Splunk IT Service Intelligence

Agenda

- Splunk ITSI Overview
- Advantages
- Features of ITSI
- Use case of ITSI
- Hands-on with ITSI Sandbox

ITSI Overview

- To visualize the interrelationship and dependencies of business and technical services.

- **Business Service :** A service is utilized by the end user. For example, Online service request system.

- **Technical Service :** An internal or external system used to provide the other services. For Example, domain name system (DNS).

- **Key Performance Indicator (KPI)** is a saved search which produces metrics like CPU utilization %, average response time or error rate.

- **Health Score** is a score from 0 to 100 that helps determine the health of the service calculated every minute and it is based on the weighted status of all the KPI with in the services.

Advantages

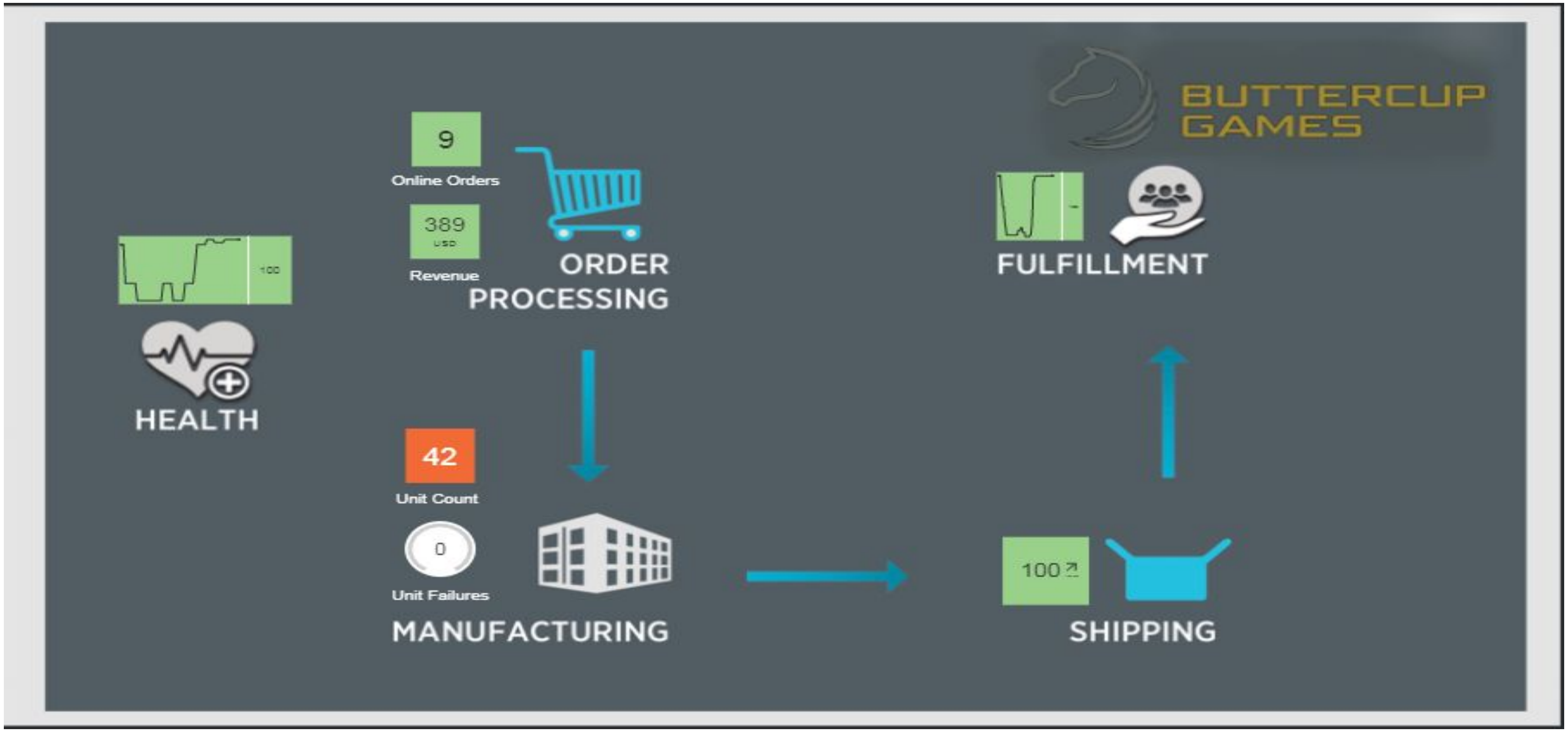
- Employ AI to Predict and Prevent Imminent Outages.
- Create a 360-Degree View for Smarter Troubleshooting and Monitoring.
- Prioritize problem resolution with event analytics
- Transform IT Operations with a True AIOps Platform

Features

- Glass tables
- Deep dives
- Multi-KPI Alerts
- Episode review
- Service Analyzer

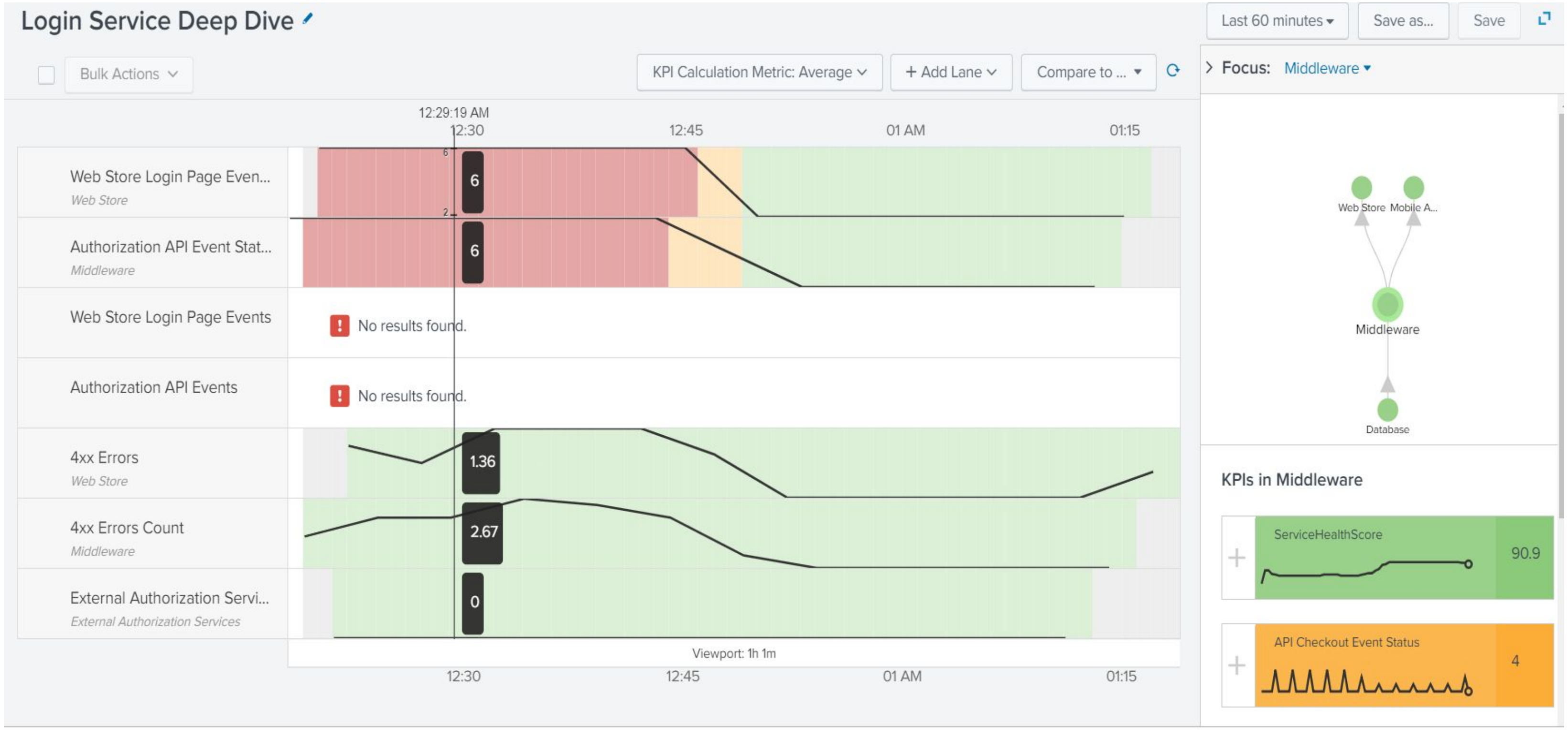
Glass tables

- Visualize and monitor services; share institutional knowledge.



Deep dives

- Troubleshoot the issues and perform root cause analysis. Swim lanes are used to identify the variations in a specific time.



Login Service Deep Dive

KPI Calculation Metric: Average

Focus: Middleware

No results found.

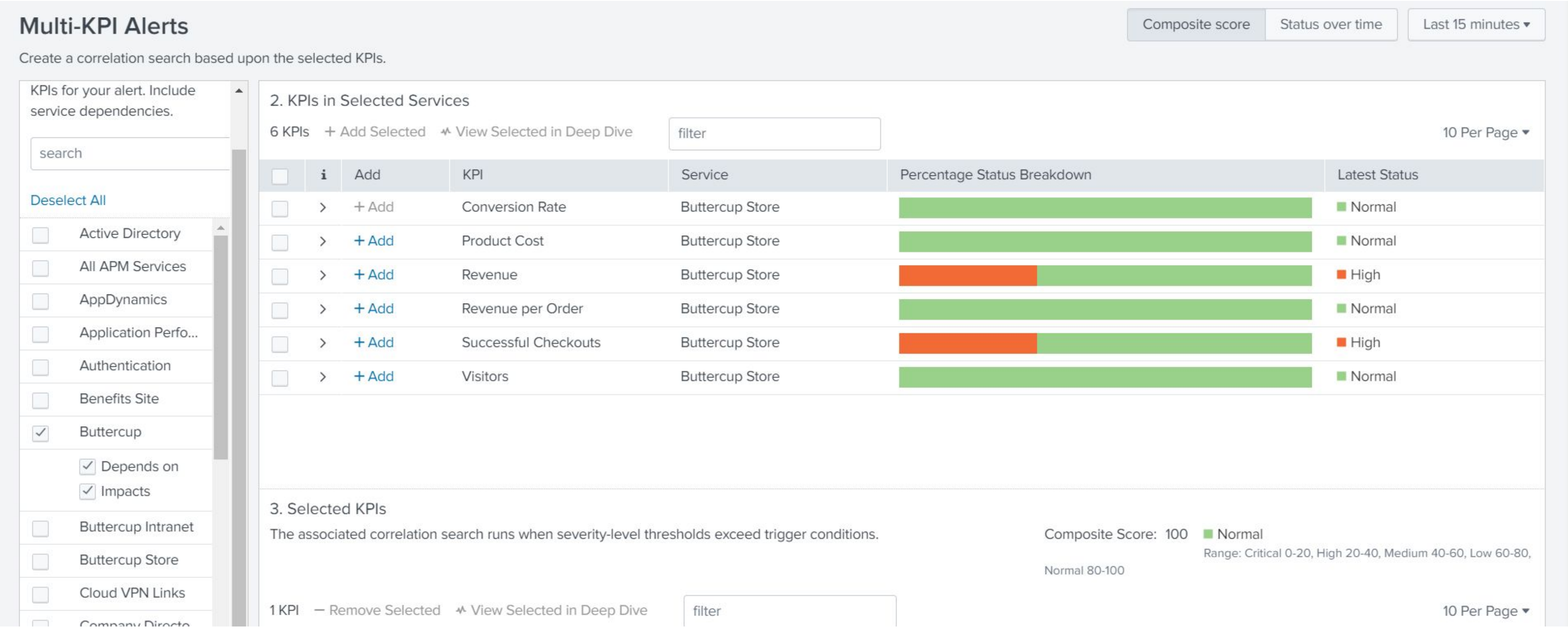
No results found.

Viewport: 1h 1m

KPIs in Middleware

Multi-KPI Alerts

- Generate notable events based on trigger condition occurs simultaneously.



Multi-KPI Alerts

Create a correlation search based upon the selected KPIs.

KPIs for your alert. Include service dependencies.

- □ Active Directory
- □ All APM Services
- □ AppDynamics
- □ Application Perfo...
- □ Authentication
- □ Benefits Site
- ☑ Buttercup
  - ☑ Depends on
  - ☑ Impacts
- □ Buttercup Intranet
- □ Buttercup Store
- □ Cloud VPN Links
- □ Company Directo

2. KPIs in Selected Services

6 KPIs + Add Selected View Selected in Deep Dive

□	i	Add	KPI	Service	Percentage Status Breakdown	Latest Status
□	›	+ Add	Conversion Rate	Buttercup Store	🟩	🟩 Normal
□	›	+ Add	Product Cost	Buttercup Store	🟩	🟩 Normal
□	›	+ Add	Revenue	Buttercup Store	🟥🟩	🟥 High
□	›	+ Add	Revenue per Order	Buttercup Store	🟩	🟩 Normal
□	›	+ Add	Successful Checkouts	Buttercup Store	🟥🟩	🟥 High
□	›	+ Add	Visitors	Buttercup Store	🟩	🟩 Normal

3. Selected KPIs

The associated correlation search runs when severity-level thresholds exceed trigger conditions.

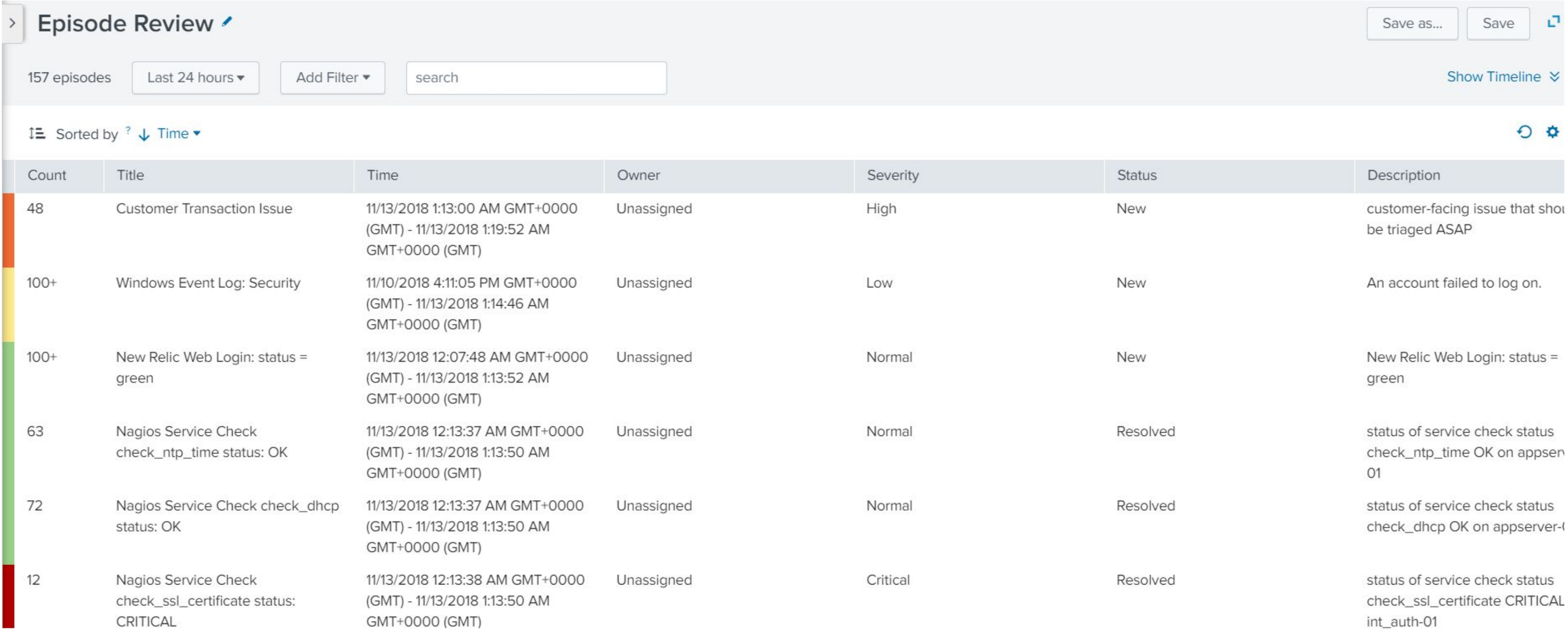
Composite Score: 100 🟩 Normal

Range: Critical 0-20, High 20-40, Medium 40-60, Low 60-80, Normal 80-100

1 KPI — Remove Selected View Selected in Deep Dive

Episode Review

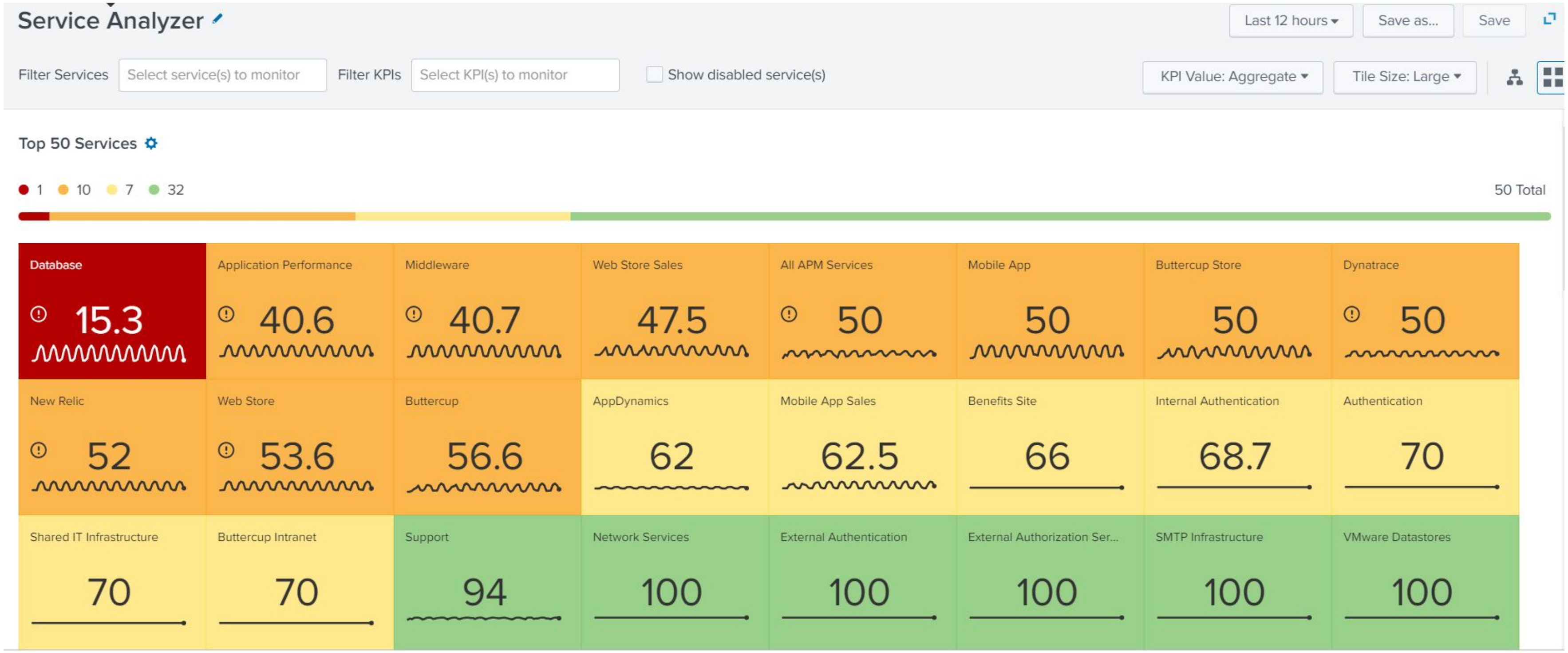
- Episode Review to see alerts for issues that are currently impacting services or might potentially impact services.
- Episode Review displays notable events (alerts) generated by ITSI multi-KPI alerts, correlation searches, and anomaly detection algorithms.



Count	Title	Time	Owner	Severity	Status	Description
48	Customer Transaction Issue	11/13/2018 1:13:00 AM GMT+0000 (GMT) - 11/13/2018 1:19:52 AM GMT+0000 (GMT)	Unassigned	High	New	customer-facing issue that shou be triaged ASAP
100+	Windows Event Log: Security	11/10/2018 4:11:05 PM GMT+0000 (GMT) - 11/13/2018 1:14:46 AM GMT+0000 (GMT)	Unassigned	Low	New	An account failed to log on.
100+	New Relic Web Login: status = green	11/13/2018 12:07:48 AM GMT+0000 (GMT) - 11/13/2018 1:13:52 AM GMT+0000 (GMT)	Unassigned	Normal	New	New Relic Web Login: status = green
63	Nagios Service Check check_ntp_time status: OK	11/13/2018 12:13:37 AM GMT+0000 (GMT) - 11/13/2018 1:13:50 AM GMT+0000 (GMT)	Unassigned	Normal	Resolved	status of service check status check_ntp_time OK on appser 01
72	Nagios Service Check check_dhcp status: OK	11/13/2018 12:13:37 AM GMT+0000 (GMT) - 11/13/2018 1:13:50 AM GMT+0000 (GMT)	Unassigned	Normal	Resolved	status of service check status check_dhcp OK on appserver-
12	Nagios Service Check check_ssl_certificate status: CRITICAL	11/13/2018 12:13:38 AM GMT+0000 (GMT) - 11/13/2018 1:13:50 AM GMT+0000 (GMT)	Unassigned	Critical	Resolved	status of service check status check_ssl_certificate CRITICAL int_auth-01

Service Analyzer

- Monitor overall status of all services and KPIs.



Service Analyzer

Last 12 hours ▾ | Save as... | Save

Filter Services: Select service(s) to monitor

Filter KPIs: Select KPI(s) to monitor

□ Show disabled service(s)

KPI Value: Aggregate ▾

Tile Size: Large ▾

Top 50 Services

● 1 ● 10 ● 7 ● 32

50 Total

Database 15.3	Application Performance 40.6	Middleware 40.7	Web Store Sales 47.5	All APM Services 50	Mobile App 50	Buttercup Store 50	Dynatrace 50
New Relic 52	Web Store 53.6	Buttercup 56.6	AppDynamics 62	Mobile App Sales 62.5	Benefits Site 66	Internal Authentication 68.7	Authentication 70
Shared IT Infrastructure 70	Buttercup Intranet 70	Support 94	Network Services 100	External Authentication 100	External Authorization Ser... 100	SMTP Infrastructure 100	VMware Datastores 100

Hands-on

Lets get hands dirt using Splunk ITSI

Configure Teams

- Configure -> Team
- Click New Team, then give the team name and permissions.
- While creating a new service, you can assign this team or you can edit the existing service to assign this team.
- Based on the team access, user can access the remaining services.

Create Entity

- Configure -> Entities
- Click create entity -> create single entitiy
- Give the name for an entity
- Add alias and fileds

Thank you…!