Splunk And SCADA – Soul Mates Forever

Chris Duffey

SCADA Coordinator, SCADA Infrastructure & Cyber Security

Enterprise Products Partners

.conf2016

splunk>

Disclaimer

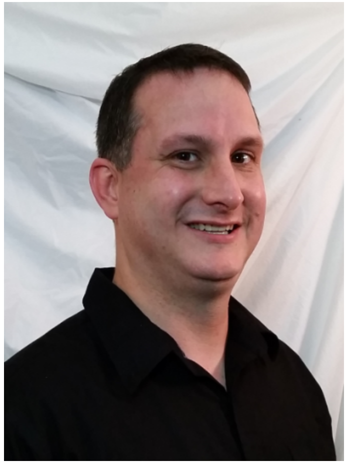
During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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

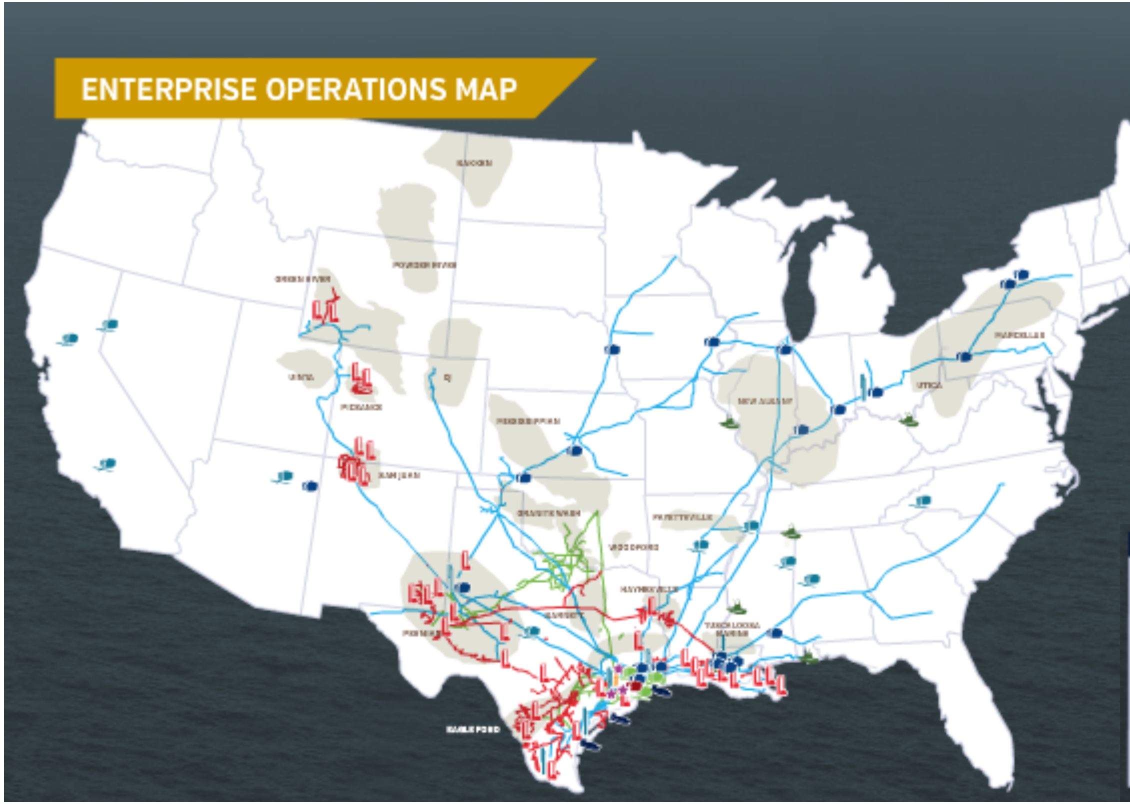
- Introduction
- Where Were We?
- Where Are We?
- Where Are We Going?

Introduction

- Chris Duffey, SCADA Coordinator at Enterprise Products
- Worked in SCADA for ~10 years
  - Internal Development on in-house SCADA system
  - System Support
  - Infrastructure & Cyber Security
- Working with Splunk for 18 months



Introduction



MAP KEY
VIEW GULF COAST
RESET MAP
NATURAL GAS PIPELINE
NGL/REFINED PRODUCTS PIPELINE
CRUDE OIL PIPELINE
CRUDE OIL TERMINAL
NGL/REFINED PRODUCTS TERMINAL
NATURAL GAS PROCESSING/TREATING PLANT
OCTANE ENHANCEMENT FACILITY
ISOMERIZATION FACILITY
NGL/REFINED PRODUCTS STORAGE
NATURAL GAS STORAGE
NGL/PROPYLENE FRACTIONATION FACILITY
IMPORT/EXPORT TERMINAL
MARINE SERVICES
MAJOR PRODUCING BASIN

Enterprise Products Partners L.P.

Introduction

OT vs IT

- Technologies
  - Proprietary
  - Legacy (30+ years) and New
  - Isolation (no Internet connection)
  - 24-7 365 Days a year (no downtime)
- Safety Culture
  - Patching and Approved Software
  - No automated “fixes”
  - “If it ain’t broke, don’t fix it” - cost

Where We Were

Where We Were

How We Got Started

- Evaluation of SEIM Products began in 2013
- Looked for Vendor Approved products
- Began looking at TCO and full value of products
- Initial system that was quoted would have cost $600+ K for initial investment
- Looked for tools that could do more with less
- In August 2014, POV "Proof Of Value" with Splunk

Where We Were

Our Story

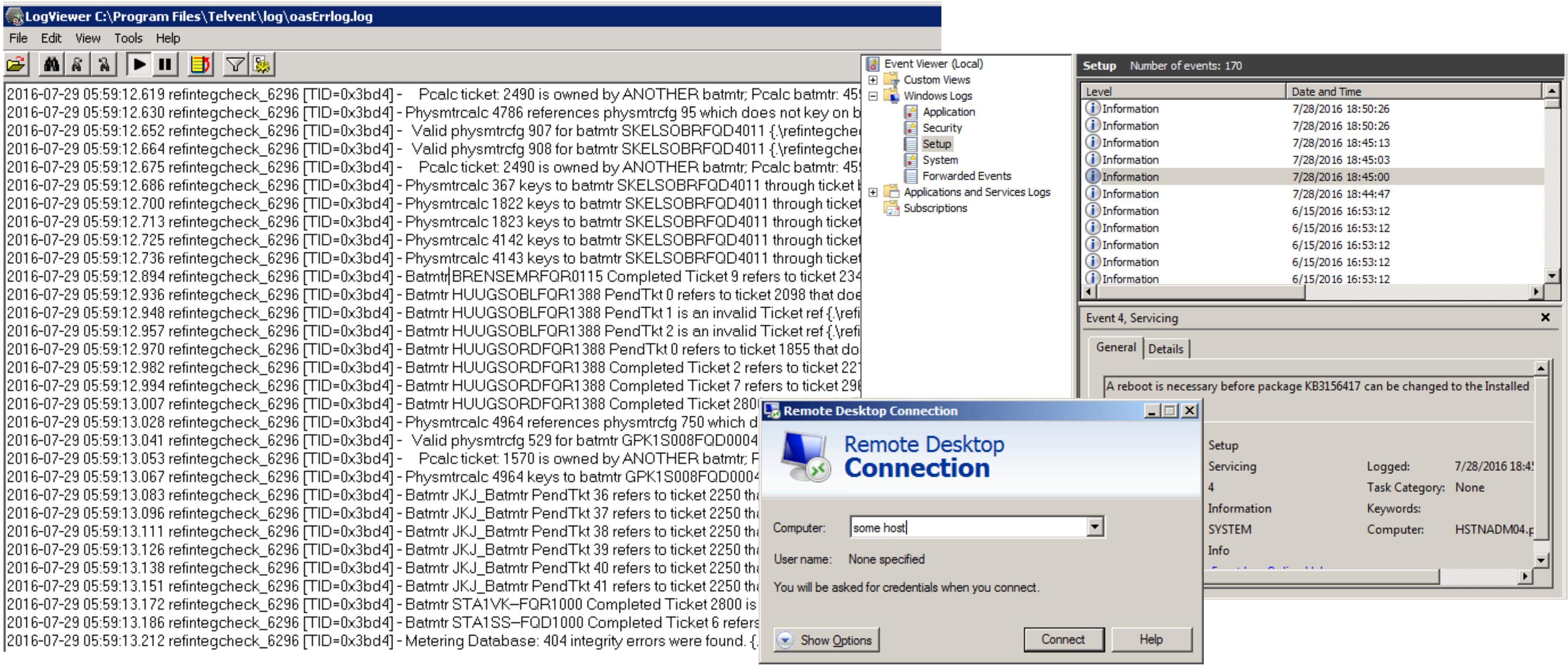
- New SCADA System Implementations
  - Legacy systems would remain for 2+ years
  - Need to support both older and new technologies
  - Need to use existing resources
- Everything was reacting after critical issues
- Difficulties meeting SLA's (Regulatory)
- Increased focus on cyber security of SCADA Systems

Where We Were

Our Tools

- Vendor provided tools limited or required a lot of time
  - Lots of time logging into server
  - Alerting capabilities were limited and not customizable
- Lots of available tools
  - Not approved by vendor
  - Not suitable for SCADA environment
- Vendor claims on system resources and sizing was not always accurate

Troubleshooting



LogViewer C:\Program Files\Telvent\log\oasErrlog.log
File Edit View Tools Help

```
2016-07-29 05:59:12.619 refintegcheck_6296 [TID=0x3bd4] -   Pcalc ticket: 2490 is owned by ANOTHER batmtr; Pcalc batmtr: 45
2016-07-29 05:59:12.630 refintegcheck_6296 [TID=0x3bd4] - Physmtrcalc 4786 references physmtrcfg 95 which does not key on b
2016-07-29 05:59:12.652 refintegcheck_6296 [TID=0x3bd4] -  Valid physmtrcfg 907 for batmtr SKELSOBRFQD4011 {.\refintegche
2016-07-29 05:59:12.664 refintegcheck_6296 [TID=0x3bd4] -  Valid physmtrcfg 908 for batmtr SKELSOBRFQD4011 {.\refintegche
2016-07-29 05:59:12.675 refintegcheck_6296 [TID=0x3bd4] -   Pcalc ticket: 2490 is owned by ANOTHER batmtr; Pcalc batmtr: 45
2016-07-29 05:59:12.686 refintegcheck_6296 [TID=0x3bd4] - Physmtrcalc 367 keys to batmtr SKELSOBRFQD4011 through ticket
2016-07-29 05:59:12.700 refintegcheck_6296 [TID=0x3bd4] - Physmtrcalc 1822 keys to batmtr SKELSOBRFQD4011 through ticket
2016-07-29 05:59:12.713 refintegcheck_6296 [TID=0x3bd4] - Physmtrcalc 1823 keys to batmtr SKELSOBRFQD4011 through ticket
2016-07-29 05:59:12.725 refintegcheck_6296 [TID=0x3bd4] - Physmtrcalc 4142 keys to batmtr SKELSOBRFQD4011 through ticket
2016-07-29 05:59:12.736 refintegcheck_6296 [TID=0x3bd4] - Physmtrcalc 4143 keys to batmtr SKELSOBRFQD4011 through ticket
2016-07-29 05:59:12.894 refintegcheck_6296 [TID=0x3bd4] - Batmtr BRENSEMRFQR0115 Completed Ticket 9 refers to ticket 234
2016-07-29 05:59:12.936 refintegcheck_6296 [TID=0x3bd4] - Batmtr HUUGSOBLFQR1388 PendTkt 0 refers to ticket 2098 that doe
2016-07-29 05:59:12.948 refintegcheck_6296 [TID=0x3bd4] - Batmtr HUUGSOBLFQR1388 PendTkt 1 is an invalid Ticket ref {.\refi
2016-07-29 05:59:12.957 refintegcheck_6296 [TID=0x3bd4] - Batmtr HUUGSOBLFQR1388 PendTkt 2 is an invalid Ticket ref {.\refi
2016-07-29 05:59:12.970 refintegcheck_6296 [TID=0x3bd4] - Batmtr HUUGSORDFQR1388 PendTkt 0 refers to ticket 1855 that do
2016-07-29 05:59:12.982 refintegcheck_6296 [TID=0x3bd4] - Batmtr HUUGSORDFQR1388 Completed Ticket 2 refers to ticket 22
2016-07-29 05:59:12.994 refintegcheck_6296 [TID=0x3bd4] - Batmtr HUUGSORDFQR1388 Completed Ticket 7 refers to ticket 29
2016-07-29 05:59:13.007 refintegcheck_6296 [TID=0x3bd4] - Batmtr HUUGSORDFQR1388 Completed Ticket 280
2016-07-29 05:59:13.028 refintegcheck_6296 [TID=0x3bd4] - Physmtrcalc 4964 references physmtrcfg 750 which d
2016-07-29 05:59:13.041 refintegcheck_6296 [TID=0x3bd4] -  Valid physmtrcfg 529 for batmtr GPK1S008FQD0004
2016-07-29 05:59:13.053 refintegcheck_6296 [TID=0x3bd4] -   Pcalc ticket: 1570 is owned by ANOTHER batmtr; P
2016-07-29 05:59:13.067 refintegcheck_6296 [TID=0x3bd4] - Physmtrcalc 4964 keys to batmtr GPK1S008FQD0004
2016-07-29 05:59:13.083 refintegcheck_6296 [TID=0x3bd4] - Batmtr JKJ_Batmtr PendTkt 36 refers to ticket 2250 th
2016-07-29 05:59:13.096 refintegcheck_6296 [TID=0x3bd4] - Batmtr JKJ_Batmtr PendTkt 37 refers to ticket 2250 th
2016-07-29 05:59:13.111 refintegcheck_6296 [TID=0x3bd4] - Batmtr JKJ_Batmtr PendTkt 38 refers to ticket 2250 th
2016-07-29 05:59:13.126 refintegcheck_6296 [TID=0x3bd4] - Batmtr JKJ_Batmtr PendTkt 39 refers to ticket 2250 th
2016-07-29 05:59:13.138 refintegcheck_6296 [TID=0x3bd4] - Batmtr JKJ_Batmtr PendTkt 40 refers to ticket 2250 th
2016-07-29 05:59:13.151 refintegcheck_6296 [TID=0x3bd4] - Batmtr JKJ_Batmtr PendTkt 41 refers to ticket 2250 th
2016-07-29 05:59:13.172 refintegcheck_6296 [TID=0x3bd4] - Batmtr STA1VK–FQR1000 Completed Ticket 2800 is
2016-07-29 05:59:13.186 refintegcheck_6296 [TID=0x3bd4] - Batmtr STA1SS–FQD1000 Completed Ticket 6 refers
2016-07-29 05:59:13.212 refintegcheck_6296 [TID=0x3bd4] - Metering Database: 404 integrity errors were found. {
```

Setup Number of events: 170

Level	Date and Time
Information	7/28/2016 18:50:26
Information	7/28/2016 18:50:26
Information	7/28/2016 18:45:13
Information	7/28/2016 18:45:03
Information	7/28/2016 18:45:00
Information	7/28/2016 18:44:47
Information	6/15/2016 16:53:12
Information	6/15/2016 16:53:12
Information	6/15/2016 16:53:12
Information	6/15/2016 16:53:12
Information	6/15/2016 16:53:12

Event 4, Servicing

A reboot is necessary before package KB3156417 can be changed to the Installed

Setup			
Servicing		Logged:	7/28/2016 18:4
4		Task Category:	None
Information		Keywords:	
SYSTEM		Computer:	HSTNADM04.p
Info			

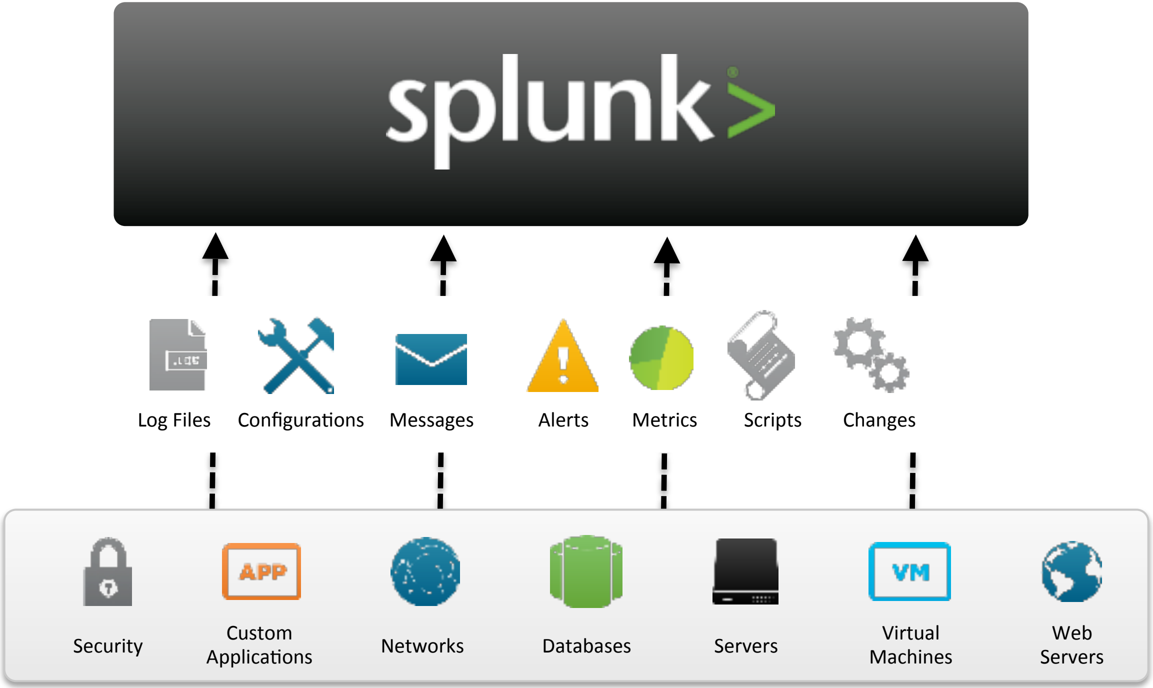
Computer: some host

User name: None specified

You will be asked for credentials when you connect.

Where We Are

Where We Are



- System Overviews and Stability
- Security
- SLA
- Reporting and Empowering other groups

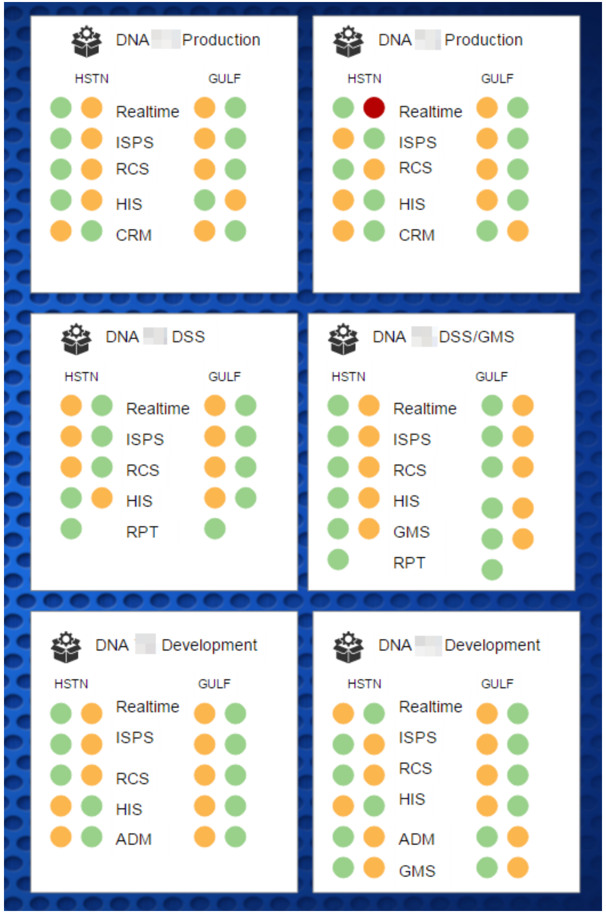
Where We Area

- Splunk Enterprise 225 GB Daily
  - Windows, Unix, Linux, SCADA Applications, Third Party Logs, Interface Logging, Environment Monitoring, etc.
- Splunk for Enterprise Security 50 GB Daily
  - Palo Alto, Active Directory, iLO, VPN, RDP, etc.
- Splunk for VMware 50 GB Daily
- Splunk IT Service Intelligence 50 GB Daily

Where We Are

System Overviews

- System States of All systems
- Ability to at a glance see abnormal results
- Correlate system events with other parts of the system
  - Network logs
  - Windows logs
  - Applications logs
  - Security logs



DNA [redacted] Production

HSTN			GULF	
🟢	🟠	Realtime	🟠	🟢
🟢	🟠	ISPS	🟠	🟢
🟢	🟠	RCS	🟠	🟢
🟢	🟠	HIS	🟢	🟠
🟠	🟢	CRM	🟠	🟢

DNA [redacted] Production

HSTN			GULF	
🟢	🔴	Realtime	🟠	🟢
🟠	🟢	ISPS	🟠	🟢
🟢	🟠	RCS	🟠	🟢
🟠	🟢	HIS	🟠	🟢
🟠	🟢	CRM	🟢	🟠

DNA [redacted] DSS

HSTN			GULF	
🟠	🟢	Realtime	🟠	🟢
🟠	🟢	ISPS	🟠	🟢
🟠	🟢	RCS	🟠	🟢
🟢	🟠	HIS	🟠	🟢
🟢		RPT	🟢	

DNA [redacted] DSS/GMS

HSTN			GULF	
🟢	🟠	Realtime	🟢	🟠
🟢	🟠	ISPS	🟢	🟠
🟢	🟠	RCS	🟢	🟠
🟢	🟠	HIS	🟢	🟠
🟢	🟠	GMS	🟢	🟠
🟢		RPT	🟢	

DNA [redacted] Development

HSTN			GULF	
🟢	🟠	Realtime	🟠	🟢
🟢	🟠	ISPS	🟠	🟢
🟢	🟠	RCS	🟠	🟢
🟠	🟢	HIS	🟠	🟢
🟠	🟢	ADM	🟠	🟢

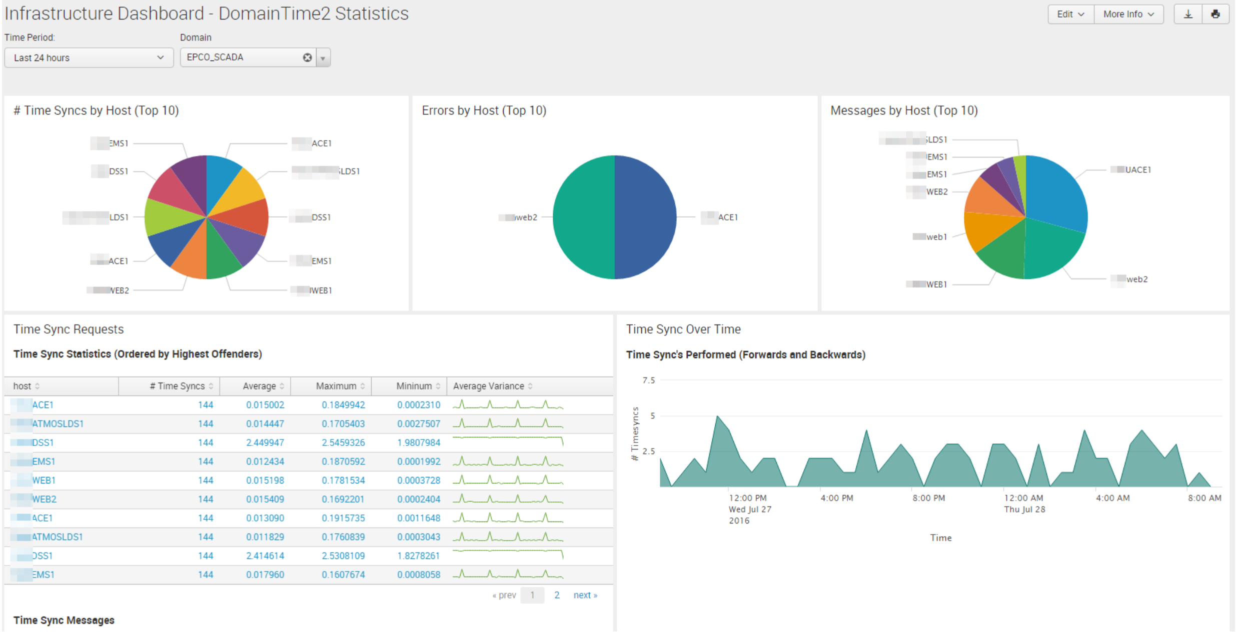
DNA [redacted] Development

HSTN			GULF	
🟠	🟢	Realtime	🟠	🟢
🟢	🟠	ISPS	🟠	🟢
🟢	🟠	RCS	🟠	🟢
🟠	🟢	HIS	🟠	🟢
🟢	🟠	ADM	🟢	🟠
🟢	🟠	GMS	🟢	🟠

Where We Are

System Stability

- Time is important in SCADA (> 5 seconds and things shut down)
- In addition field devices need to be time synched and DST can wreak havoc



Infrastructure Dashboard - DomainTime2 Statistics

Time Period: Last 24 hours

Domain: EPCO_SCADA

Time Sync Requests

Time Sync Statistics (Ordered by Highest Offenders)

host	# Time Syncs	Average	Maximum	Mininum	Average Variance
[redacted]ACE1	144	0.015002	0.1849942	0.0002310	
[redacted]ATMOSLDS1	144	0.014447	0.1705403	0.0027507	
[redacted]DSS1	144	2.449947	2.5459326	1.9807984	
[redacted]EMS1	144	0.012434	0.1870592	0.0001992	
[redacted]WEB1	144	0.015198	0.1781534	0.0003728	
[redacted]WEB2	144	0.015409	0.1692201	0.0002404	
[redacted]ACE1	144	0.013090	0.1915735	0.0011648	
[redacted]ATMOSLDS1	144	0.011829	0.1760839	0.0003043	
[redacted]DSS1	144	2.414614	2.5308109	1.8278261	
[redacted]EMS1	144	0.017960	0.1607674	0.0008058	

« prev 1 2 next »

Time Sync Messages

Time Sync Over Time

Time Sync's Performed (Forwards and Backwards)

Where We Are

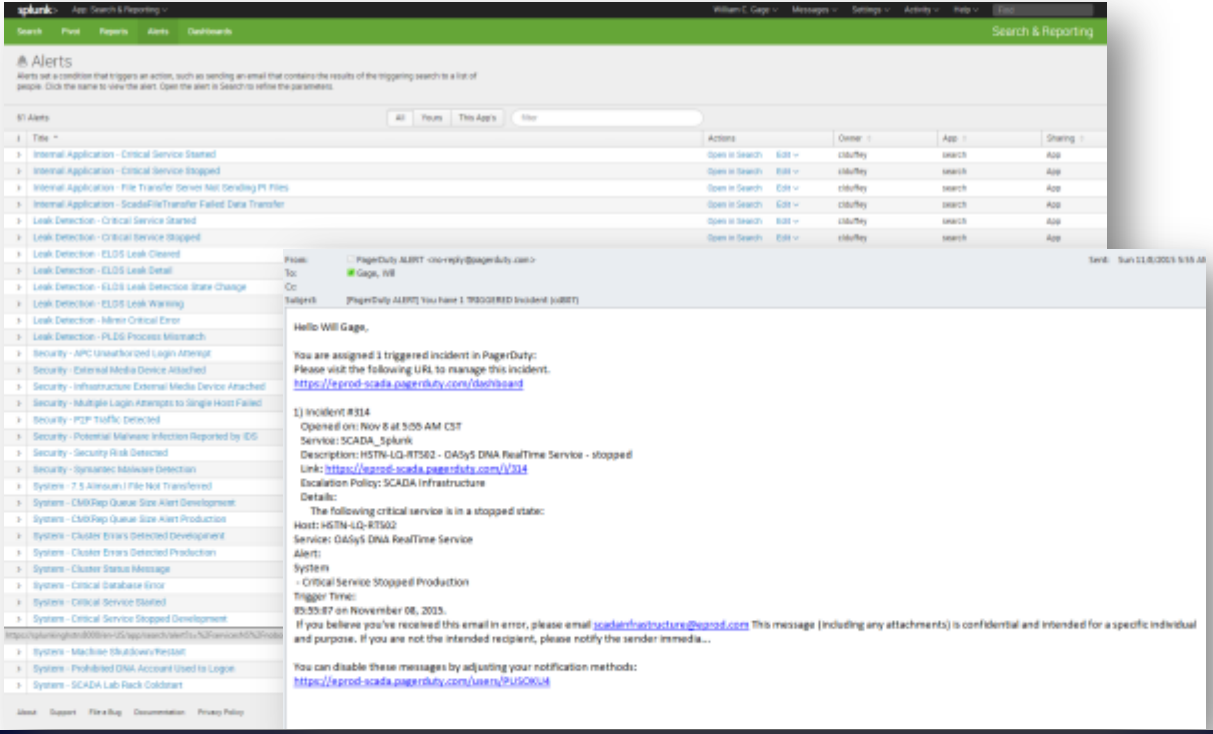
- Alerting and Reporting (SLA)

- Aware of issues within 1~ minute
- Rigorous escalations
- Prescriptive alerting
- Resolution in 4 minutes or less

NOW w/

pagerduty

(This is a legal steroid for SPLUNK!)



Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

61 Alerts

Title	Actions	Owner	App	Sharing
Internal Application - Critical Service Started	Open in Search Edit	cduffey	search	App
Internal Application - Critical Service Stopped	Open in Search Edit	cduffey	search	App
Internal Application - File Transfer Server Not Sending PI Files	Open in Search Edit	cduffey	search	App
Internal Application - ScadaFileTransfer Failed Data Transfer	Open in Search Edit	cduffey	search	App
Leak Detection - Critical Service Started	Open in Search Edit	cduffey	search	App
Leak Detection - Critical Service Stopped	Open in Search Edit	cduffey	search	App
Leak Detection - ELDS Leak Cleared				
Leak Detection - ELDS Leak Detail				
Leak Detection - ELDS Leak Detection State Change				
Leak Detection - ELDS Leak Warning				
Leak Detection - Mimir Critical Error				
Leak Detection - PLDS Process Mismatch				
Security - APC Unauthorized Login Attempt				
Security - External Media Device Attached				
Security - Infrastructure External Media Device Attached				
Security - Multiple Login Attempts to Single Host Failed				
Security - P2P Traffic Detected				
Security - Potential Malware Infection Reported by IDS				
Security - Security Risk Detected				
Security - Symantec Malware Detection				
System - 7.5 Almsum I File Not Transferred				
System - CMXRep Queue Size Alert Development				
System - CMXRep Queue Size Alert Production				
System - Cluster Errors Detected Development				
System - Cluster Errors Detected Production				
System - Cluster Status Message				
System - Critical Database Error				
System - Critical Service Started				
System - Critical Service Stopped Development				
System - Machine Shutdown/Restart				
System - Prohibited DNA Account Used to Logon				
System - SCADA Lab Rack Coldstart				

From: PagerDuty ALERT <no-reply@pagerduty.com>
To: Gage, Will
Cc:
Subject: [PagerDuty ALERT] You have 1 TRIGGERED Incident (cd8BT)
Sent: Sun 11/8/2015 5:55 AM

Hello Will Gage,

You are assigned 1 triggered incident in PagerDuty:
Please visit the following URL to manage this incident.
https://eprod-scada.pagerduty.com/dashboard

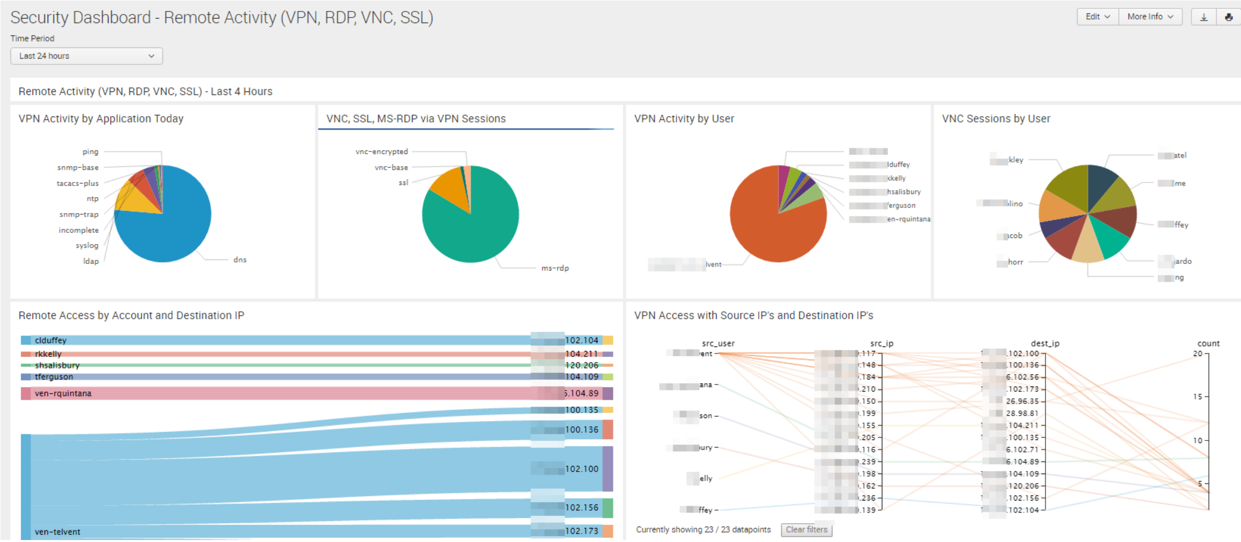
1) Incident #314
  Opened on: Nov 8 at 5:55 AM CST
  Service: SCADA_Splunk
  Description: HSTN-LQ-RT502 - OASyS DNA RealTime Service - stopped
  Link: https://eprod-scada.pagerduty.com/i/314
  Escalation Policy: SCADA Infrastructure
  Details:
    The following critical service is in a stopped state:
Host: HSTN-LQ-RT502
Service: OASyS DNA RealTime Service
Alert:
System
 - Critical Service Stopped Production
Trigger Time:
05:55:07 on November 08, 2015.
If you believe you've received this email in error, please email scadainfrastructure@eprod.com This message (including any attachments) is confidential and intended for a specific individual and purpose. If you are not the intended recipient, please notify the sender immedia...

You can disable these messages by adjusting your notification methods:
https://eprod-scada.pagerduty.com/users/PUSOKU4

Where We Are

System Security

- Perimeter monitoring for suspicious activity
- Ability to view remote access into system
- Ability to view user activity with system



Security Dashboard - Remote Activity (VPN, RDP, VNC, SSL)

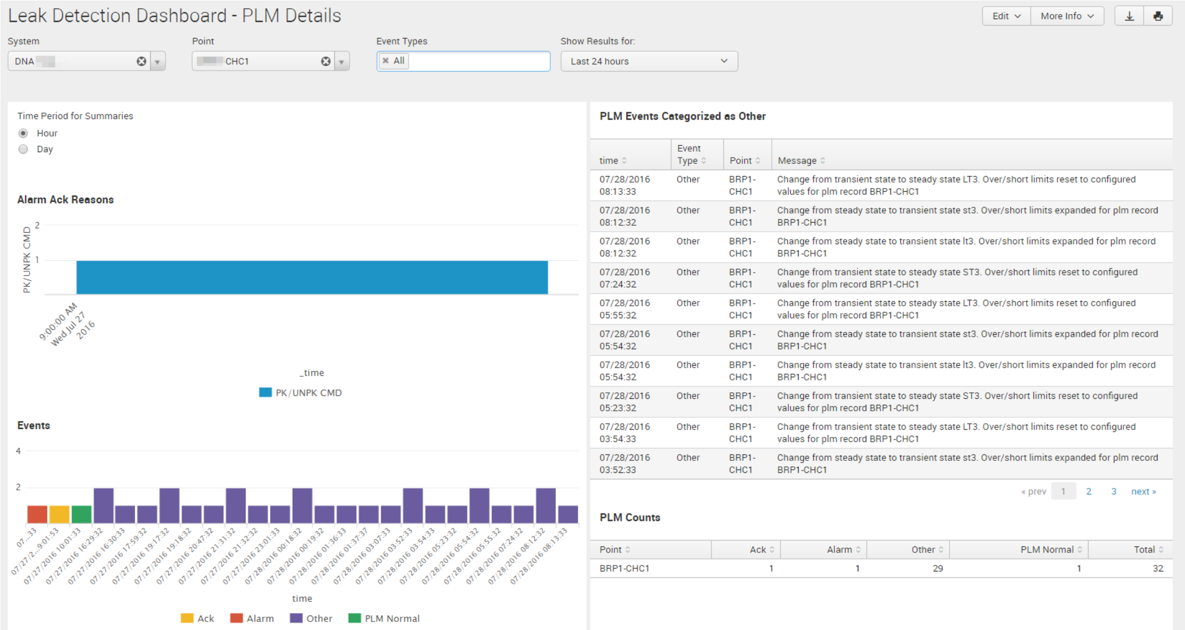
Time Period: Last 24 hours

Remote Activity (VPN, RDP, VNC, SSL) - Last 4 Hours

Where We Are

- Empowering Employees and Other Groups

- Leak Detection
  - Needed long term tracking
  - Identify priorities and track progress
  - Ability to see configurations and alerts
  - Used to influence decisions about staffing and funding



Leak Detection Dashboard - PLM Details

System: DNA [redacted]

Point: [redacted] CHC1

Event Types: × All

Show Results for: Last 24 hours

Time Period for Summaries

● Hour

○ Day

Alarm Ack Reasons

Events

PLM Events Categorized as Other

time	Event Type	Point	Message
07/28/2016 08:13:33	Other	BRP1-CHC1	Change from transient state to steady state LT3. Over/short limits reset to configured values for plm record BRP1-CHC1
07/28/2016 08:12:32	Other	BRP1-CHC1	Change from steady state to transient state st3. Over/short limits expanded for plm record BRP1-CHC1
07/28/2016 08:12:32	Other	BRP1-CHC1	Change from steady state to transient state lt3. Over/short limits expanded for plm record BRP1-CHC1
07/28/2016 07:24:32	Other	BRP1-CHC1	Change from transient state to steady state ST3. Over/short limits reset to configured values for plm record BRP1-CHC1
07/28/2016 05:55:32	Other	BRP1-CHC1	Change from transient state to steady state LT3. Over/short limits reset to configured values for plm record BRP1-CHC1
07/28/2016 05:54:32	Other	BRP1-CHC1	Change from steady state to transient state st3. Over/short limits expanded for plm record BRP1-CHC1
07/28/2016 05:54:32	Other	BRP1-CHC1	Change from steady state to transient state lt3. Over/short limits expanded for plm record BRP1-CHC1
07/28/2016 05:23:32	Other	BRP1-CHC1	Change from transient state to steady state ST3. Over/short limits reset to configured values for plm record BRP1-CHC1
07/28/2016 03:54:33	Other	BRP1-CHC1	Change from transient state to steady state LT3. Over/short limits reset to configured values for plm record BRP1-CHC1
07/28/2016 03:52:33	Other	BRP1-CHC1	Change from steady state to transient state st3. Over/short limits expanded for plm record BRP1-CHC1

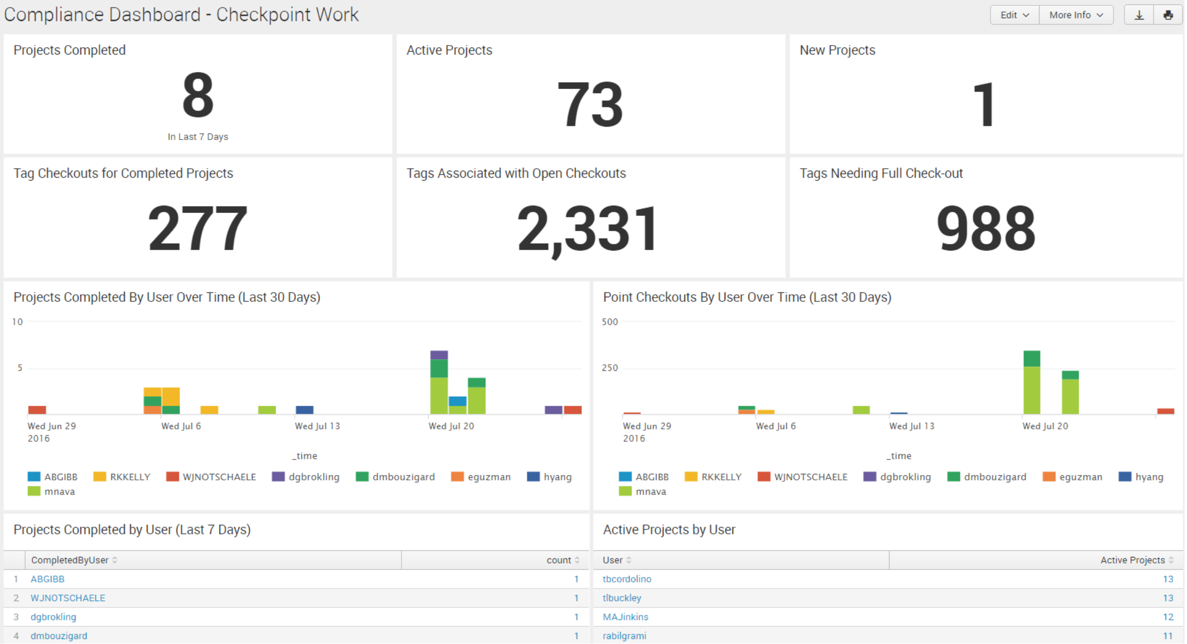
PLM Counts

Point	Ack	Alarm	Other	PLM Normal	Total
BRP1-CHC1	1	1	29	1	32

Where We Are

- Empowering Employees and Other Groups

- Compliance
  - Tracking activity with field operations
  - Providing information on work-load balance
  - Ability to investigate outages
  - Ability to view configuration changes



Compliance Dashboard - Checkpoint Work

Projects Completed

8

In Last 7 Days

Active Projects

73

New Projects

1

Tag Checkouts for Completed Projects

277

Tags Associated with Open Checkouts

2,331

Tags Needing Full Check-out

988

Projects Completed By User Over Time (Last 30 Days)

Point Checkouts By User Over Time (Last 30 Days)

Projects Completed by User (Last 7 Days)

	CompletedByUser	count
1	ABGIBB	1
2	WJNOTSCHAELE	1
3	dgbrokling	1
4	dmbouzigard	1

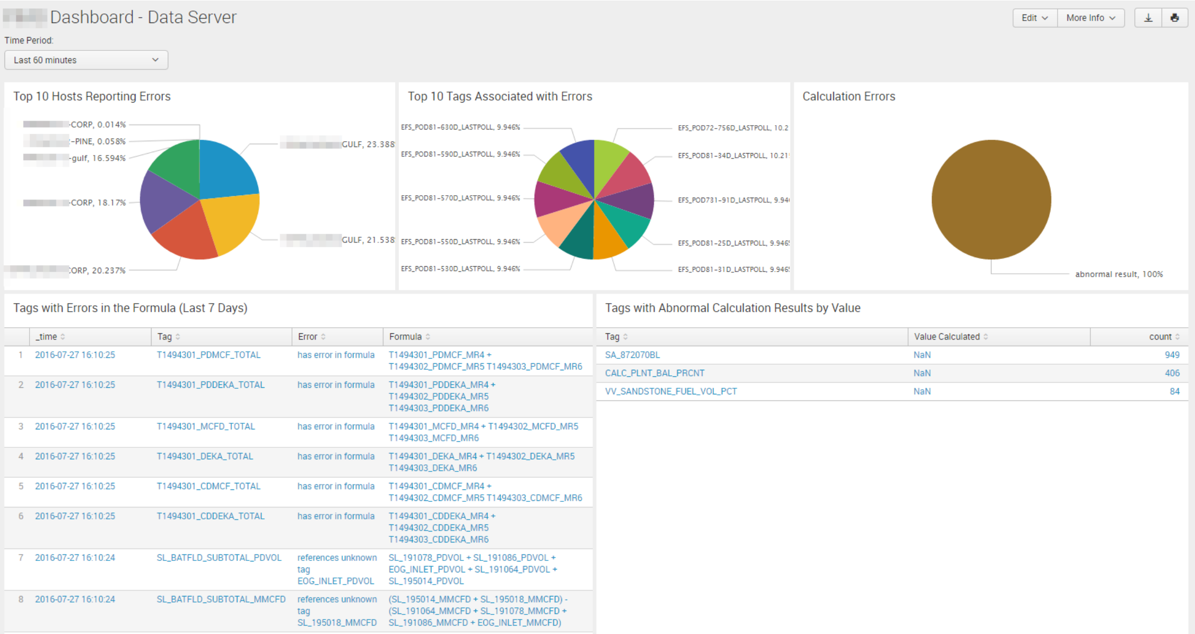
Active Projects by User

User	Active Projects
tbcordolino	13
tlbuckley	13
MAJinkins	12
rabilgrami	11

Where We Are

- Empowering Employees and Other Groups

- Internal Systems Support
  - Real performance beyond perfmon
  - See configuration problems
  - View errors in logs (worst offenders)
  - Splunk as data source



[redacted] Dashboard - Data Server

Time Period: Last 60 minutes

Top 10 Hosts Reporting Errors

[redacted]-CORP, 0.014%
[redacted]-PINE, 0.058%
[redacted]-gulf, 16.594%
[redacted]-CORP, 18.17%
[redacted]CORP, 20.237%
[redacted]GULF, 23.388
[redacted]GULF, 21.538

Top 10 Tags Associated with Errors

EFS_POD81-630D_LASTPOLL, 9.946%
EFS_POD81-590D_LASTPOLL, 9.946%
EFS_POD81-570D_LASTPOLL, 9.946%
EFS_POD81-550D_LASTPOLL, 9.946%
EFS_POD81-530D_LASTPOLL, 9.946%
EFS_POD72-756D_LASTPOLL, 10.2
EFS_POD81-34D_LASTPOLL, 10.21
EFS_POD731-91D_LASTPOLL, 9.94
EFS_POD81-25D_LASTPOLL, 9.946
EFS_POD81-31D_LASTPOLL, 9.946

Calculation Errors

Tags with Errors in the Formula (Last 7 Days)

	_time	Tag	Error	Formula
1	2016-07-27 16:10:25	T1494301_PDMCF_TOTAL	has error in formula	T1494301_PDMCF_MR4 + T1494302_PDMCF_MR5 T1494303_PDMCF_MR6
2	2016-07-27 16:10:25	T1494301_PDDEKA_TOTAL	has error in formula	T1494301_PDDEKA_MR4 + T1494302_PDDEKA_MR5 T1494303_PDDEKA_MR6
3	2016-07-27 16:10:25	T1494301_MCFD_TOTAL	has error in formula	T1494301_MCFD_MR4 + T1494302_MCFD_MR5 T1494303_MCFD_MR6
4	2016-07-27 16:10:25	T1494301_DEKA_TOTAL	has error in formula	T1494301_DEKA_MR4 + T1494302_DEKA_MR5 T1494303_DEKA_MR6
5	2016-07-27 16:10:25	T1494301_CDMCF_TOTAL	has error in formula	T1494301_CDMCF_MR4 + T1494302_CDMCF_MR5 T1494303_CDMCF_MR6
6	2016-07-27 16:10:25	T1494301_CDDEKA_TOTAL	has error in formula	T1494301_CDDEKA_MR4 + T1494302_CDDEKA_MR5 T1494303_CDDEKA_MR6
7	2016-07-27 16:10:24	SL_BATFLD_SUBTOTAL_PDVOL	references unknown tag EOG_INLET_PDVOL	SL_191078_PDVOL + SL_191086_PDVOL + EOG_INLET_PDVOL + SL_191064_PDVOL + SL_195014_PDVOL
8	2016-07-27 16:10:24	SL_BATFLD_SUBTOTAL_MMCFD	references unknown tag SL_195018_MMCFD	(SL_195014_MMCFD + SL_195018_MMCFD) - (SL_191064_MMCFD + SL_191078_MMCFD + SL_191086_MMCFD + EOG_INLET_MMCFD)

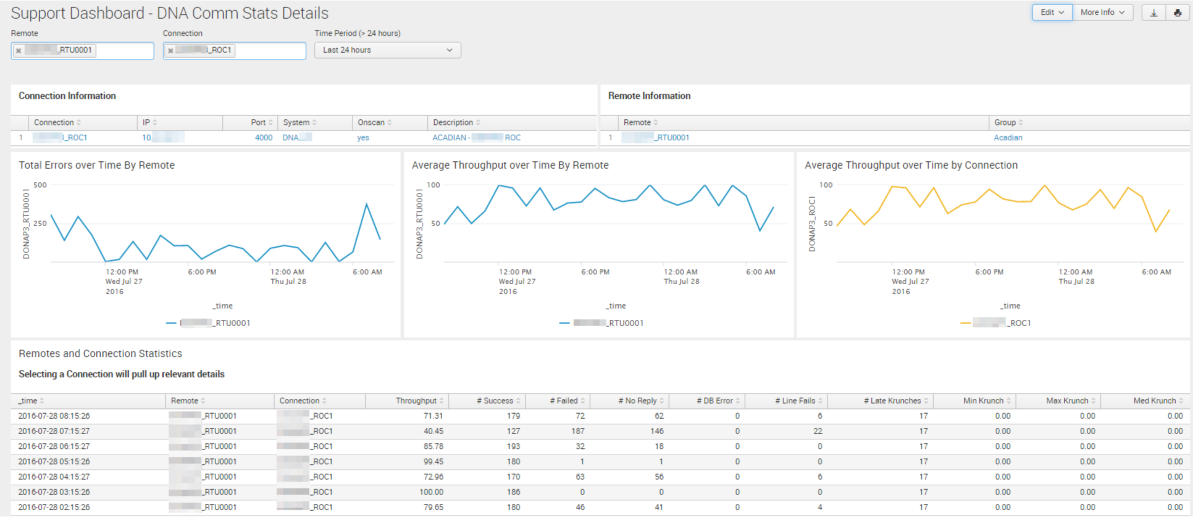
Tags with Abnormal Calculation Results by Value

Tag	Value Calculated	count
SA_872070BL	NaN	949
CALC_PLNT_BAL_PRCNT	NaN	406
VV_SANDSTONE_FUEL_VOL_PCT	NaN	84

Where We Are

- Empowering Employees and Other Groups

- Support Staff
  - View communication problems
  - Historical trending
  - Tags being sent to PI
  - Independent of system



Support Dashboard - DNA Comm Stats Details

Remote: [redacted]_RTU0001

Connection: [redacted]_ROC1

Time Period (> 24 hours): Last 24 hours

Connection Information

	Connection	IP	Port	System	Onscan	Description
1	[redacted]_ROC1	10.[redacted]	4000	DNA[redacted]	yes	ACADIAN - [redacted] ROC

Remote Information

	Remote	Group
1	[redacted]_RTU0001	Acadian

Total Errors over Time By Remote

Average Throughput over Time By Remote

Average Throughput over Time by Connection

Remotes and Connection Statistics

Selecting a Connection will pull up relevant details

_time	Remote	Connection	Throughput	# Success	# Failed	# No Reply	# DB Error	# Line Fails	# Late Krunches	Min Krunch	Max Krunch	Med Krunch
2016-07-28 08:15:26	[redacted]_RTU0001	[redacted]_ROC1	71.31	179	72	62	0	6	17	0.00	0.00	0.00
2016-07-28 07:15:27	[redacted]_RTU0001	[redacted]_ROC1	40.45	127	187	146	0	22	17	0.00	0.00	0.00
2016-07-28 06:15:27	[redacted]_RTU0001	[redacted]_ROC1	85.78	193	32	18	0	0	17	0.00	0.00	0.00
2016-07-28 05:15:26	[redacted]_RTU0001	[redacted]_ROC1	99.45	180	1	1	0	0	17	0.00	0.00	0.00
2016-07-28 04:15:27	[redacted]_RTU0001	[redacted]_ROC1	72.96	170	63	56	0	6	17	0.00	0.00	0.00
2016-07-28 03:15:26	[redacted]_RTU0001	[redacted]_ROC1	100.00	186	0	0	0	0	17	0.00	0.00	0.00
2016-07-28 02:15:26	[redacted]_RTU0001	[redacted]_ROC1	79.65	180	46	41	0	4	17	0.00	0.00	0.00

Where We Want To Be

2017 Goal

- Splunk IT Service Intelligence fully implemented for “services” and predictive system modelling
- Splunk for Enterprise Security fully implemented for SEIM in SCADA Systems/Networks
- HA for Indexers
- Increase from 225GB to 300GB of Daily Ingest for Splunk Enterprise
- Provide even more Data Analytics and Insight for SCADA Groups and Control Center

What Have We Gained

- Ability to be pro-active when responding to incidents to meet SLA's
- Dramatic reduction to investigate incidents (50%+)
- Reporting for other groups to help them do their jobs
- Troubleshoot and correlate data for root-cause-analysis
- Visibility, visibility, visibility

THANK YOU

.conf2016

splunk>