Splunk SAP: 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

- 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%
Truth #2: Heroes Target Projects with Business Impact

- **47yr**
- **$23B**
- **87%**
- **77%**
- **121K**
- **41K**
- **25**
- **120**
- **1500**

- **Age**
- **Revenue**
- **Fortune 500 Customers**
- **Global Revenue Touched**
- **Users**
- **Installations**
- **Customers**
- **Countries**
- **Partners**
Truth #3: Heroes Understand Risk & Reward

Product Investments
4+ years and counting as well release of new feature pack every 6 months¹
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
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
<table>
<thead>
<tr>
<th>Category</th>
<th>Last 24 hours</th>
<th>Pass</th>
<th>Fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login by privileged user</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users having excessive rights</td>
<td>58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileged SAP users enabled</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users with default or well known password</td>
<td>3,475</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client open for change</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Namespace open for change</td>
<td>235</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login by multiple IDs on 1 terminal</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple logins by 1 ID on different terminals</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login by 1 ID in different geos</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password policy parameters</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Debug mode used</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User type changed</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Downloaded a file (NW7.31-)</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active users not logged in for 30 days or more</td>
<td>4,163</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execution of sensitive transactions</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users with sensitive authorization</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users with dev keys</td>
<td>143</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failed logons from multiple users on 1 terminal</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

- 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

- 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 SECURITY MATURITY MODEL

- Super Admin Monitoring
- Splunk SAP Security

RHONDOS CYBERSECURITY FOR SAP WITH POWERCONNECT & SPLUNK
Business Hero

David Clawson
Splunk YODA
Typical Fortune 500 Company

The Cost of Downtime

$10,000,000 per minute

Average Busiest Day

30% Uptime

70% MTTR

Improvements
Use Case Example: Supply Chain System Health
Big Pharma Charge Back

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

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

IBM Gentran stands out in two areas as a process bottleneck

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 middleware

- **Not filling**
  - big orders don’t leave the doc
Performance Hero

Matt Colabrese
Director of Customer Success
The Bare Necessities
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

Ticket 1: Priority High
Work Process Utilization >50%

Ticket 2: Priority Critical
Work Process Utilization >75%

Ticket 3: Priority Critical
NRIVSHADOW table locked >20min

NRIVSHADOW table unlocked by DBA with WP Utilization at 86%

Work Process Utilization returns to normal levels

Ticket 4: Priority Critical
Per Solution Manager, Update2 response time >SOP in all instances
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 .....
Thank You!

info@rhondos.com
### Key Use Cases for “Splunking” SAP

#### Security

**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.

#### Performance

**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.

#### Migration

**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

#### Business Flow

**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.