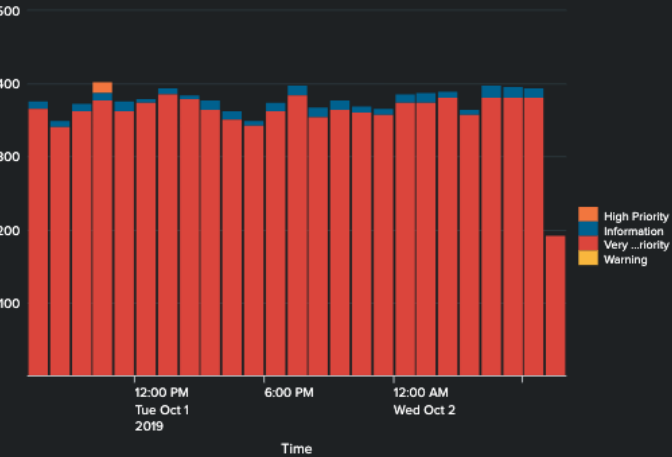
Range SAP System

Last 24 hours ID7 X Hide Filters

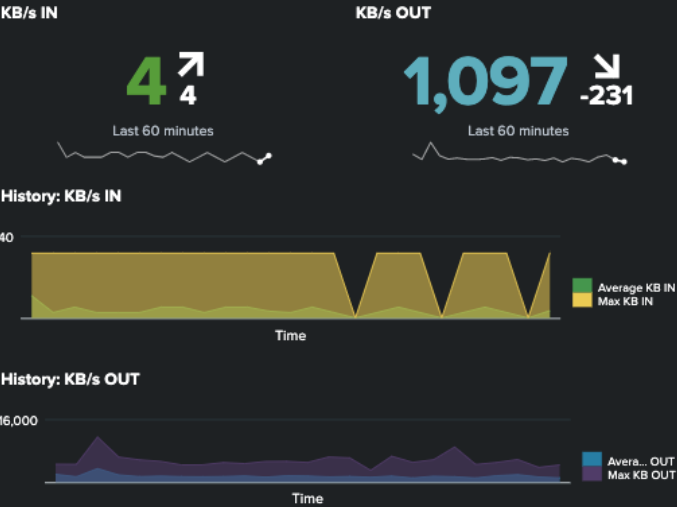
Authentication Activity



System Logs



Network Activity



Security Scorecard

Passed	Failed
9	10
Security Case	
Login by privileged user	2
Users having excessive rights	58
Privileged SAP users enabled	10
Users with default or well known password	3475
Client open for change	7

Number of Logged in Users (Geo)

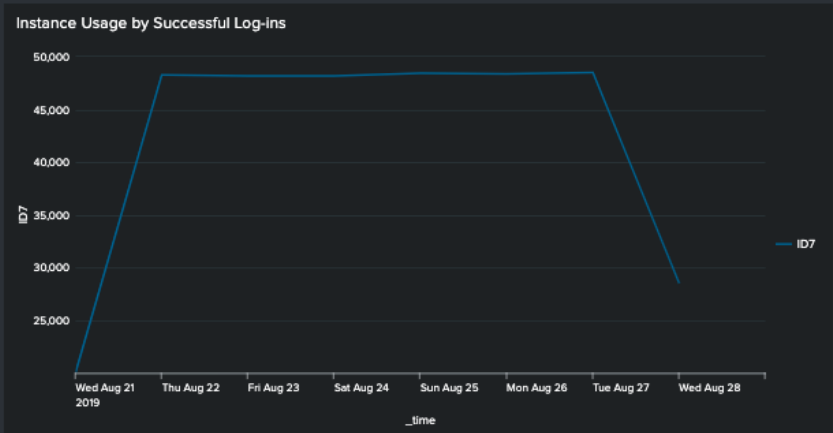


Security Scorecard

Edit Export ▾ ...

Range SAP System
Last 24 hours ▾ ID7 ▾ X [Hide Filters](#)

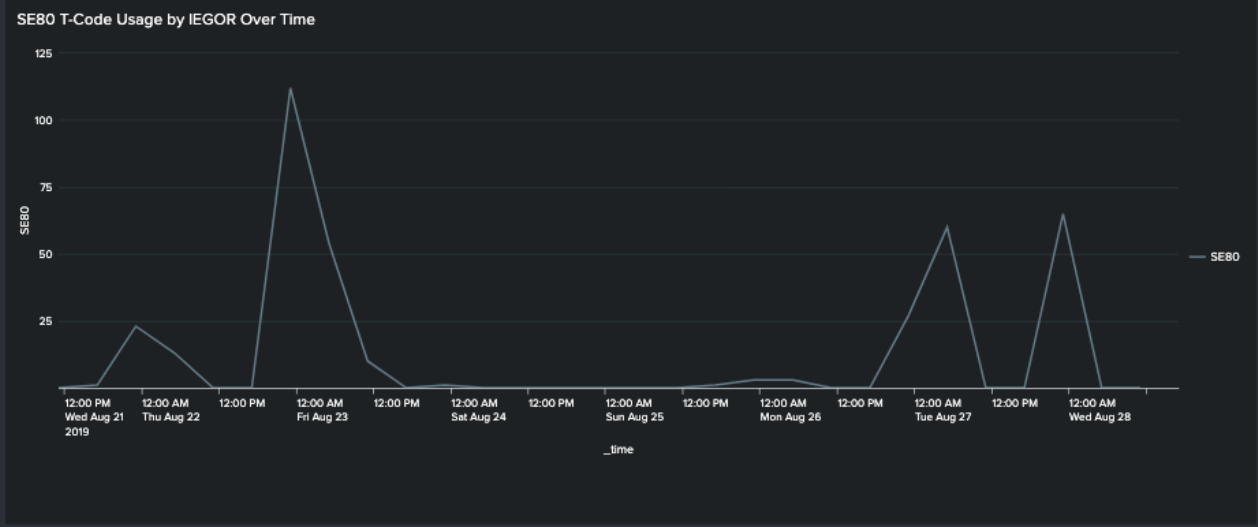
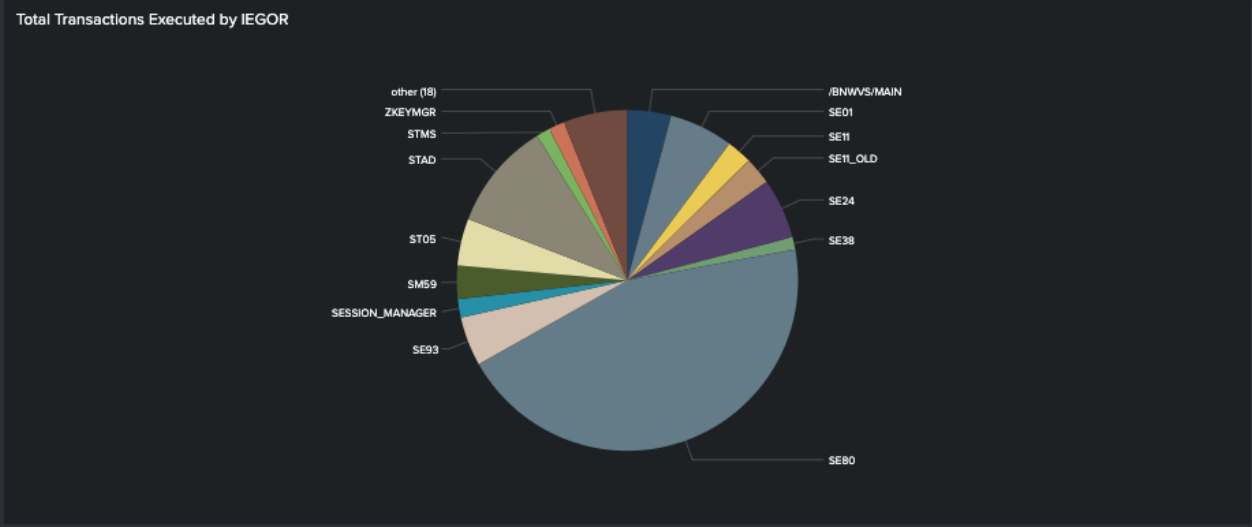
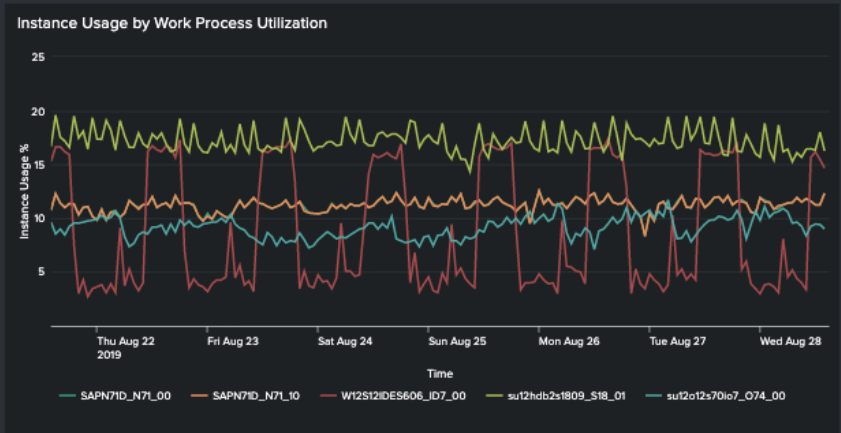
Total No. of Checks		No. of Checks Passed		No. of Checks Failed	
19		7		12	
Login by privileged user		Users having excessive rights		Privileged SAP users enabled	
1		58		10	
Users with default or well known password					
3,475					
Client open for change		Namespace open for change		Login by multiple IDs on 1 terminal	
7		235		1	
				Multiple logins by 1 ID on different terminals	
				0	
				Login by 1 ID in different geos	
				0	
Password policy parameters		Debug mode used		User type changed	
5		1		0	
				Downloaded a file (NW7.31+)	
				1	
				Active users not logged in for 30 days or more	
				4,163	
Execution of sensitive transactions		Users with sensitive authorization		Users with dev keys	
0		0		143	
				Failed logons from multiple users on 1 terminal	
				0	
				Change in RFC destination	
				0	



Top Users

	Logins
ALGUSER	
TECHIDATA	2384
SOLOMON	1847
BOHNSTEDT	678
IEGOR	529
SAP*	193
BUCHERT	179
CM_DEMO_LP	185
CM_BATCH	42
MICHALSKY	37
SDCAUTO	35

« prev123next »



SAP Global Transactions By IEGOR (raw)

Transactions	Average	Response Time	CPU Time	Transactions Performed	Max Value	Exceeded Threshold	Roll In Count	Roll In Time	Roll Out Count	Roll Out Time	Roll Time	Lock Count	Lock Time	Database Calls	Database Call Time	Dialog Steps	GUI Net Time	GUI time	Maximum Memory	Max Page Memory	Max Roll Memory	Processor Time	Act_encode	Roll Wait Time	Threshold
SE80	-1.56	1835.18	111.47	50896	2722.00	5461	3.42	2.69	3.43	2.05	1072.15	3.57	0.64	387.06	301.34	273.36	369.43	998.92	37506.92	0.00	150.40	439.73	af77527ac4361ea988e181fc62c55a99	2.37	3.00
/BNWVS/MAIN	-2.75	7312.70	434.40	10002	1553.00	1285	2.44	1.91	2.49	1.40	948.81	6.16	13.19	4810.89	743.89	77.11	292.02	1092.89	68788.78	0.00	124.69	4130.88	f971c95906a23491f670bf530028f697	1.66	3.00
SE24	2.62	2640.37	94.44	6347	1265.00	794	3.29	2.05	3.30	2.67	1131.18	1.71	0.34	202.68	574.29	322.52	372.39	1176.72	19077.03	0.00	93.74	904.52	87d52c974d3d6c5c05f0a93ccceb6319	2.36	3.00

Sales Order Fraud Dashboard

Apr 15 through 26, 2019

Submit

Hide Filters

Rush Orders

25[↑]₂₁

Orders Created

61[→]₀

Orders Deleted

0[↘]₋₁

Even Invoice Values						Invoice Amount Anomaly by Vendor						
Sales Invoice # ⇅	Currency ⇅	Net Value ⇅	EntryDate ⇅	EntryTime ⇅	isEven ⇅	is_outlier ⇅	Sales Invoice # ⇅	Currency ⇅	Net Value ⇅	Sales Group ⇅	EntryDate ⇅	EntryTime ⇅
0000050985	EUR	1656.80	2019-04-25	15:25:12	Non-Even	YES	0005987342	EUR	416700.00	101	2019-03-11	16:32:52
0000050984	EUR	4142.00	2019-04-25	15:23:22	Even Price	NO	0000050985	EUR	1656.80	101	2019-04-25	15:25:12
0000050983	EUR	1303.80	2019-04-25	15:20:55	Even Price	NO	0000050984	EUR	4142.00	101	2019-04-25	15:23:22
0000050982	EUR	3454.20	2019-04-25	15:14:51	Even Price	NO	0000050983	EUR	1303.80	101	2019-04-25	15:20:55
0000050980	EUR	3300.00	2019-04-25	15:04:40	Even Price	NO	0000050982	EUR	3454.20	101	2019-04-25	15:14:51
« prev 1 2 3 next »						« prev 1 2 3 4 next »						

Sales Orders Deleted			Deleted Sales Order v2		
_time ↕	SalesOrderNumber ↕	DeletedBy ↕	_time ↕	SalesOrderNumber ↕	Username ↕
2019-04-17 12:18:48	0000049461	MATTC	2019-04-17 17:36:49	0000049461	MATTC

Drilldown Details

Order Information:

Sales Order0000049461

Group ID/Organization ID101/1000

Order Currency and AmountEUR 1151.40

Create Date2019-04-18 05:15:33

Created ByMATTC

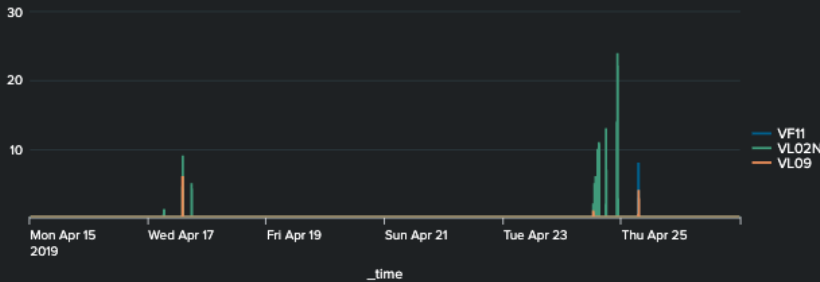
Deletion Date2019-04-17T12:18:48.000-07:00

Deleted ByMATTC

User Roles

Profile ↕	AGName ↕
IDES_IDA_SUP	Z_BNWVS_ADMIN_ALL_TASKS
IDES_SWITCH	Z_BNWVS_ADMIN_CHANGE
R3_TRUSTED	
SAP_ALL	
SAP_NEW	
S_USER_AUTH	
T-A4240002	
T-N1070002	

Transactions by User



Role & Profile Assignment										Summary of Actions Taken by User	
_time ↕	ACTION ↕	ATTRBT ↕	BNAME ↕	MODBE ↕	MODDA ↕	MODTI ↕	NEW_TEXT ↕	NEW_VAL ↕	TCODE ↕	ALGUSER ↕	Summary of Actions Taken ↕
2019-04-24 06:50:57	Password status changed	USR02-PWDINITIAL	DBURNS	MATTC	20190424	235057		Initial	SU01	MATTC	Authorizations for User DBURNS Changed
2019-04-24 06:50:57	Password changed	USR02-BCODE	DBURNS	MATTC	20190424	235057		New	SU01		Download 13515 Bytes to File C:\Users\Matt Colabrese\Do...\SAP GUI\fosail_order.htm Dynamic ABAP Coding: Event - Event Type: D! Checksum: /1SAI/SAS48B6E529E15551961A0C=XT Dynamic ABAP Coding: Event - Event Type: D! Checksum: /1SAI/SAS48B6E529E15551961A0C=XTI Dynamic ABAP Coding: Event - Event Type: D! Checksum: /1SAI/SAS59CC40E6F5FFCD4F11AE=XT

SAP SECURITY MATURITY MODEL

MATURITY



- Super Admin Monitoring
- Splunk SAP Security



SAP Monitoring
With SolMan -
99 Hours of
Data Retention



Sending
SM20 Logs
to Splunk



SAP Security
Data in Splunk -
90 Days of
Data Retention



Custom SAP
Security
Dashboards and
Alerts In Splunk



SAP Firefighter
ID Tracking
and Alerting
In Splunk



Real-Time
SAP Order
Fraud Alerting



SAP Data In
Splunk ES
With Phantom
Automation
and Response



Business Hero

David Clawson

Principal, Growth
Splunk YODA

Typical Fortune 500 Company

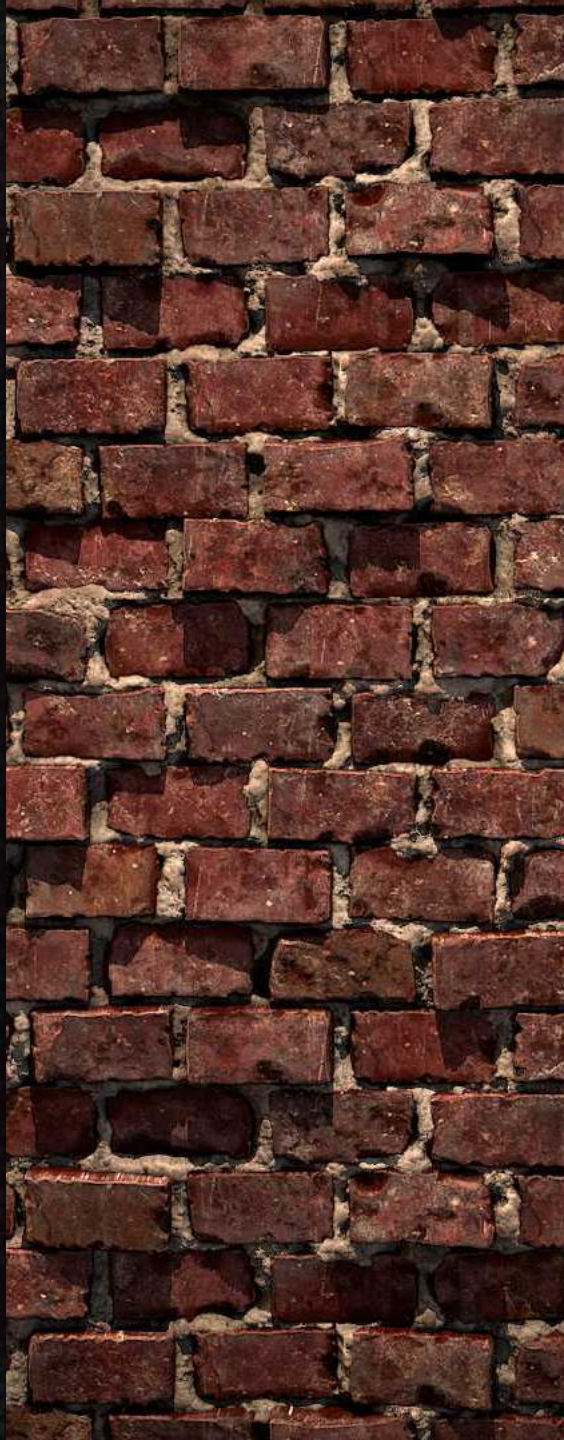
The Cost of Downtime

\$10,000,000
per minute

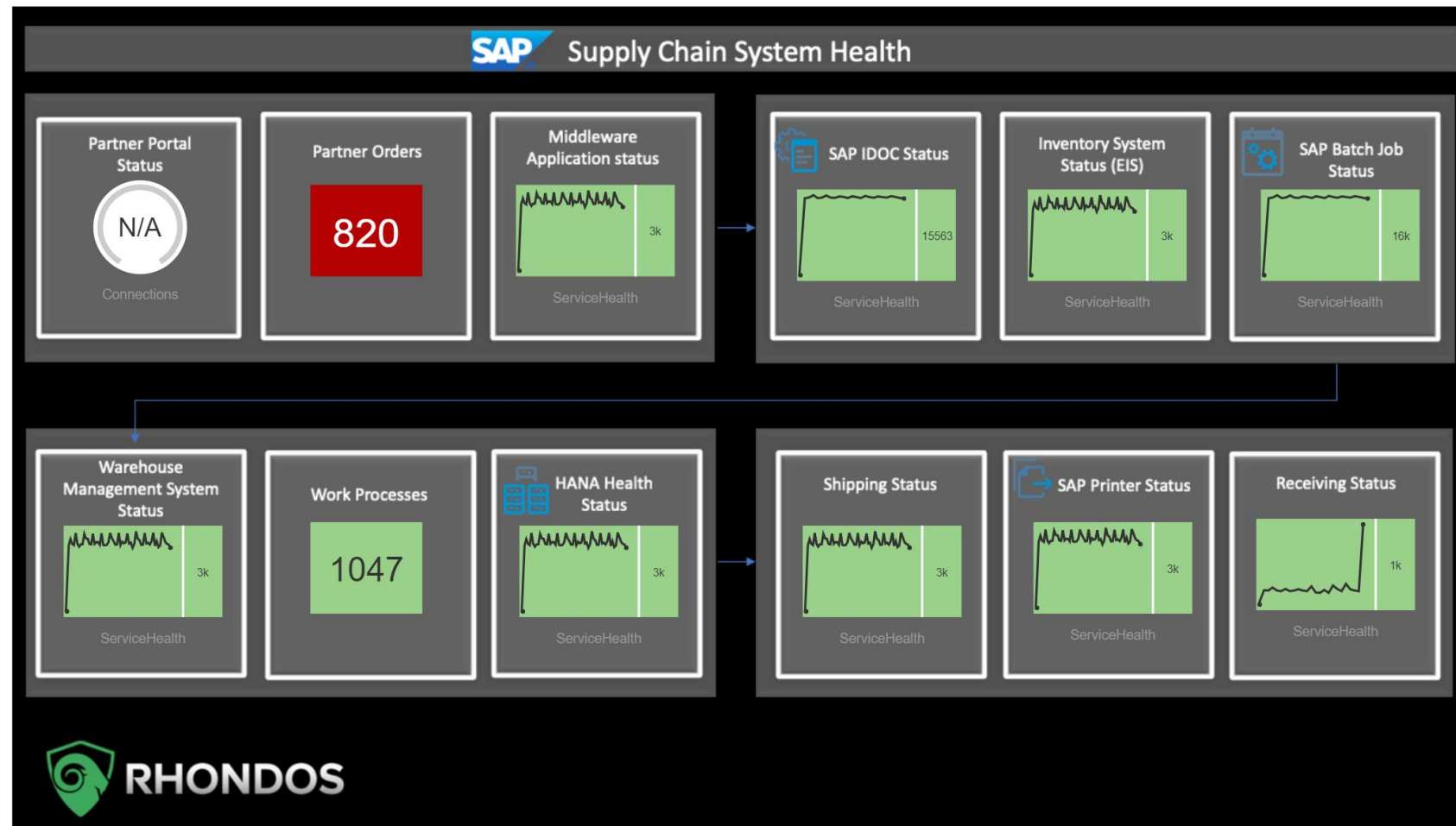
Average Busiest Day

30%
Uptime
Improvements

70%
MTTR

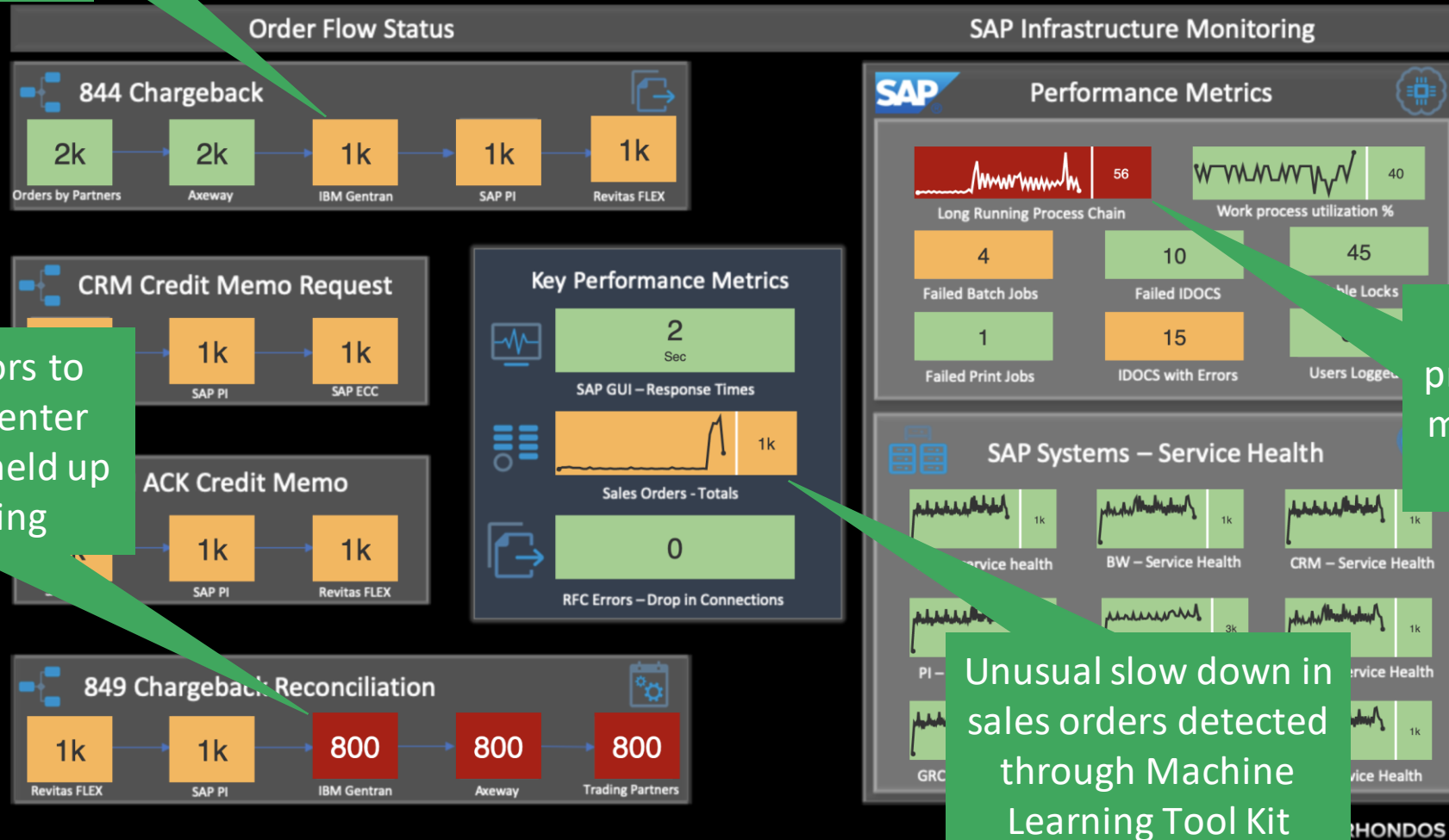


Use Case Example: Supply Chain System Health



Big Pharma Charge Back

IBM Gentran stands out in two areas as a process bottleneck



Interface errors to distribution center printers have held up Bills of Lading

Downstream processing for critical management reports is held up by IBM

Unusual slow down in sales orders detected through Machine Learning Tool Kit

Example of unplanned SAP outage impacting:

- ▶ Logistics execution
 - big orders to major accounts
- ▶ SAP Not printing
 - big orders don't role
- ▶ Order on Truck but Truck not rolling
 - trucks bill of lading can't print from SAP
 - wrong paperwork
 - service bus failed to complete in SAP
- ▶ Big wholesale orders
 - Order Somehow wrong
 - ran order on old data
 - didn't see that batch jobs
 - or input from middle ware
- ▶ Not filling
 - big orders don't leave the doc



SM58

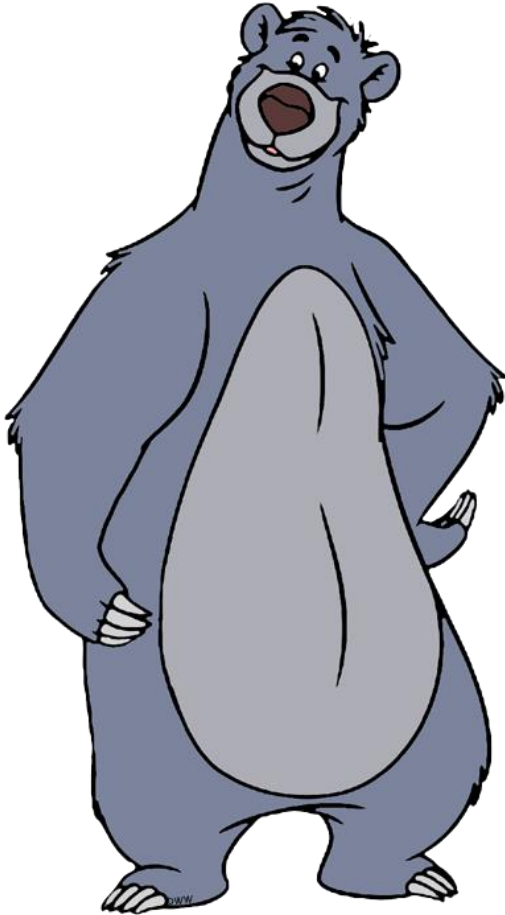
Failures
Successes
Transactions

IDOC

Performance Hero

Matt Colabrese
Principal Consultant
Director of Customer Success

What does it take to get PowerConnect running?



- ▶ Two hours for prep and prerequisites
- ▶ One hour to install the SAP Add-On
- ▶ Two hours to configure the SAP Add-On
- ▶ Three hours to validate data and tweak lookups



SAP Daily Checklist

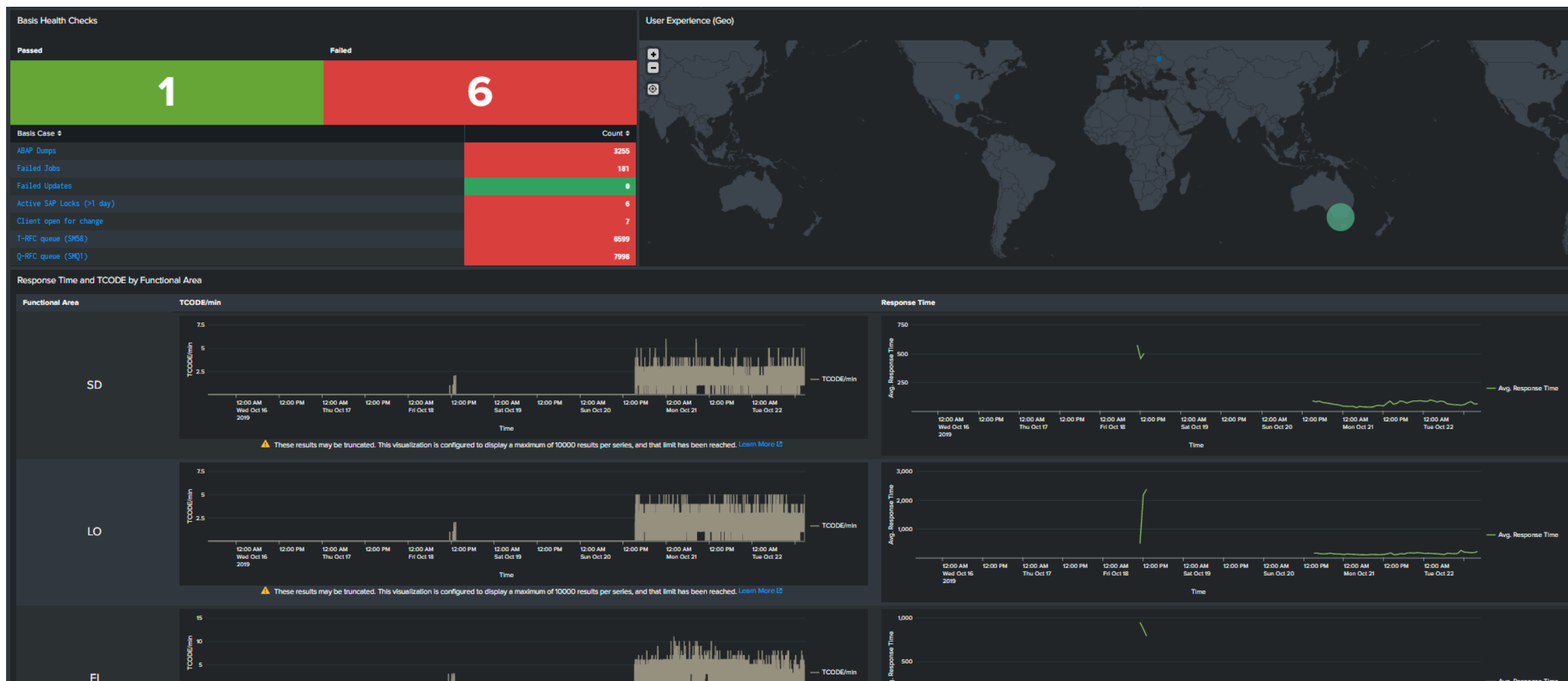
Reduce or eliminate the manual time associated with monitoring SAP uptime





SAP Daily Checklist

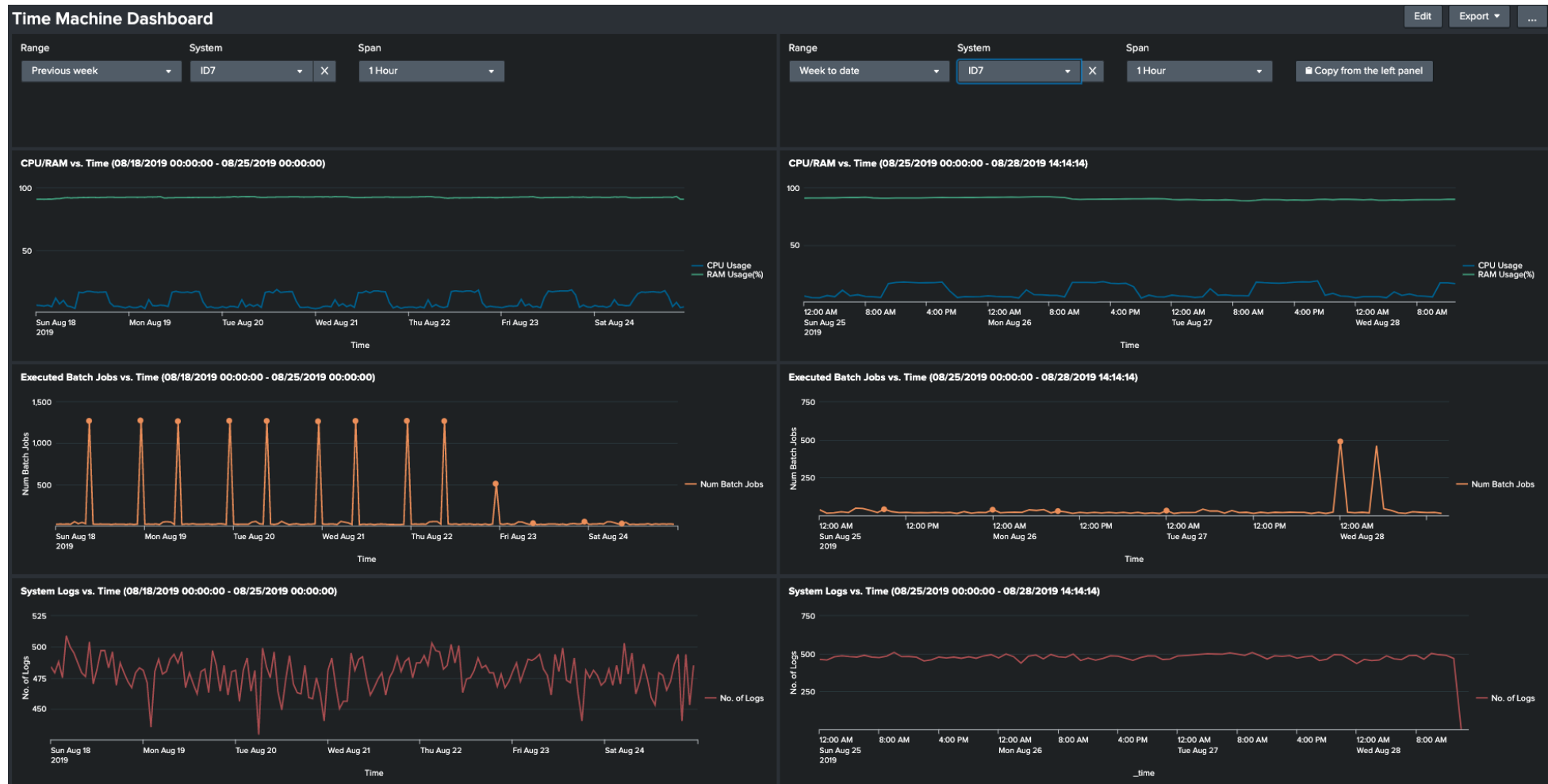
Reduce or eliminate the manual time associated with monitoring SAP uptime





SAP Time Machine

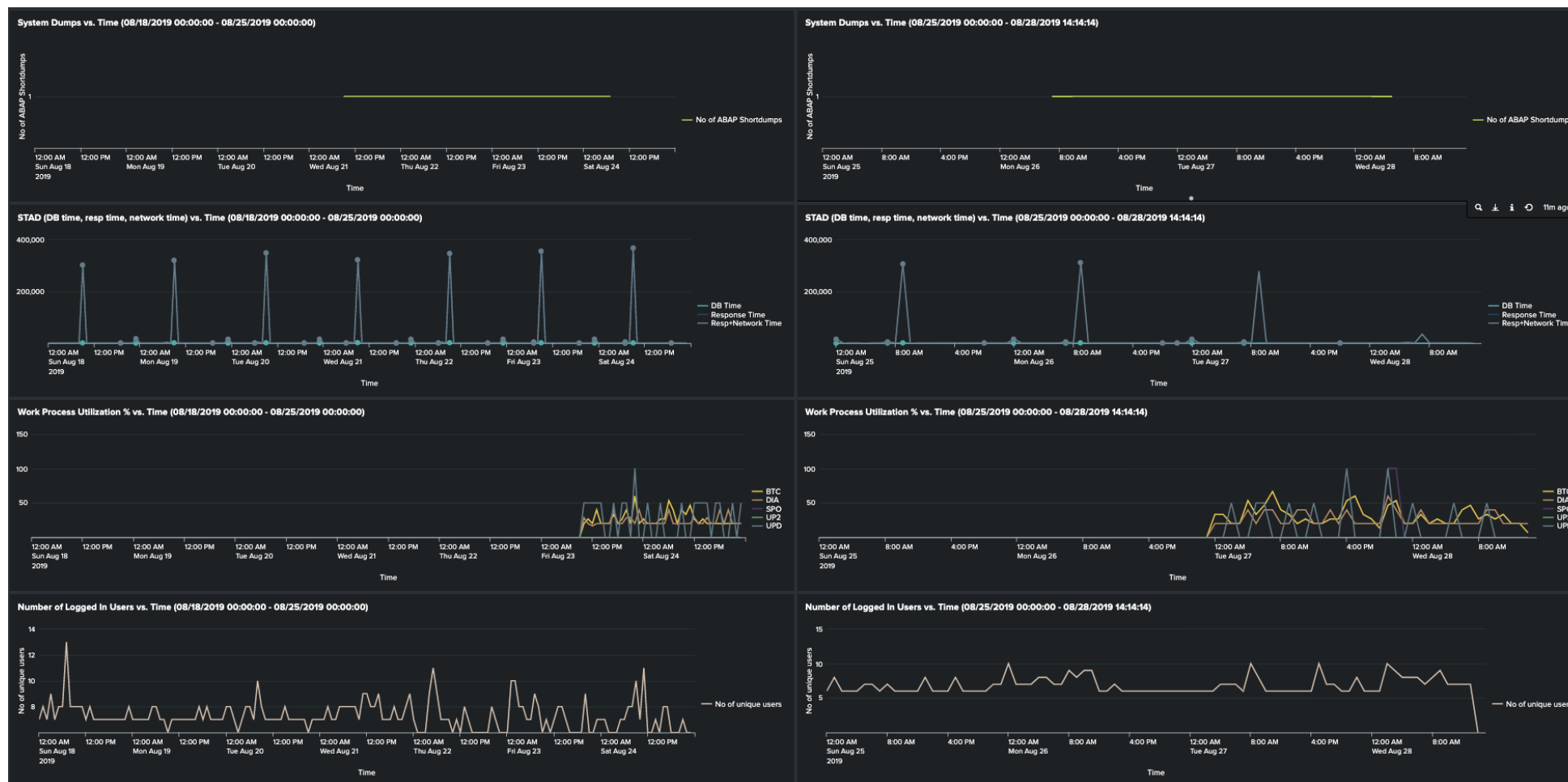
Provide unprecedented views comparing SAP performance at different times





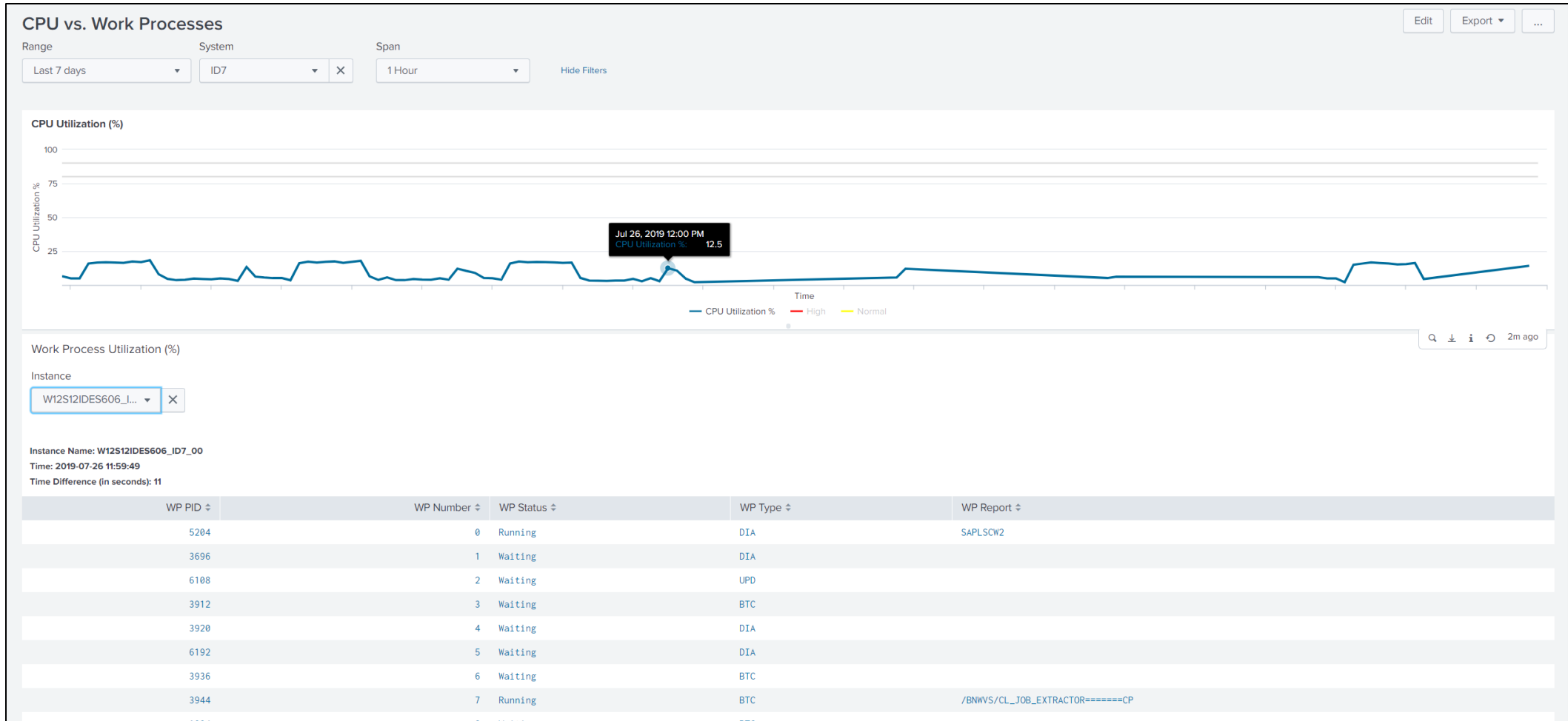
SAP Time Machine

Provide unprecedented views comparing SAP performance at different times



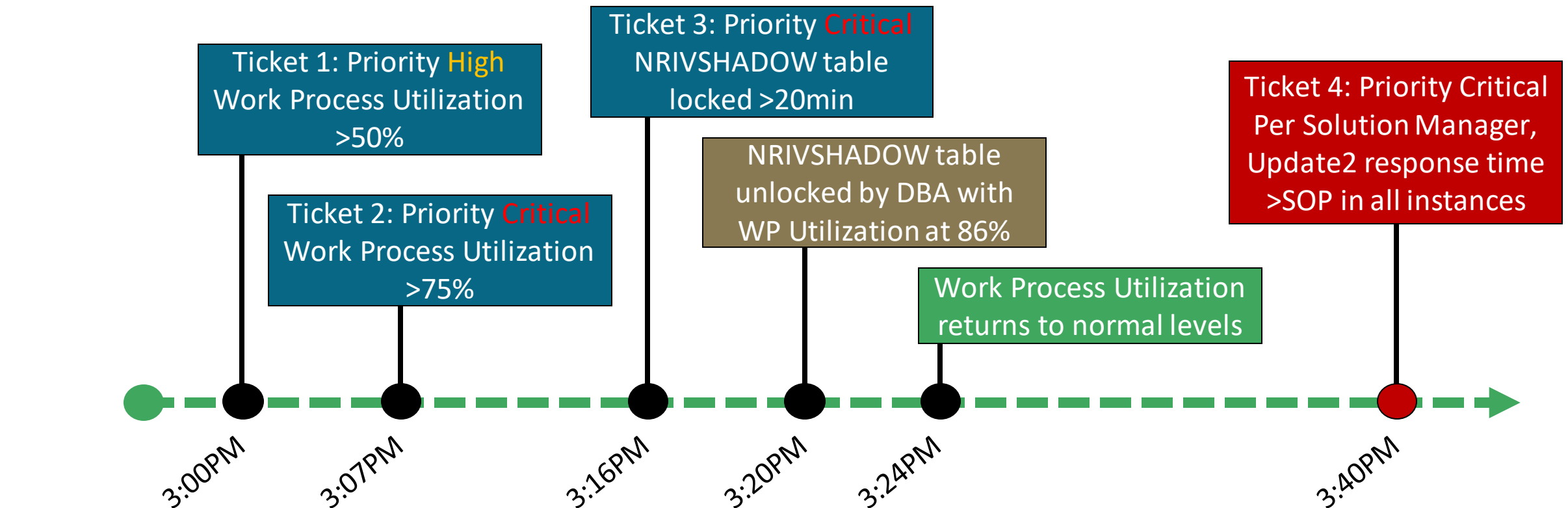
SAP Performance Snapshots

Conduct root cause analysis of performance issues with time correlation searches



Real-Time Alerts & Visibility

Achieve NEGATIVE(!) mean time to resolution by fixing issues before they escalate



Typical Benefits & Return on Investment



Reduce manual monitoring efforts by internal/offshore teams by 50%



Accelerate cumbersome compliance audits and mitigate insider threat



Slash MTTR and RCA of issues across SAP systems and interfaces by 70%



Eliminate 30% of your annual P1/P2 tickets and spend less time in war rooms

Find out more at



Splunk Guest Blog
Splunking SAP and Turning Data
into Action
<https://www.splunk.com/blog/2019/09/19/splunking-sap-and-turning-data-into-action.html>



Biweekly Webinars

October 16th 2:00 PM EST – BE THE HERO

OCTOBER 31ST 1:00 pm EST – INVESTIGATING SAP IN REAL TIME!

www.rhondos.com/webinar



Tera Booth #174

Thank You!

**RHONDOS**info@rhondos.com

Key Use Cases for “Splunking” SAP

Security	Performance	Migration	Business Flow
SAP Data Analysed • Full SM20 audit log • User location, profiles, roles • User reports and system log Insights Provided • Analysis of troublesome or unexpected login behavior • Geographic view of system usage. • Anomalies in system log, e.g. increased message frequency. • UI details e.g. versions.	SAP Data Analysed • Application, GUI, transaction response times (STAD) • SAP uptime & availability • Real time database health Insights Provided • Real-time and historic view of load and response by user, transaction code or any field in the dataset. • Availability of SAP solution components.	SAP Data Analysed • User Activity and Security Access logs • Custom program utilization • Uptime & response time comparisons to legacy • HANA health & consistency checks Insights Provided • Current state benchmarking • Integrator accountability • Go-Live confidence	SAP Data Analysed • Batch job execution statistics • IDOC & change documents processing • PI/PO message processing Insights Provided • Status of critical business processes. • Business process context via IDOC content, e.g. sales data or PO without PR.