

Welcome we will get started shortly...

Splunk ITSI Workshop



Presenter: Paul Winchester

16th June 2020

Note: This workshop is based on Splunk's own Splunk4Ninjas – ITSI sessions.
Also note: This is not an actual picture of me. But it's quite close...



Register and Create Your Environment

1. If you've not yet created your Splunk environment, use this link to register:

http://splunk4rookies.com/4320/self_register

2. Log into you instance:

http://<aws_instance>:8000/en-US/

username : admin

password : smartway

Please note that the instances take 30mins to initialise due to Machine Learning backfilling.

Congratulations! Your Splunk sandbox has been created.
You have **48 hours** ahead to play until termination.

Please allow a few minutes for your instance(s) to be accessible.

Access link(s):
<http://ec2-34-253-204-181.eu-west-1.compute.amazonaws.com:80>

First Name*

Last Name*

Job Title*

Email*

Areas of interest* Application Delivery
 Business Analytics
 Internet of Things
 IT Operations Analytics
 Security & Fraud

Message*



Agenda

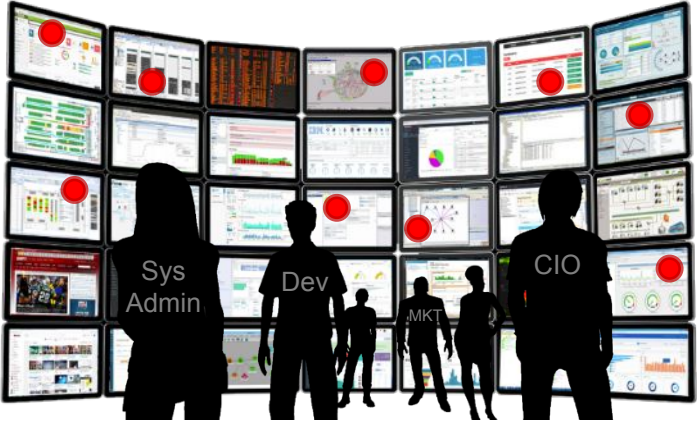
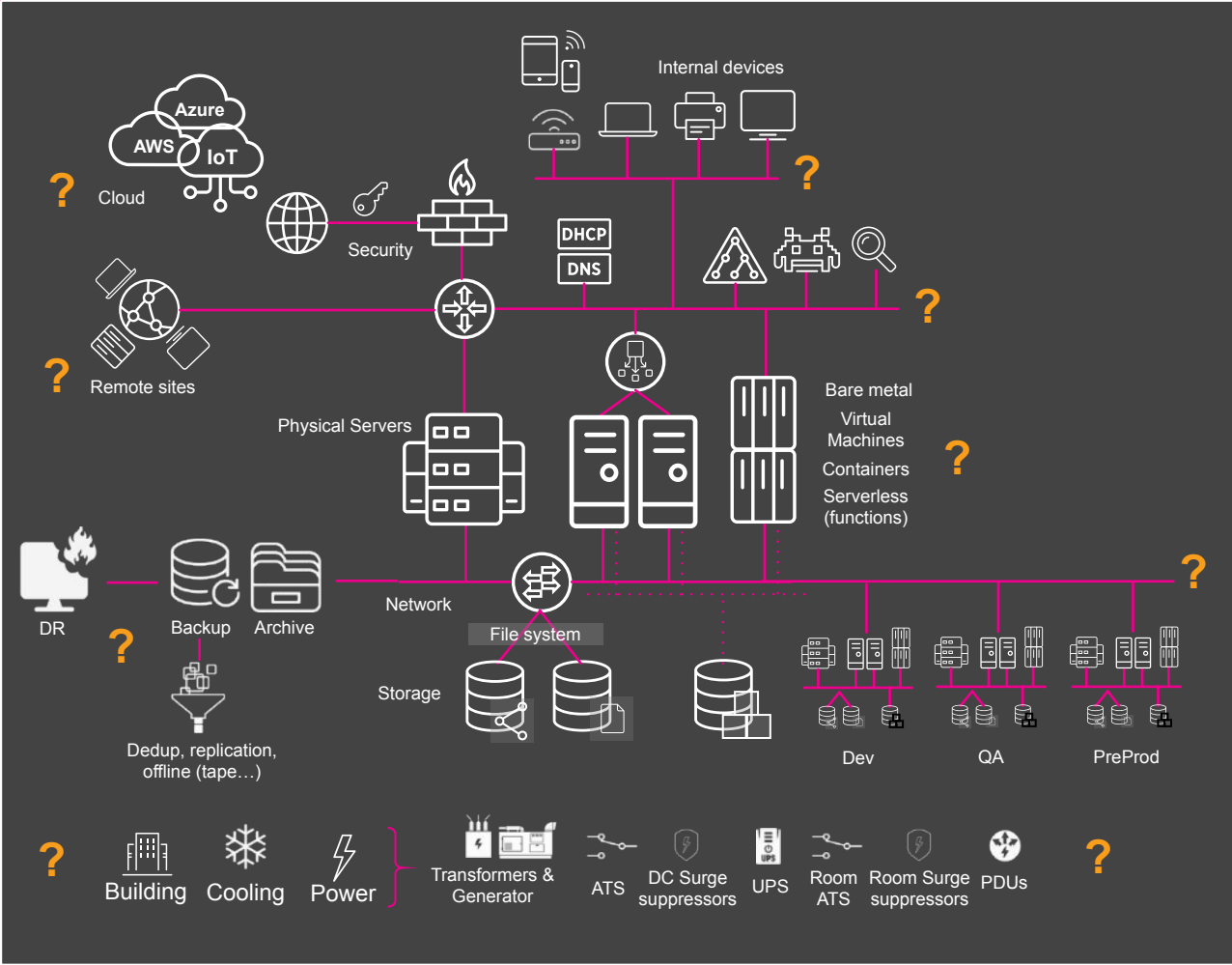
- IT Service Intelligence Overview
- Create a Service
- Creation of two KPI's
- Machine Learning
 - Apply Adaptive Thresholds
 - Predict Analytics
- Deep Dives
- Glass Tables
- Event Analytics Demystified
- Somerford's approach to ITSI

IT Service Intelligence

Complexity obscures the data you need

IT Ops teams continue to struggle to monitor, investigate, analyze & act

- DEV/APPS
- CLOUD
- OFFICE
- DR
- REMOTE
- SECURITY
- STORAGE
- NETWORK
- SERVERS
- BUILDING



Too Many Tools

Siloed Views of Data

Too Much Event Noise

Long Times to Resolve

The impact can be significant

Putting revenue, customer experience, employee effectiveness & innovation at risk



Lost Revenue

Outages and incidents impact the services and apps driving revenues



Poor Customer Experiences

Customers click away and brand reputation is damaged



Decreased Employee Effectiveness

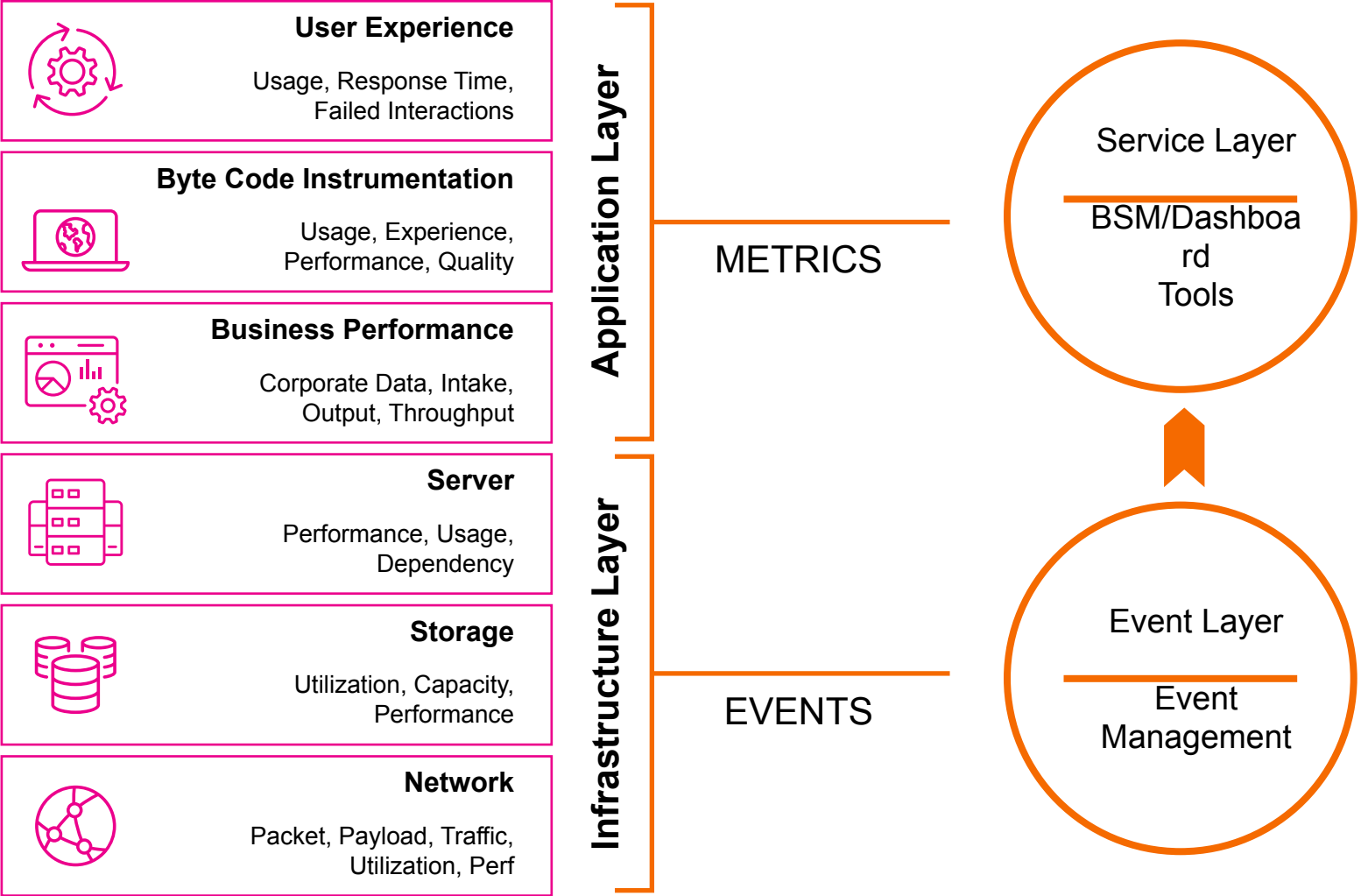
Teams thrash, finger-point, and key employees leave



Struggle to Innovate

IT spends too much time fixing problems instead of innovating and transforming

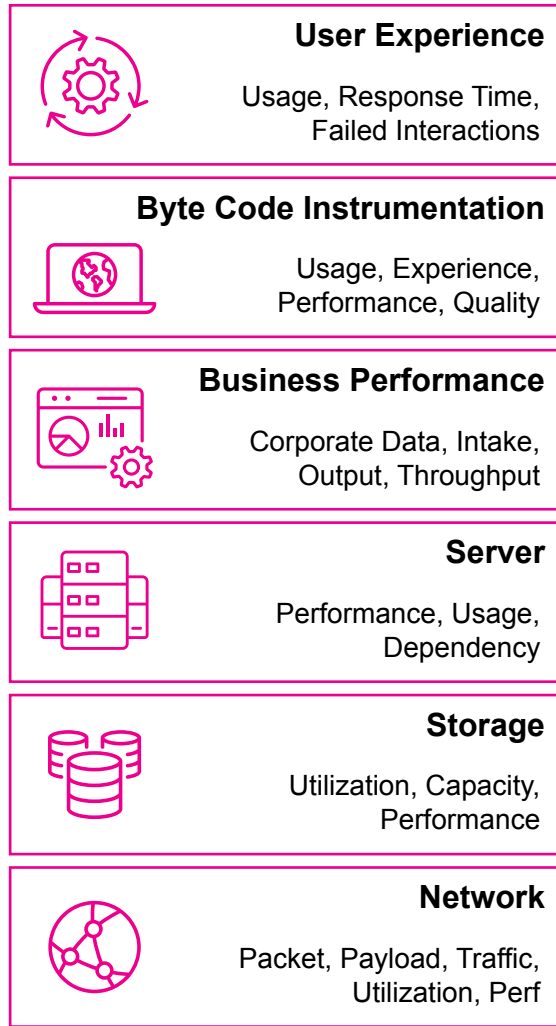
Why The Old Ways Disappoint



Challenges

- ▶ Many disparate components
- ▶ Brittle integrations
- ▶ Data is summarized and lost
- ▶ Longer root-cause identification
- ▶ End-to-end view challenging
- ▶ Labor-intensive to manage
- ▶ Not agile for digital business

IT Service Intelligence Platform Approach



Application Layer

Infrastructure Layer

MACHINE DATA



Splunk Approach:

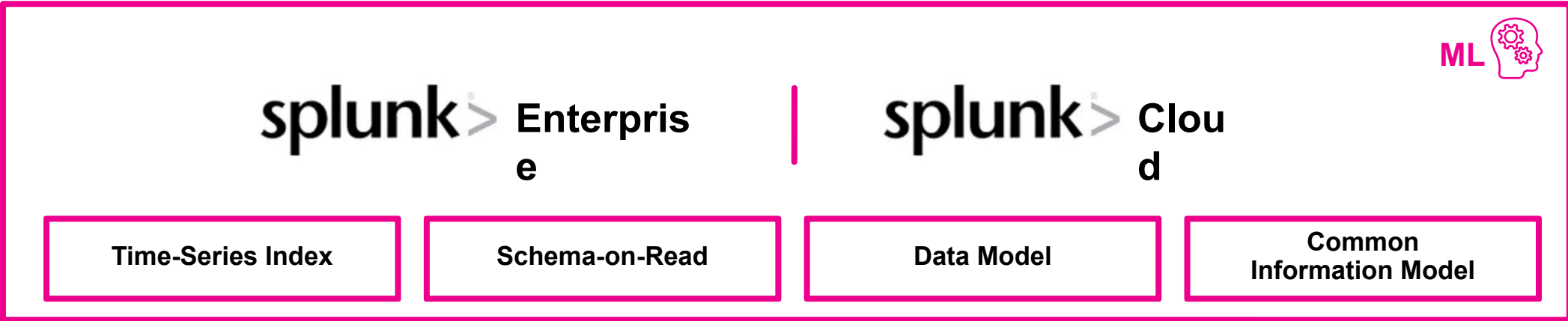
- ▶ Single repository for ALL data
- ▶ Data in original raw format
- ▶ Machine learning
- ▶ Simplified architecture
- ▶ Fewer resources to manage
- ▶ Collaborative approach

Splunk IT Service Intelligence

Data-driven service monitoring and analytics



Splunk IT Service Intelligence





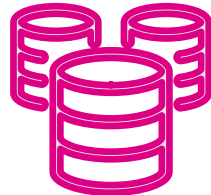
Key Terminology

What is a Service

A logical group of technology components that a user deems important to be monitored together. Services can encompass multiple tiers of the IT domain.



Online Store
Service



Database
Service



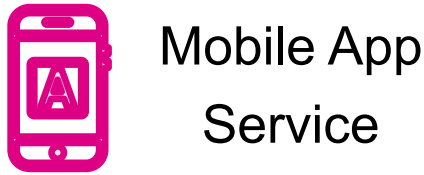
Mobile App
Service



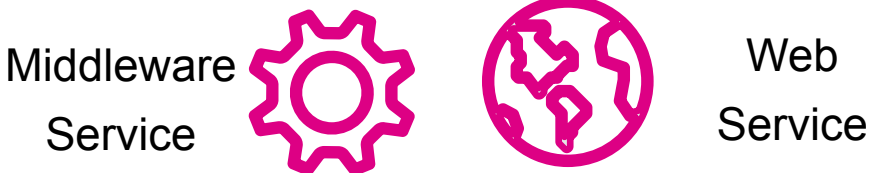
Call Centre
Service

Service Dependencies

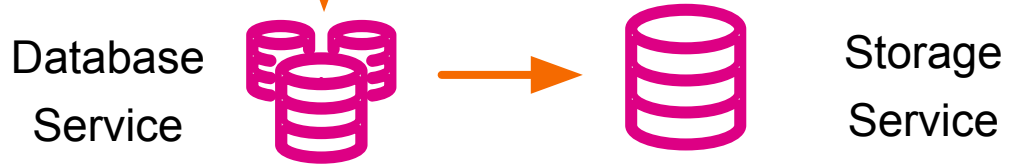
Business Services



Application Services

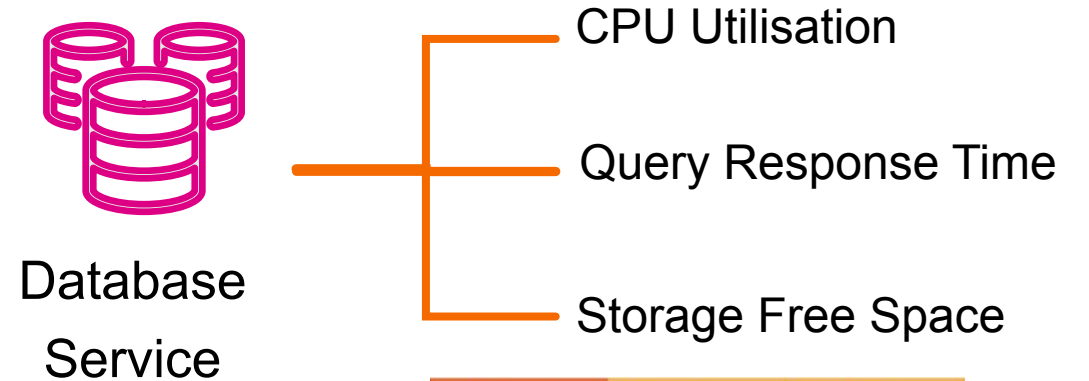
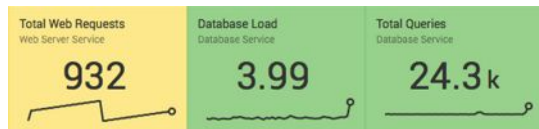
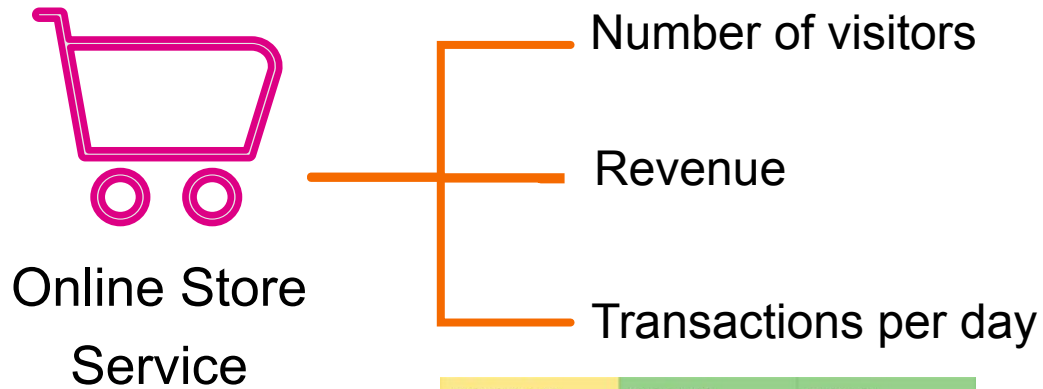


Technical Services



What is a KPI

A Key Performance Indicator and Health Scores constitute the means by which Services are monitored. A KPI is a Splunk saved search in ITSI that helps monitor a specific value.






What is a Health Score

A Health score is a score from 0-100 (0 being critical and 100 being normal) that measures the health of a Service. It is calculated based on all KPIs importance and its status.



What is an Entity

An **Entity** is an optional sub-element of a KPI.
A KPI can be filtered by entities.
ITSI can import entities from CMDBs & other sources

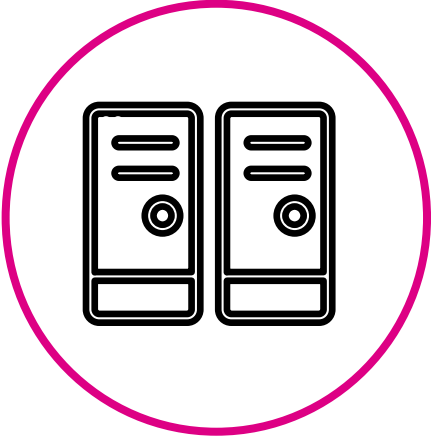
Severity ▾	Entity Name ⇅	Value ⇅
Critical	ⓘ mysql-02	 0 %
Normal	mysql-01	 33.26 %
Normal	mysql-03	 30.7 %
Normal	mysql-04	 28.05 %

ITSI Service Definition

To summarize a service is comprised of:



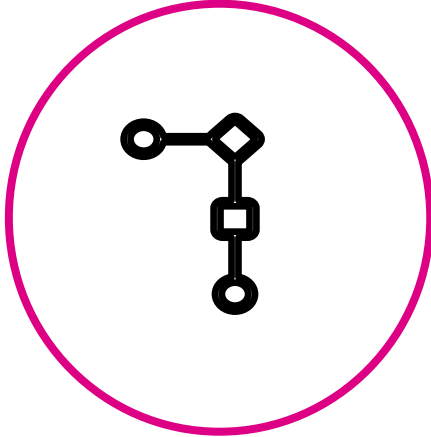
A Service
Health Score



0 or More
Entities



0 or More
KPIs



0 or More
Dependencies



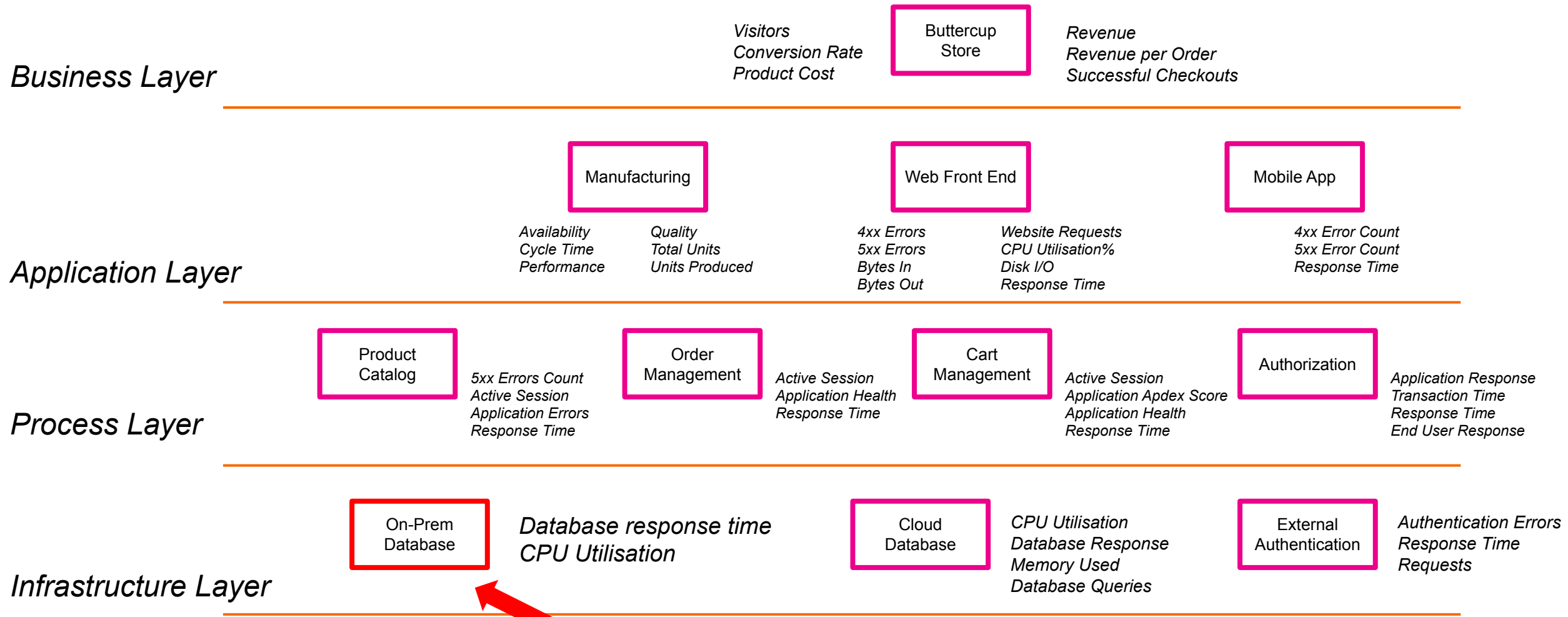
Workshop Back Story

Workshop Back Story

- ▶ Buttercup Store has just deployed a new Web service, **however** the engineers forgot to include database monitoring.
- ▶ Splunk administrators have deployed collectors on the infrastructure and have requested that we build a service centric monitoring solution.
- ▶ The CxO has just also requested that we include some 'AI' as they read on a website Artificial Intelligence can solve everything!
- ▶ The lab exercises start on the back of a **service decomposition workshop** to identify all the components that make up this service.

Service Decomposition Outcome

Example diagram detailing the content of a service, typically this is a photo of a whiteboard



Missing Service & KPIs

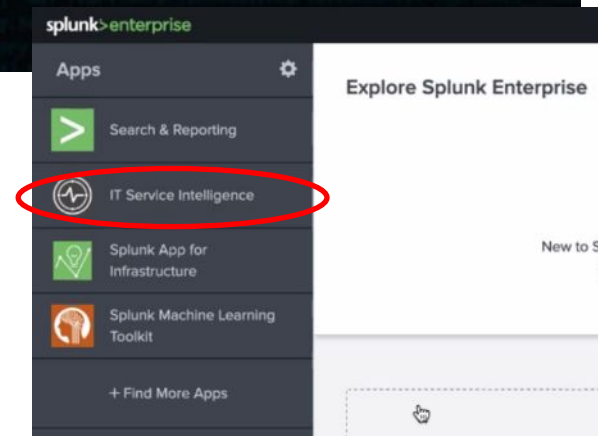
Let's get stuck in to it!

Point your browser to : http://<aws_instance>:8000/en-US/

This will be the link you got when you registered.




If it does not come up by default, select the IT Service Intelligence app

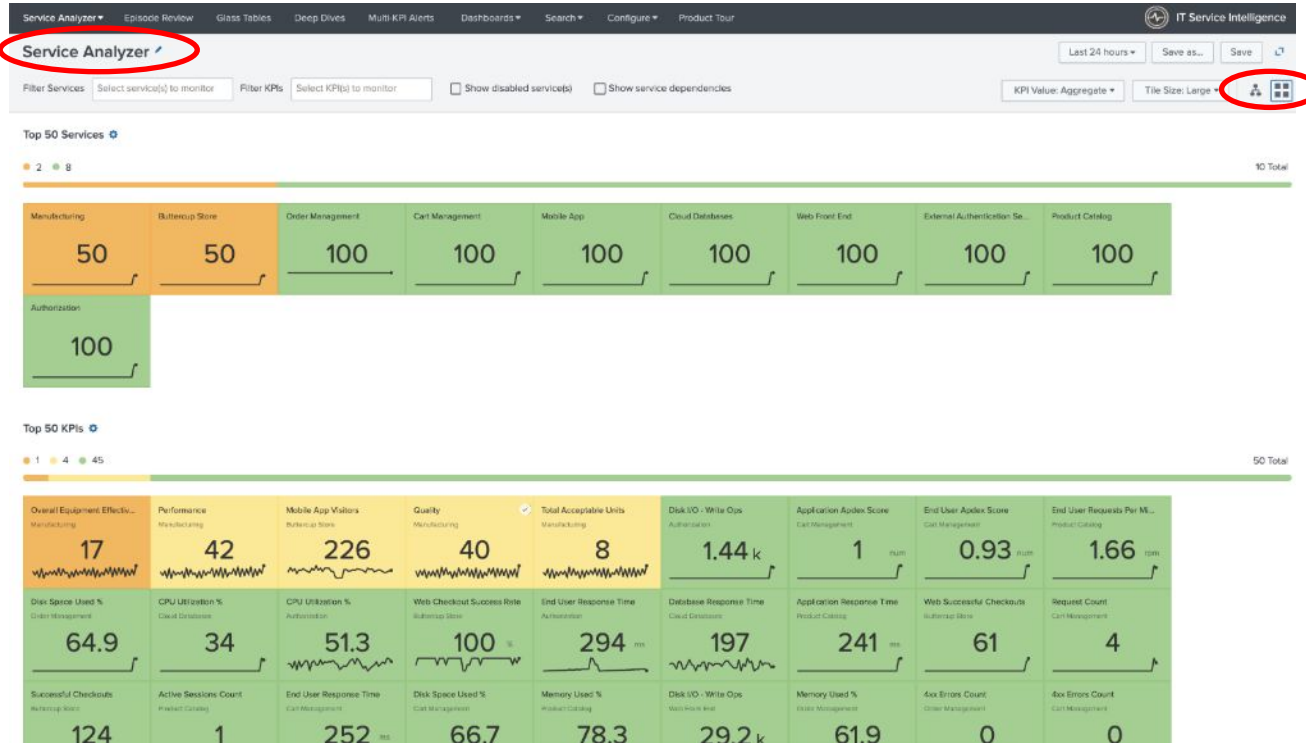


Services Exercise

Service Analyzer

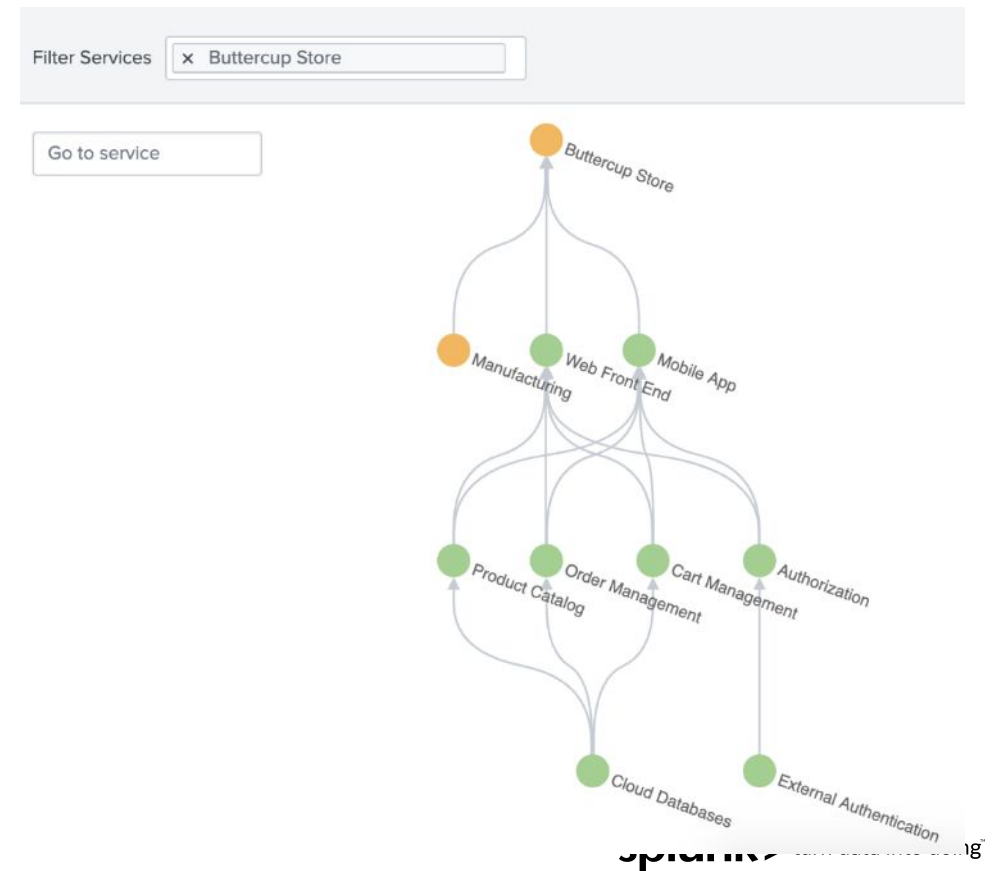
The Service Analyzer view provides a visual representation of our services and the KPIs associated KPIs. The highest severity is brought to the top left of each group.

- ▶ Select the 'Default Service Analyzer' view.
- ▶ Click on the  icon to switch the visualization to tree view



Service Tree

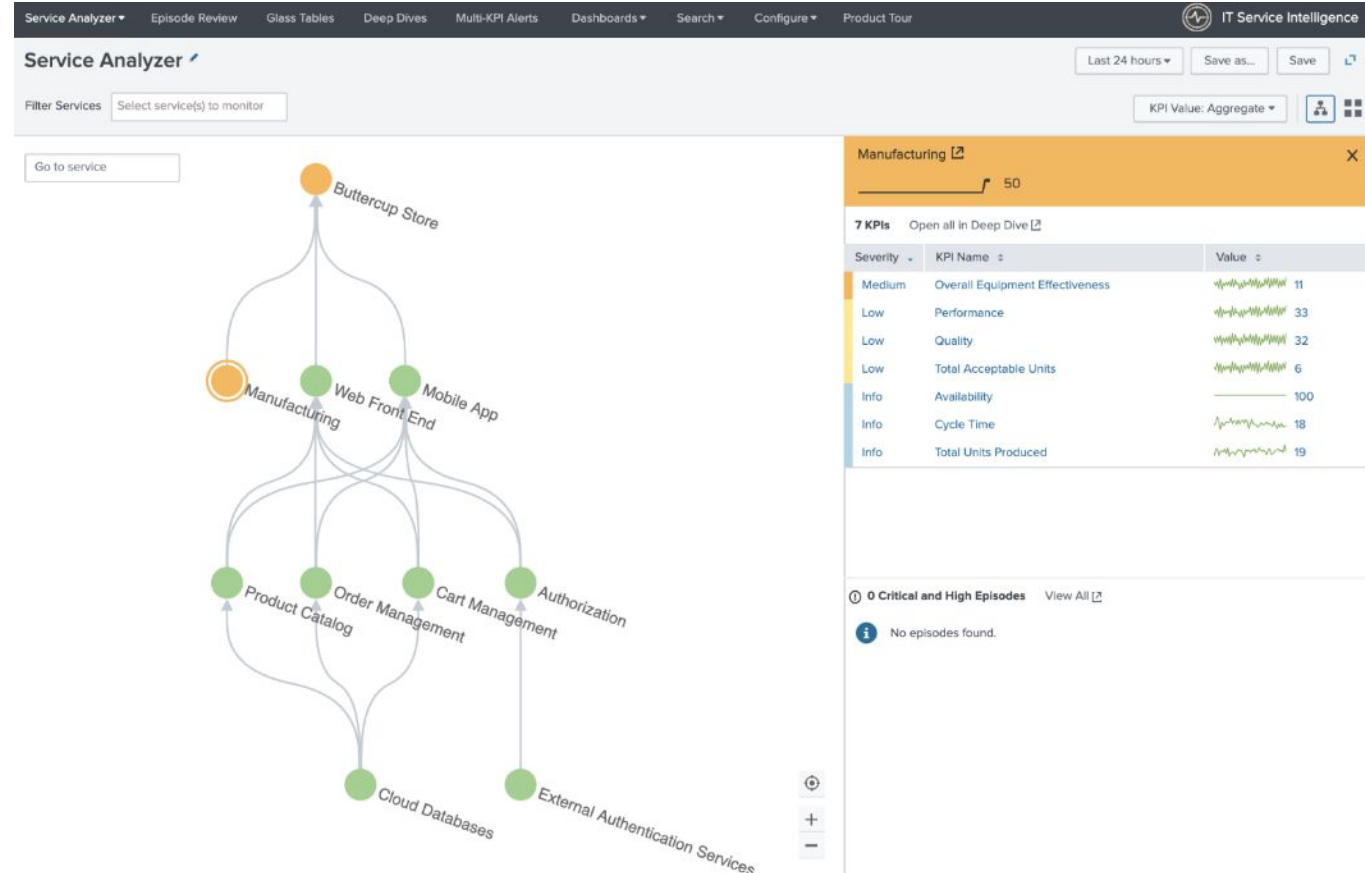
- ▶ The Service Analyzer tree view provides a visual representation of our services and the dependencies between them. Using this view you will also see the KPIs, entities, and most critical notable events associated with a service.
- ▶ The health of a service is affected by the health of a child service
- ▶ The tree can be built manually, however typically this is imported from a CMDB or a search



Service Tree

We can see that there is an issue with the Manufacturing service.

- ▶ Click on the effected service (***Manufacturing***) to investigate which KPIs have degraded.
- ▶ Review which entities are effected.



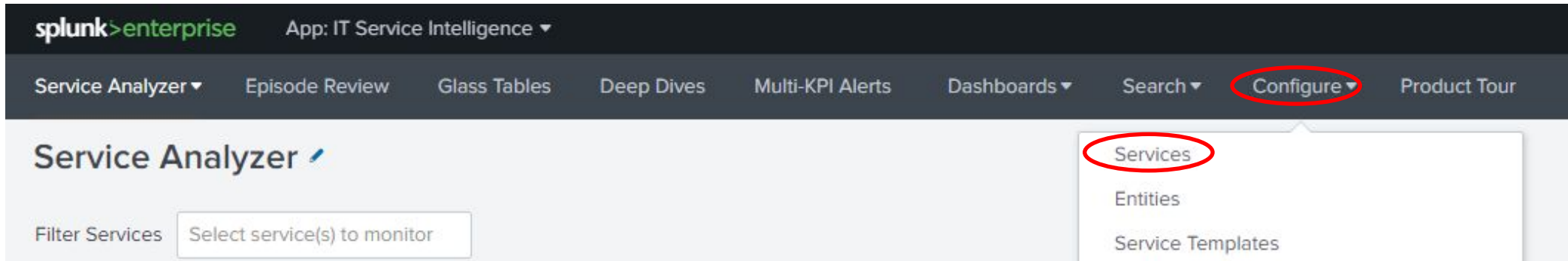
Services Lab

During the service decomposition workshop we identified a missing 'On-Prem Database' service. In this lab we are going to create this new service, we will review the ITSI DB module and then select a service template.

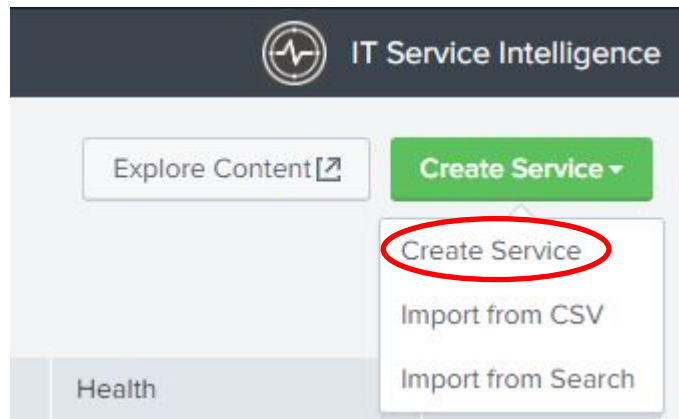
- ▶ To create a service you can use (Technical) KPI's that comes with modules:
 - ▶ OS: Linux, Unix & Windows
 - ▶ Web server: Apache & Microsoft IIS
 - ▶ Application server: Tomcat & Websphere
 - ▶ Database: Microsoft SQL & Oracle
 - ▶ Storage: Netapp ONTAP & EMC VNX
 - ▶ Load Balancer: F5 Big IP & Netscaler
 - ▶ Virtualisation: VMWare & Hyper=V

Services Lab

▶ Select the Configure menu + Services



▶ Click Create Service > Create Service



Services Lab

- ▶ Name the service as 'On-Prem Database'
- ▶ Check '**Database**' in modules list
 - Review the selected KPIs
 - *Do not hit the 'Create' button!*
- ▶ ITSI suggests best KPIs for database monitoring

Create Service ×

Title* On-Prem Database

Description optional

Team? Global ▾

Manually add service content

Link service to a service template

Add prebuilt KPIs from modules

Application Monitoring

Application Servers

Databases

End User Experience Manag...

Load Balancers

OS Hosts Monitoring

Service for Database Instances that provides KPIs for monitoring popular Database technologies.

5/7 KPIs selected

Database Active Connection

Database Connection Pool Used %

Database Deadlock Rate

Database Query Response Time

Cancel

Services Lab

Instead we are going to utilize the ITSI service templates feature, this will build the service with predefined KPIs.

- ▶ Select '*Link service to a service template*' button
- ▶ Choose '**On-Prem Database**' template
- ▶ Click the '*Enable 7 days of backfill for all Service KPIs*' option
 - *Please note the option is hidden below so you will need to scroll down!*
- ▶ Click '*Create*' button

Create Service

Title * On-Prem Database

Description optional

Team ? Global

Manually add service content

Link service to a service template

Add prebuilt KPIs from modules

Link to template On-Prem Database

On-Prem Database Details

- > 2 Entity Rules
- > 7 KPIs
- > 0 services already linked to this template

Settings

Enable 7 days of backfill for all service KPIs. ?

Cancel Create

Services Lab

- ▶ The new 'On-Prem Database' service is based on a template, if you review the 'Entities' tab we can see that the entities are already filtered.

The screenshot shows the 'On-Prem Database' service configuration page. The 'Entities' tab is active. Below the navigation tabs, there is a descriptive text: 'Entity Rules allow for the optional, dynamic filtering of KPIs and can help in root cause analysis. A service need not define any Entity Rules and is not limited to only the entities matching Entity Rules.'

There are four Entity Rules defined:

- Rule 1: Info dropdown, 'itsi_role' selected, matches 'database_instance' (circled in red).
- Rule 2: Alias dropdown, 'database_instance' selected, matches 'mysql*'.
- Rule 3: Info dropdown, 'itsi_role' selected, matches 'SAI'.
- Rule 4: Alias dropdown, 'host' selected, matches 'mysql*'.

Below the rules, there are buttons for '+ Add Rule (AND)' and '+ Add Set of Rules (OR)'.

The 'Matched Entities' section shows a table with 4 entities. The first three rows are circled in red:

Title	Aliases	Info
mysql-01	10.2.2.1, mysql-01	linux, database, 2.6.32-573.8.1.el6.x86_64, db, mysql-01, sai, eyjob3n0jogim15c3fsltayiwgimlwjogjwjjumi4xin0=
mysql-02	10.2.2.2, mysql-02	linux, database, 2.6.32-573.8.1.el6.x86_64, db, mysql-02, sai, eyjob3n0jogim15c3fsltayiwgimlwjogjwjjumi4yin0=
mysql-03	10.2.2.3, mysql-03	linux, database, 2.6.32-573.8.1.el6.x86_64, db, mysql-03, sai, eyjob3n0jogim15c3fsltayiwgimlwjogjwjjumi4zin0=

Services Lab

Under the KPIs tab we can see some KPIs that have been inherited from the service template, the padlocks indicate that changes to the template will be pushed to all linked services.

▶ Click 'Database Queries' KPIs to review.

The screenshot shows the 'On-Prem Database' service page. The 'KPIs' tab is selected and circled in red. The 'Database Queries' KPI is highlighted in a dark blue bar and also has a red circle around its padlock icon. The main content area displays the 'Database Queries' KPI description and a list of three sub-KPIs: 'Search and Calculate', 'Thresholding', and 'Anomaly Detection', each with a right-pointing chevron and a padlock icon. The left sidebar lists other KPIs such as 'Disk I/O - Read Ops', 'Disk I/O - Write Ops', 'Disk Space Used %', 'Memory Used %', 'Network Throughput - Inbound', and 'Network Throughput - Outbound', all with padlock icons.

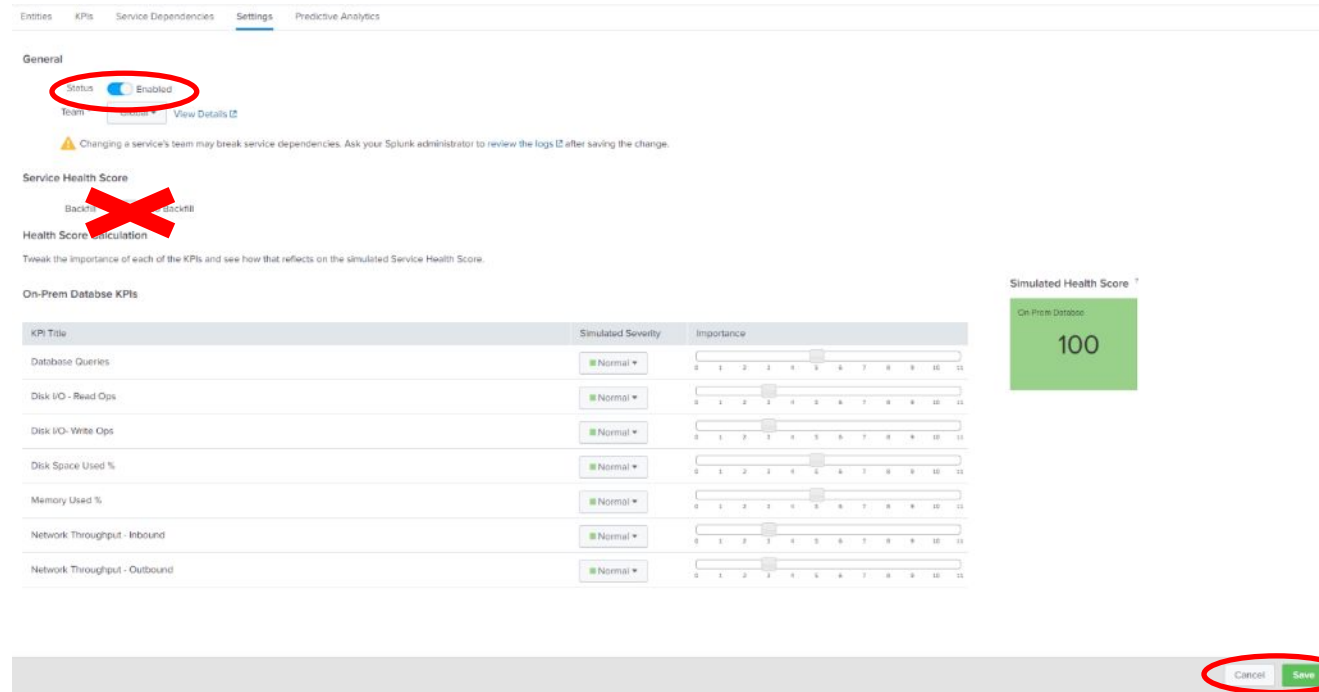
Services Lab

The 'Settings' tab enables configuration of the service attributes. The new (linked) database service is disabled by default.

- ▶ Switch to Setting tab
- ▶ Toggle status to 'Enable'
- ▶ Investigate the effect changing the Importance and Simulated Severity has, on the Simulated Health Score

▶ **Please do NOT enable Service Health Score backfill at this point**

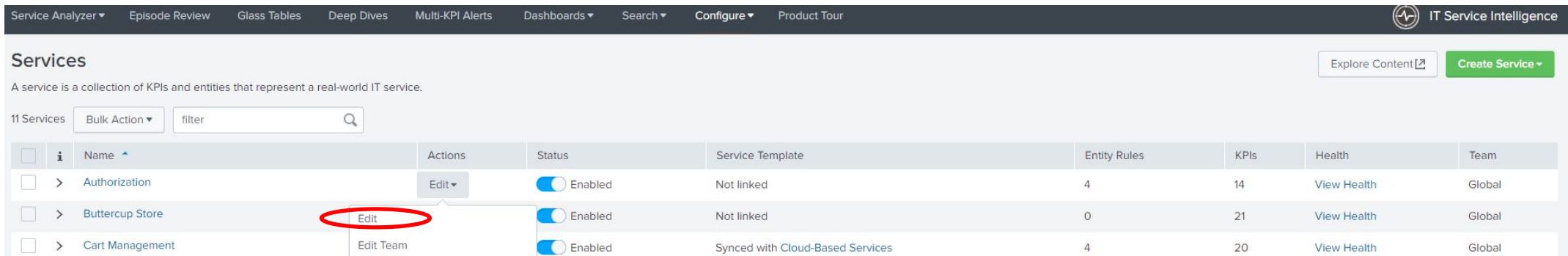
- ▶ Click the 'Save' button (Bottom-Right)



Services Lab

The new Database service will be a dependency of the **Authorization** service, any service health changes will be propagated to the parent service(s).

- ▶ Select *Configure > Services*
- ▶ Edit the *'Authorization' service*



Service Analyzer | Episode Review | Glass Tables | Deep Dives | Multi-KPI Alerts | Dashboards | Search | Configure | Product Tour | IT Service Intelligence

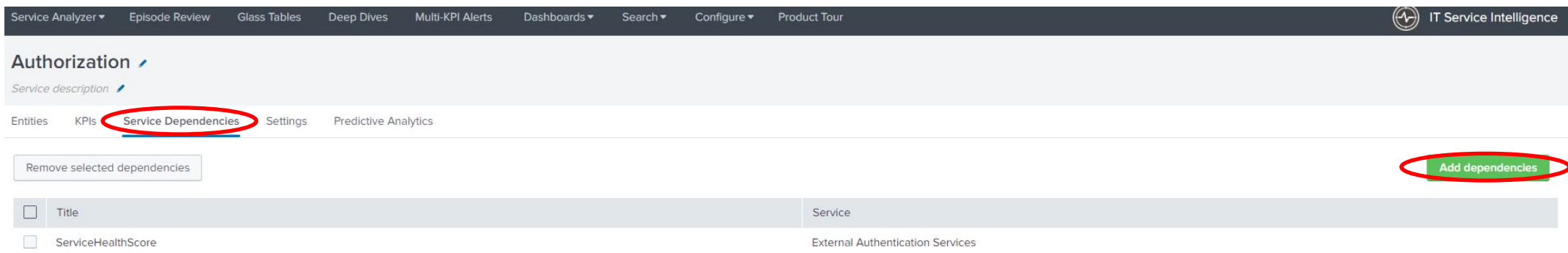
Services

A service is a collection of KPIs and entities that represent a real-world IT service.

11 Services | Bulk Action | filter

	Name	Actions	Status	Service Template	Entity Rules	KPIs	Health	Team
<input type="checkbox"/>	> Authorization	Edit	Enabled	Not linked	4	14	View Health	Global
<input type="checkbox"/>	> Buttercup Store	Edit	Enabled	Not linked	0	21	View Health	Global
<input type="checkbox"/>	> Cart Management	Edit Team	Enabled	Synced with Cloud-Based Services	4	20	View Health	Global

- ▶ Click *'Service Dependencies' tab*



Service Analyzer | Episode Review | Glass Tables | Deep Dives | Multi-KPI Alerts | Dashboards | Search | Configure | Product Tour | IT Service Intelligence

Authorization

Service description

Entities | KPIs | Service Dependencies | Settings | Predictive Analytics

Remove selected dependencies | Add dependencies

	Title	Service
<input type="checkbox"/>	ServiceHealthScore	External Authentication Services

Services Lab

- ▶ Tick 'On-Prem Database' service
- ▶ Tick the 'ServiceHealthScore'

- ▶ Press 'Done' button

- ▶ Press 'Save' button

Add dependencies

- Network Services
- Networking
- NTP
- On-Prem Database
- Order Management
- Product Catalog
- Shared Database Environment
- Shared IT Infrastructure
- Shared Storage
- Shared Storage - Arrays
- Shared Storage - LUNs
- Shared Storage - Volumes
- SMTP - DM7 In

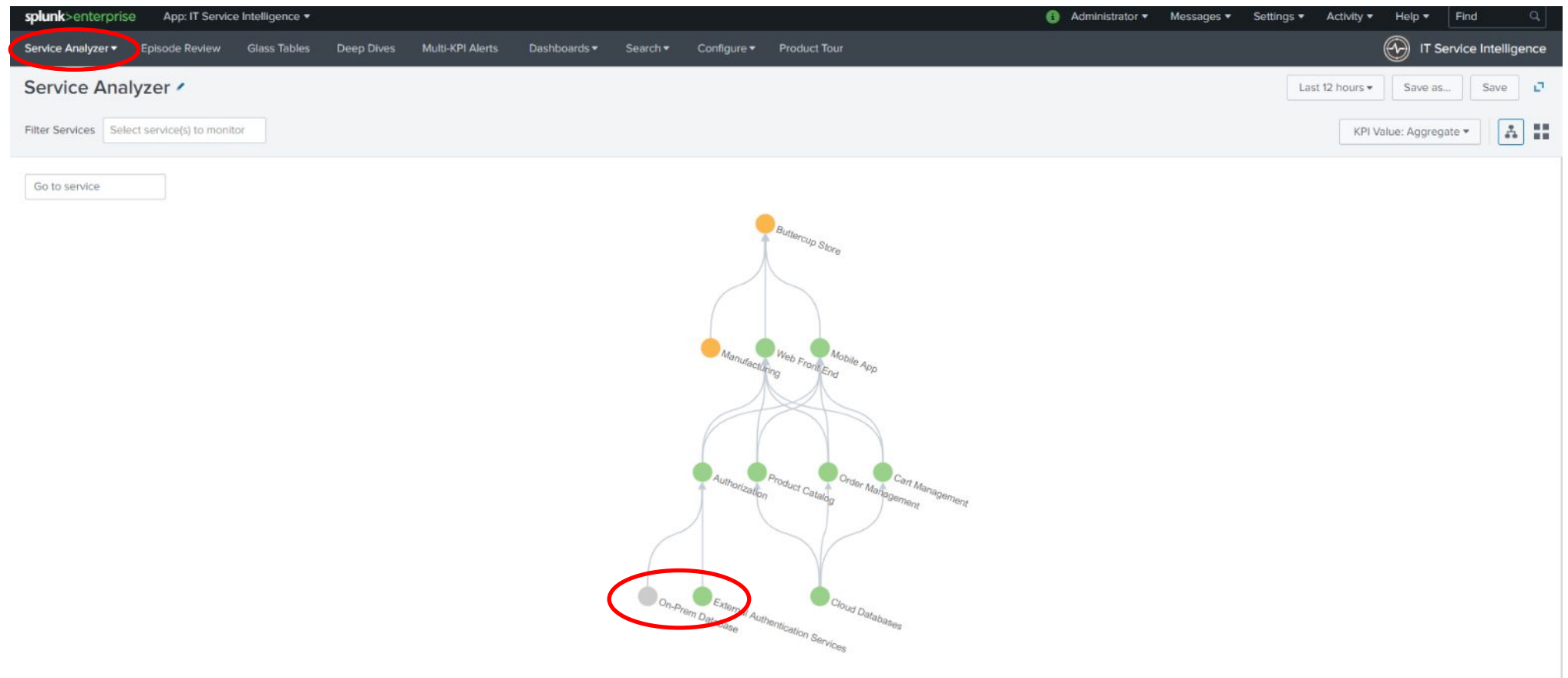
<input type="checkbox"/>	KPI Title	Service Title
<input checked="" type="checkbox"/>	ServiceHealthScore	On-Prem Database
<input type="checkbox"/>	Database Queries	On-Prem Database
<input type="checkbox"/>	Disk I/O - Read Ops	On-Prem Database
<input type="checkbox"/>	Disk I/O- Write Ops	On-Prem Database
<input type="checkbox"/>	Disk Space Used %	On-Prem Database
<input type="checkbox"/>	Memory Used %	On-Prem Database
<input type="checkbox"/>	Network Throughput - Inbound	On-Prem Database
<input type="checkbox"/>	Network Throughput - Outbound	On-Prem Database

Cancel

Done

Check Service Tree

- ▶ Next go to Service Analyzer, and select the service tree
- ▶ Check if the On-Prem database is added



KPI Exercise

KPI Lab

The new 'On-Prem Database' service is based on a template however we need to add an extra ad-hoc KPI to monitor the CPU utilization.

- ▶ Select Configure > Services
 - ▶ Select the 'On-Prem Database'
 - ▶ Select KPI tab
 - ▶ Click New > Generic KPI
 - ▶ Set Title to 'CPU Utilization %'
-
- ▶ Click 'Next' button

CPU Utilization %
Step 1 of 7: Title and Description

Title CPU Utilization %

Description optional

> Generated Search

Cancel Back Next Finish

KPI Lab

The new KPI source could be driven by a data model, ad-hoc search or a base search. It is always best to utilize base searches as they can return multiple KPI metrics with a single search.

- ▶ Click 'Base Search'
- ▶ Select 'All Metrics'
- ▶ Select 'Average CPU (Linux)'

CPU Utilization %
Step 2 of 7: Source

KPI Source ? Data Model Metrics Search Ad hoc Search **Base Search**

Base Search ? **All Metrics** ▼
[Edit Base Search](#)

Metric ? **Average CPU (Linux)** ▼

> Generated Search


Cancel Back **Next** Finish

- ▶ Click 'Next' button

KPI Lab

▶ There is no option to split this base search.

CPU Utilization % ×
Step 3 of 7: Entities

 Fields are populated from the selected base search.

Split by Entity ? Yes No

Entity Split Field ?

Filter to Entities in Service ? Yes No
Service must have entities to filter by entities.

Entity Filter Field ?

> Generated Search

▶ Click 'Next' button

KPI Lab

We need to build the KPI calculation criteria, this includes how often data is collected, the entity calculation and the calculation window.

- ▶ We have decided that the metric will be collected every 5 minutes
- ▶ We want to perform an **Average** of the metric
- ▶ Over 5 min window
- ▶ Click 'Next' button

CPU Utilization %

Step 4 of 7: Calculation

⚠ Fields are populated from the selected base search.

Calculation Options:

KPI Search Schedule ?	Every 5 minutes ▾
Entity Calculation ?	Average ▾
Service/Aggregate Calculation ?	Average ▾
Calculation Window ?	Last 5 minutes ▾
Fill Data Gaps with ?	Null values ▾
Threshold level for Null values ?	Unknown ▾

Explanation of Calculation:

Every 5 minutes take the average of avgcpu for each entity as the entity value then take the average of all entity values as

> Generated Search


Cancel Back **Next** Finish

KPI Lab

The monitoring and unit fields will be populated from the base search.

CPU Utilization %

Step 5 of 7: Optional Setup - Unit and Monitoring Lag

 Fields are populated from the selected base search.

Unit

Specify the unit of measurement to display in KPI visualizations. (For example "GB," "Mbps," "secs", etc.).

Monitoring Lag (in seconds) ?

[Determine Recommended Lag](#)

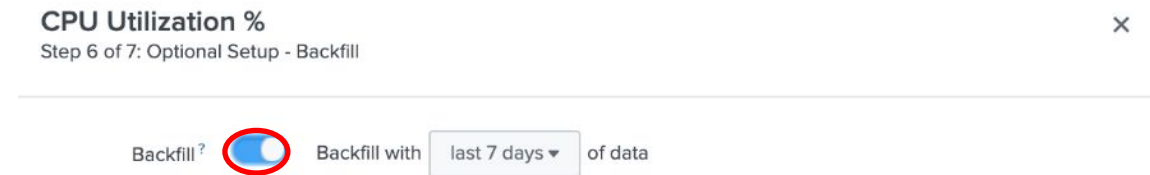
> Generated Search

 Click 'Next' button

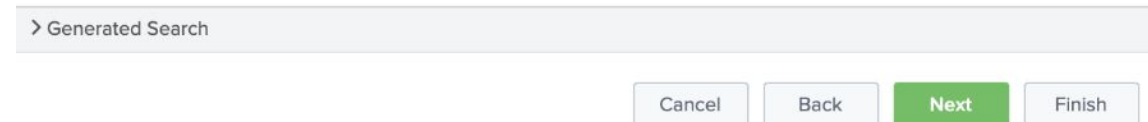
KPI Lab

We want this KPI to use data already ingested in Splunk over the last 7 days.

- ▶ Click 'Enable Backfill' button
- ▶ We will leave the backfill period as 7 days



- ▶ Click 'Next' button



KPI Lab

We need to set some static thresholds for this new KPI

- ▶ Increase time to 4 hours
- ▶ Add & configure threshold:
 - Critical = 95
 - High = 90
 - Medium = 85
 - Low = 70

- ▶ Click *'Finish'* button

CPU Utilization %
Step 7 of 7: Thresholds

Aggregate Thresholds Per-Entity Thresholds

Aggregate Threshold Values

Critical	95	x
High	90	x
Medium	85	x
Low	70	x

+ Add Threshold

Base Severity

Normal

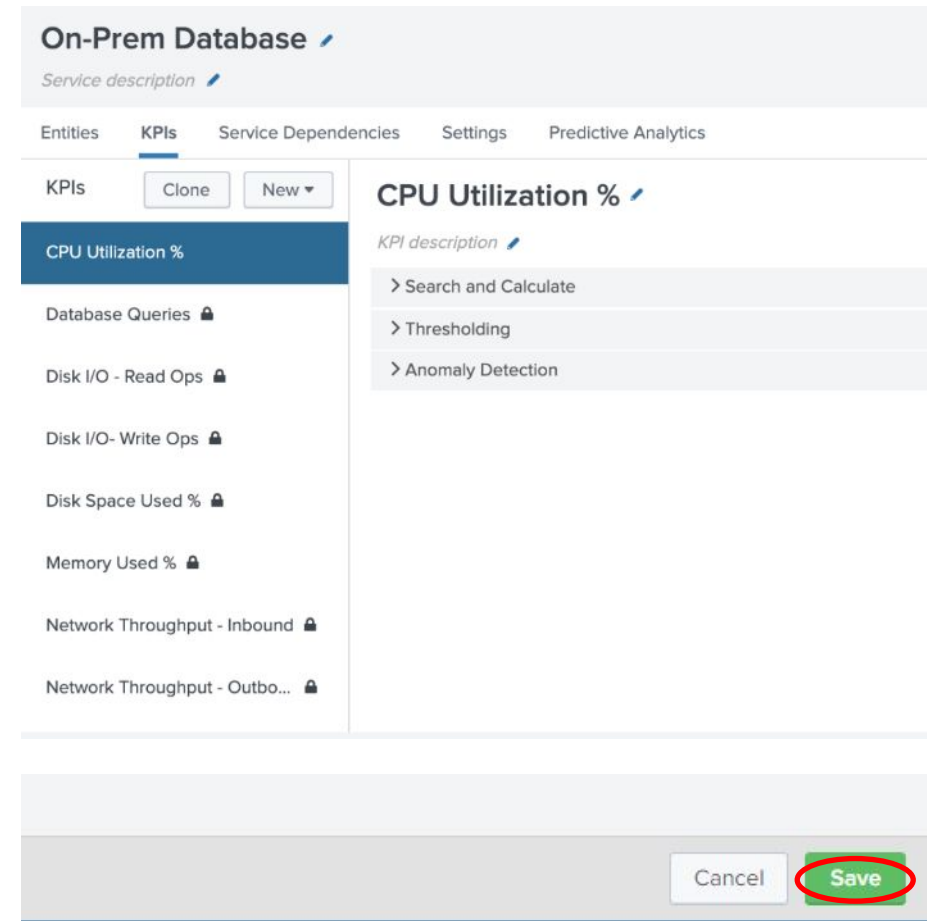
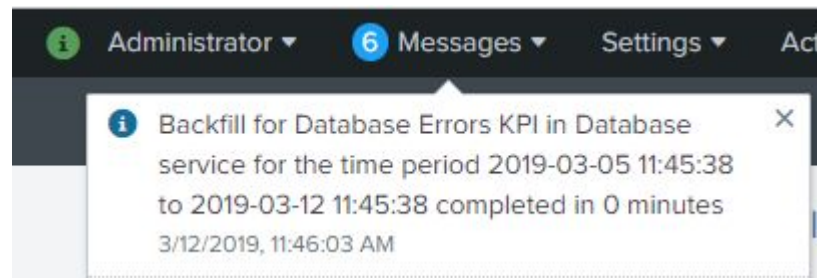
View data from last 60 minutes

> Generated Search

Cancel Back Next Finish

KPI Lab

- ▶ Note that the new KPI does not have a padlock icon. Inherited KPIs are locked to the service template so when changes are made these are pushed to the linked services, such as the one we are configuring.
- ▶ If you edit a locked KPI it will become an orphan and template changes no longer adopted
- ▶ *Click 'Save' button! Bottom Right*



KPI Lab

An important dependency for the new 'On-Prem Database' service is response time, in this lab we will add an extra KPI: 'Database Response Time'. For this KPI we use an ad-hoc search.

- ▶ Click Configure > Services
- ▶ Click 'On-Prem Database' & KPI tab
- ▶ Click New KPI > Generic KPI
- ▶ Title = 'Database Response Time'
- ▶ Click 'Next' button

The screenshot shows the Splunk Enterprise interface for configuring a new KPI. The main window is titled 'Database Response Time' and is at 'Step 1 of 7: Title and Description'. The 'Title' field contains the text 'Database Response Time', which is circled in red. The 'Description' field contains the text 'optional'. At the bottom of the window, there are three buttons: 'Cancel', 'Back', and 'Next', with the 'Next' button circled in red. The background shows the 'Database' service configuration page with various tabs and options.

KPI Lab

The new KPI source could be driven by a data model, ad-hoc search or a base search. In this instance we will create the KPI using an ad-hoc search.

- ▶ Click 'Ad-hoc Search'
 - ▶ Enter the following search:
 - `index=itsidemo sourcetype=stream:mysql query=*`
 - ▶ Enter 'time_taken' as the threshold field
 - ▶ Click 'Run Search' button to test search
-
- ▶ Click 'Next' button

Database Response Time
Step 2 of 7: Source

KPI Source ? Data Model Metrics Search Ad hoc Search Base Search

Search ? `index=itsidemo sourcetype=stream:mysql query=*`

[Run Search](#)

Threshold Field ? `time_taken`

> Generated Search

Cancel Back Next Finish

KPI Lab

We will split this KPI via the database name and filter via ip address.

- ▶ Select 'Yes' for split by entity
 - ▶ Enter 'dbname' as the split by field
 - ▶ Select 'Yes' for filter to entities in Service
 - ▶ Type 'ip' for entity filter field
-
- ▶ Click Next

Database Response Time ×
Step 3 of 7: Entities

Split by Entity ? Yes No

Entity Split Field ?

Filter to Entities in Service ? Yes No
Service must have entities to filter by entities.

Entity Filter Field ?

> Generated Search

KPI Lab

The database response time KPI will have the following calculation options.

- ▶ Schedule = Every minute
- ▶ Entity Calculation = Average
- ▶ Aggregate Calculation = Average
- ▶ Calculation Window = 5 minutes

- ▶ Click Next

Database Response Time

Step 4 of 7: Calculation

Calculation Options:

KPI Search Schedule ?	Every minute ▾
Entity Calculation ?	Average ▾
Service/Aggregate Calculation ?	Average ▾
Calculation Window ?	Last 5 minutes ▾
Fill Data Gaps with ?	Null values ▾
Threshold level for Null values ?	Unknown ▾

Explanation of Calculation:

Every minute take the average of time_taken for each entity as the entity value then take the average of all entity values as the service/aggregate value all over the last 5 minutes. Fill gaps in data with Null values and use a unknown threshold level for them.

> Generated Search

Cancel Back **Next** Finish

KPI Lab

We will leave the next screen with the default values.

Database Response Time

Step 5 of 7: Optional Setup - Unit and Monitoring Lag



Unit

Specify the unit of measurement to display in KPI visualizations. (For example "GB," "Mbps," "secs", etc.).

Monitoring Lag (in
seconds) ?

[Determine Recommended Lag](#)

 Click Next

> Generated Search

Cancel

Back

Next

Finish

KPI Lab

We want this KPI to use data already ingested in Splunk over the last 7 days. This historical data will be used in the machine learning labs.

- ▶ Click 'Enable Backfill' button
- ▶ We will leave the backfill period as 7 days

- ▶ Click 'Next' button

Database Response Time
Step 6 of 7: Optional Setup - Backfill

Backfill? Backfill with last 7 days of data

> Generated Search

Cancel Back **Next** Finish

KPI Lab

We need to set some static thresholds for this new KPI

- ▶ Increase time to 4 hours
- ▶ Add & configure threshold:
 - High = 360
 - Medium = 310
 - Low = 200
- ▶ Click 'Finish' button
- ▶ Do not forget to click 'Save' button!!

Database Response Time

Step 7 of 7: Thresholds

Aggregate Thresholds | Per-Entity Thresholds

Aggregate Threshold Values

High	360	x
Medium	310	x
Low	200	x

+ Add Threshold

Base Severity

Normal

View data from last 4 hours

> Generated Search

Cancel Back Next Finish

KPI Lab

We have two new KPIs for our On-Prem Database service, this new service can utilize past data via the Service Health Score backfill capability.

▶ Switch to the 'Settings' tab

▶ Toggle backfill on (last 7 days)

▶ Click 'Save' button

On-Prem Database

Service description

Entities KPIs Service Dependencies **Settings** Predictive Analytics

General

Status Enabled

Team [?] Global [View Details](#)

⚠ Changing a service's team may break service dependencies. Ask your Splunk administrator to [review the logs](#) after saving the change.

Service Health Score

Backfill Backfill with last 7 days of data

⚠ It is advised that you first backfill the KPIs in this service and all dependent services for at least the time range selected here. Enabling backfill for a KPI does not mean backfill has completed. Wait for a successful backfill completion message for all KPIs before backfilling the service health score.

Health Score Calculation

Tweak the importance of each of the KPIs and see how that reflects on the simulated Service Health Score.

On-Prem Database KPIs

KPI Title	Simulated Severity	Importance
CPU Utilization %	Normal	5
Database Queries	Normal	5
Database Response Time	Normal	5
Disk I/O - Read Ops	Normal	3

Simulated Health Score [?]

On-Prem Database

100

Cancel Save

KPI Lab

There are now two new KPIs visible in the Service Analyzer for the On-Prem Database service, these KPIs contain historical data and we can see there is an issue with the CPU data.

- ▶ Navigate back to Service Analyzer
- ▶ Click 'On-Prem Database' service
- ▶ Select the new 'CPU Utilization %' KPI
- ▶ Click 'mysql-02' entity

The screenshot shows the Service Analyzer interface for the 'Buttercup Store' service. On the left is a service tree with 'On-Prem Database' highlighted. The main panel displays two KPI cards: 'On-Prem Database' with a value of 87.5 and 'CPU Utilization %' with a value of 58.52. Below these are two tables. The first table lists 9 KPIs, with 'Disk Space Used %' circled in red. The second table lists 4 entities, with 'mysql-02' circled in red.

Severity	KPI Name	Value
High	Database Response Time	378.29
Low	Disk Space Used %	80.44
Normal	CPU Utilization %	58.52
Normal	Disk I/O - Read Ops	3494.33
Normal	Disk I/O - Write Ops	2899.68
Normal	Memory Used %	76.28
Normal	Network Throughout - Inbound	4.39

Severity	Entity Name	Value
Normal	mysql-01	58.13
Normal	mysql-02	66.64
Normal	mysql-03	62.67
Normal	mysql-04	46.62

KPI Lab

The 'Entities Details' view is a high-level dashboard showing metric data for the selected entity.

- ▶ Click the Splunk App for Infrastructure for more metric information.

mysql-02 Last 12 hours Edit Entity

host mysql-02 itsi_role SAI os Linux
ip 10.2.2.2 name mysql-02 [Show 4 more](#)

Modules

- [Splunk App for Infrastructure](#)

Overall Health

KPIs					Services			
Severity	KPI	Service	Sparkline	Alert Value	Severity	Service	Sparkline	Alert Value
Critical	Memory Free: MB	Database		905	Critical	Database_Original		20.0
Critical	Memory Free: MB	Database_Original		905	High	Database		34.0
Normal	CPU Utilization: %	Database		28				
Normal	Database Errors	Database		25				
Normal	Database KPI 6	Database		6				
Normal	Storage Free Space: %	Database		6				
Normal	CPU Utilization: %	Database_Original		28				

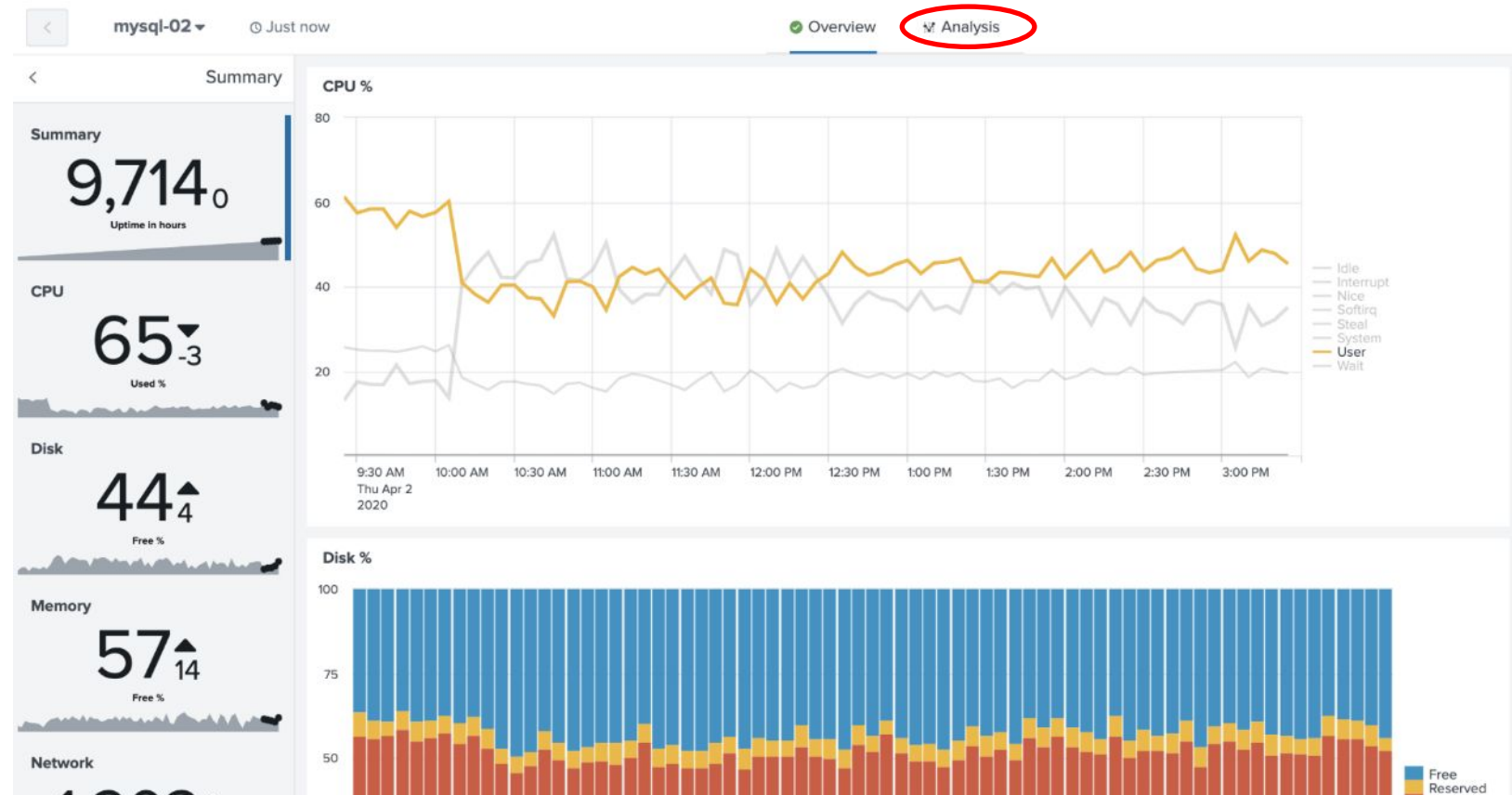
Notable Events

Entity	Notification	When
mysql-02	Nagios Service Check: check_ntp_time on mysql-02	2019-07-23T10:20:06Z
mysql-02	Nagios Service Check: check_dhcp on mysql-02	2019-07-23T10:20:06Z

KPI Lab

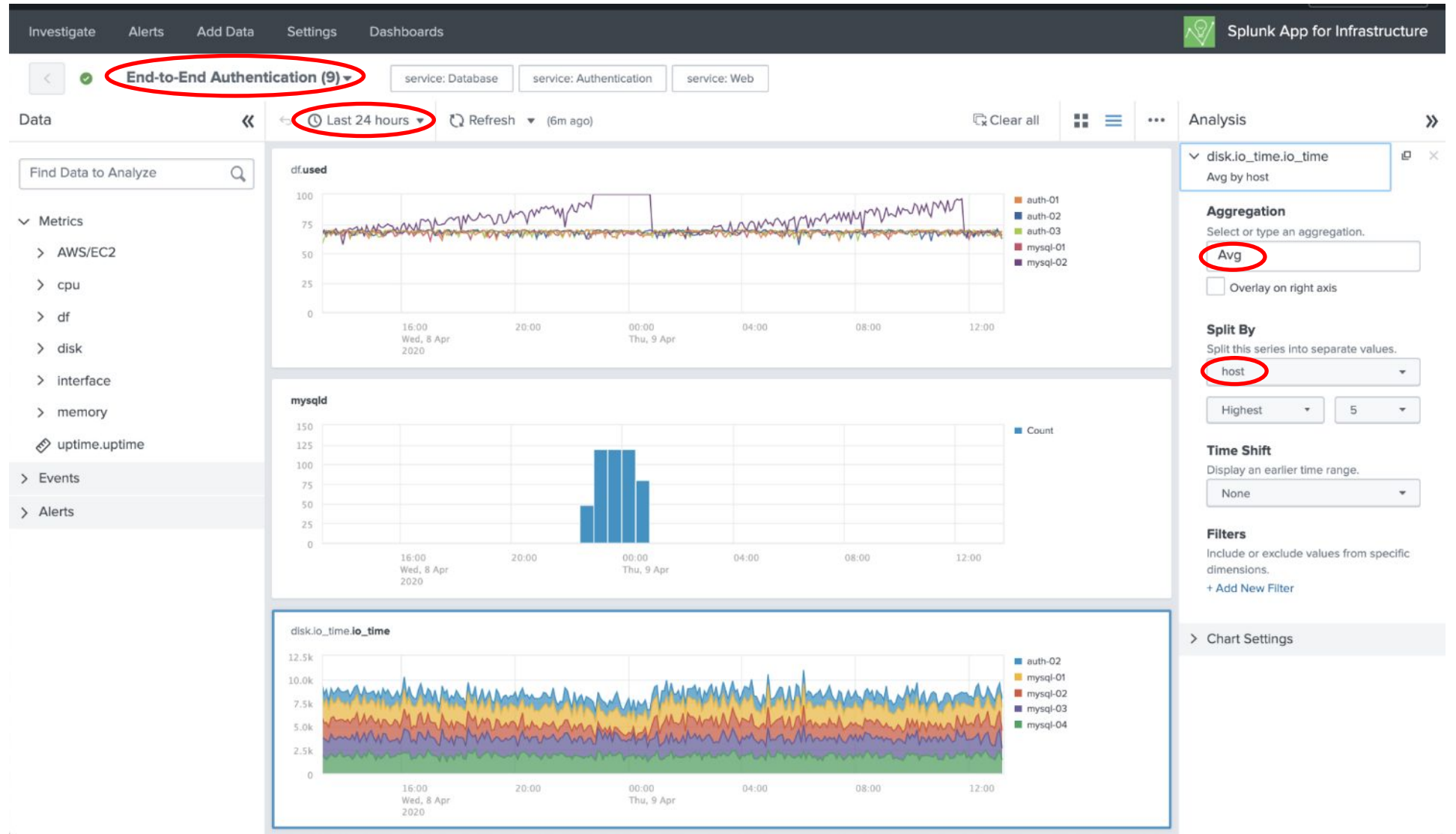
The Splunk app for Infrastructure is a workspace to quickly drag and drop metric values.

- ▶ Click the 'analysis' tab to investigate the collected metrics for this entity.



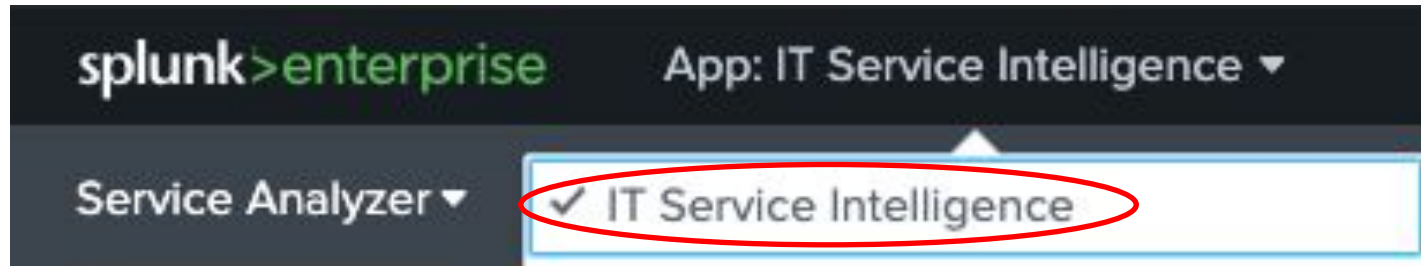
KPI Lab

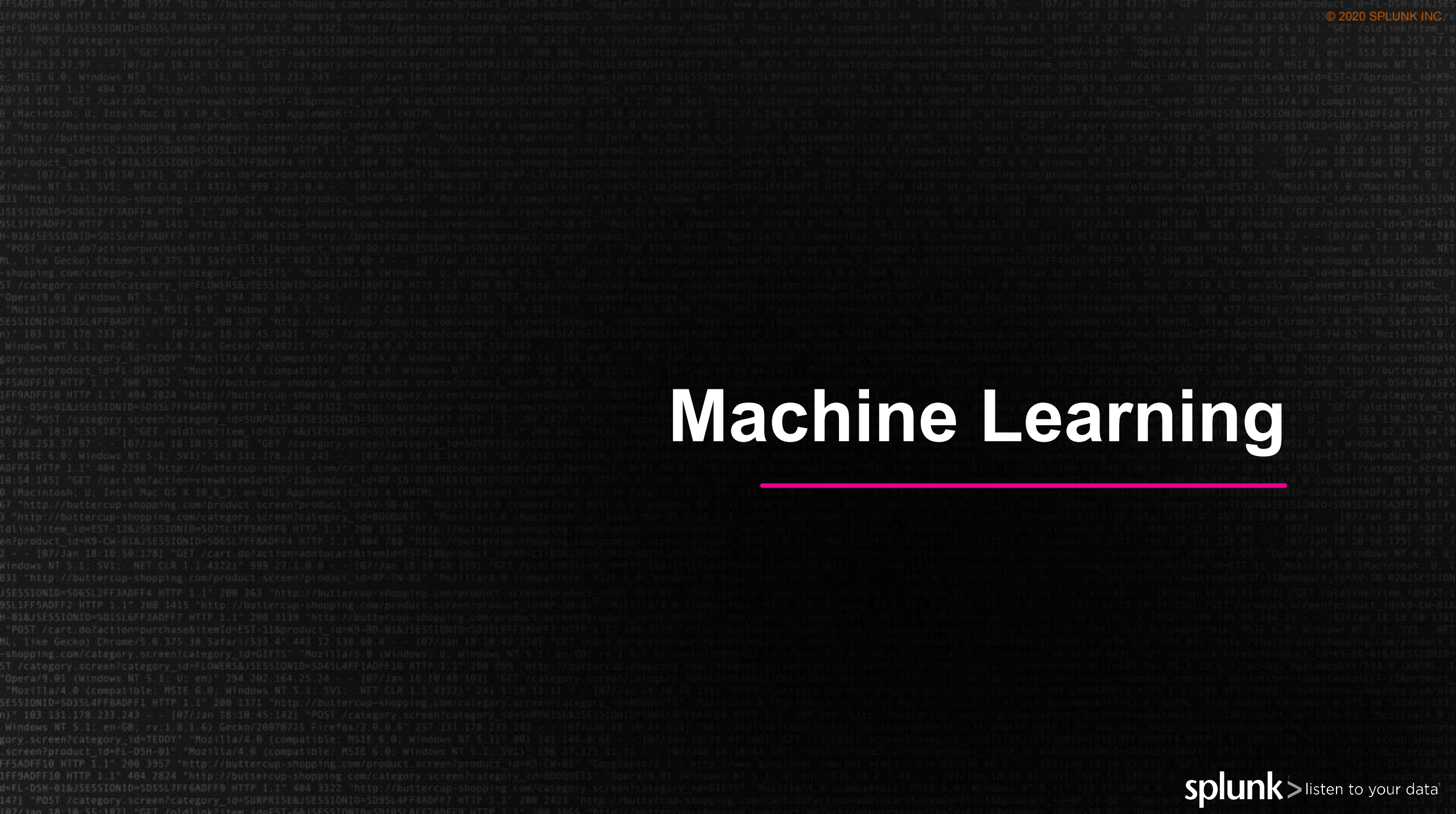
▶ Challenge – If there is time attempt to recreating the following dashboard.



KPI Lab

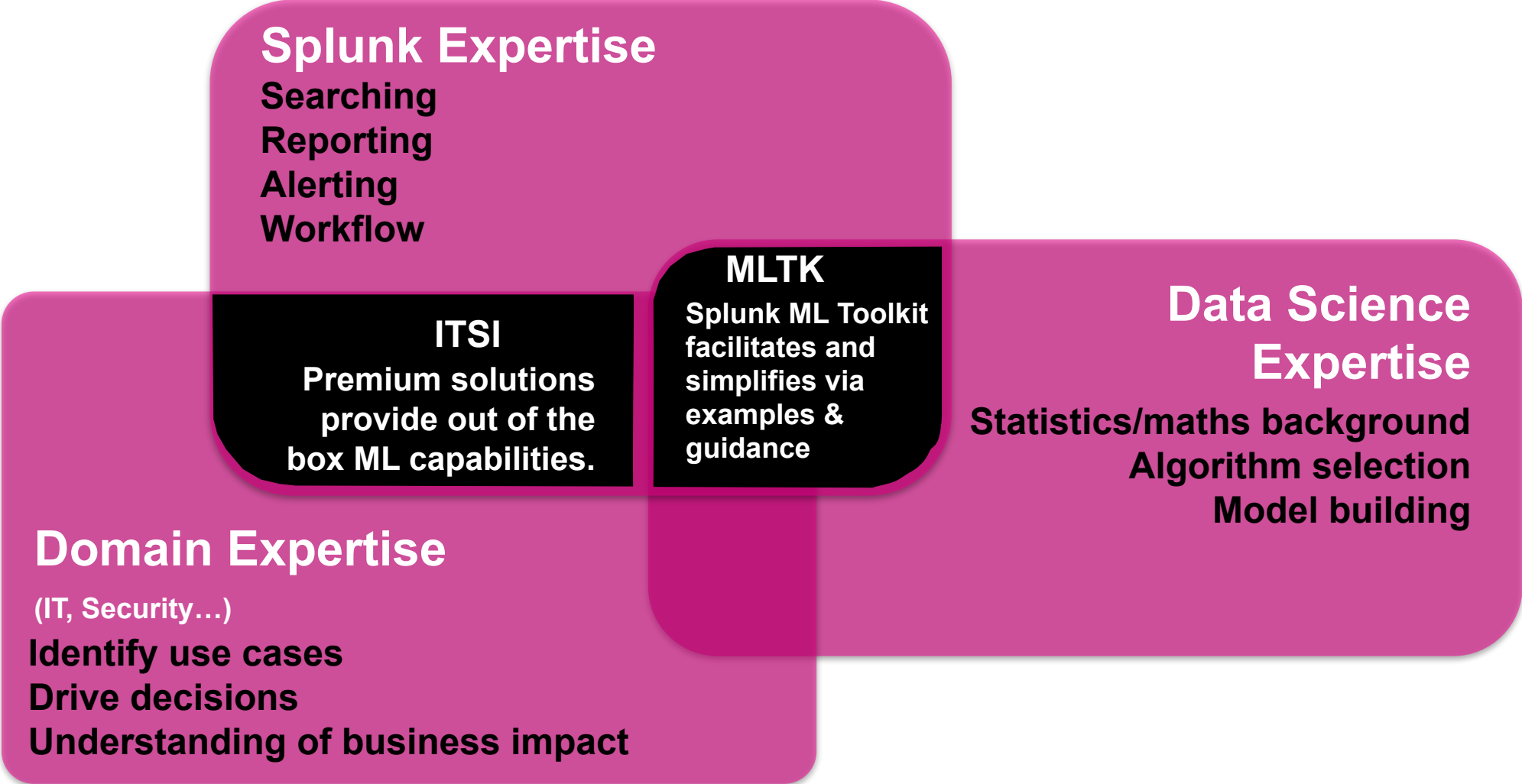
- ▶ Navigate back to ITSI app for remaining labs.





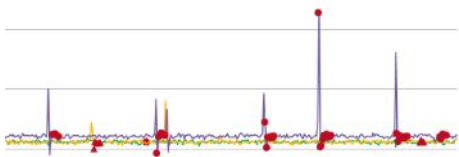
Machine Learning

Skill Areas for Machine Learning at Splunk



ITSI Machine Learning

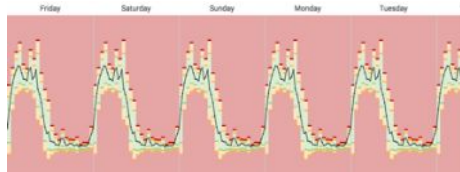
Anomaly Detection



- Deviation from past behavior
- Deviation from peers
- Unusual change in features

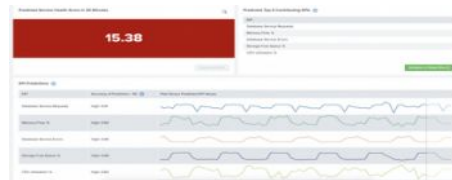
ITSI Anomaly Detection

Adaptive Thresholds



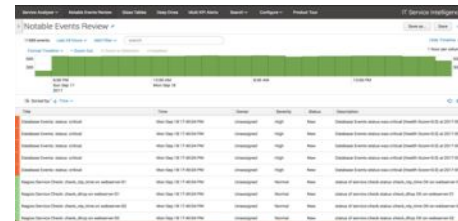
- Adaptive Thresholds**
- What is normal behaviour and what is not normal
- Ideal for cyclical and dynamic data

Predictions Analytics



- Predict Service Health Score**
- Predicting events
- Trend forecasting
- Early warning of failure
- Predictive maintenance

Event Clustering

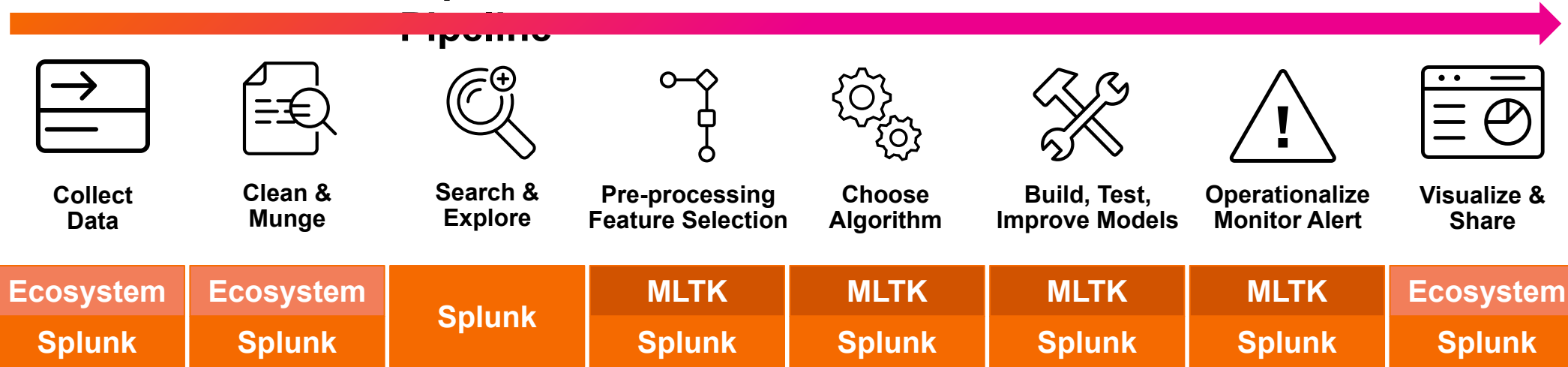


- Identify peer groups
- Event correlation
- Reduce alert noise
- ITSI Event Analytics**

Machine Learning process

- Ecosystem** Splunk's App Ecosystem contains 1000's of free add-ons for getting data in, applying structure and visualizing your data giving you faster time to value.
- MLTK** The Machine Learning Toolkit delivers new SPL commands, custom visualizations, assistants, and examples to explore a variety of ml concepts.
- Splunk** Splunk Enterprise is the mission-critical platform for indexing, searching, analyzing, alerting and visualizing machine data.

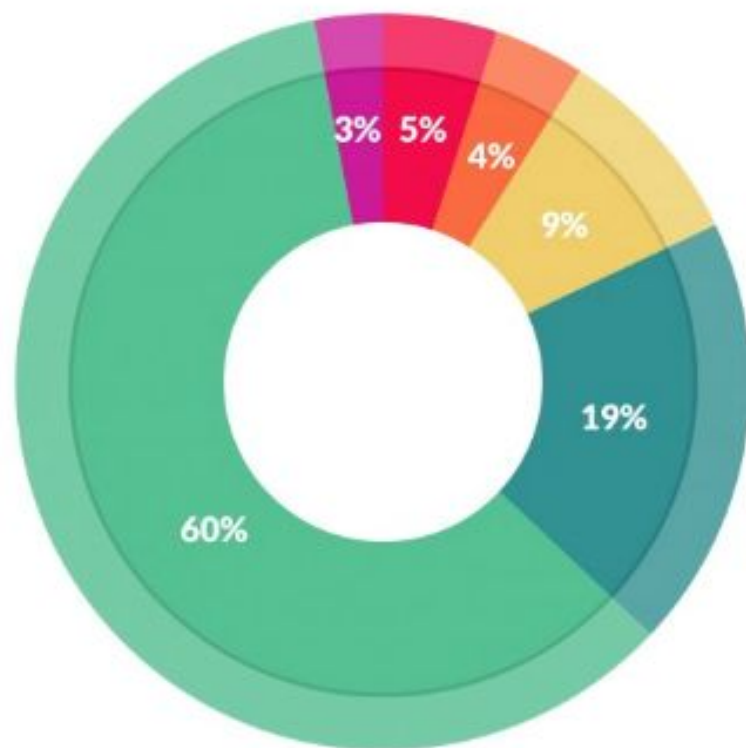
Operationalized Data Science



splunk > turn data into doing™

What Data Scientists Really Do

Data Preparation accounts for about 80% of the work of data scientists



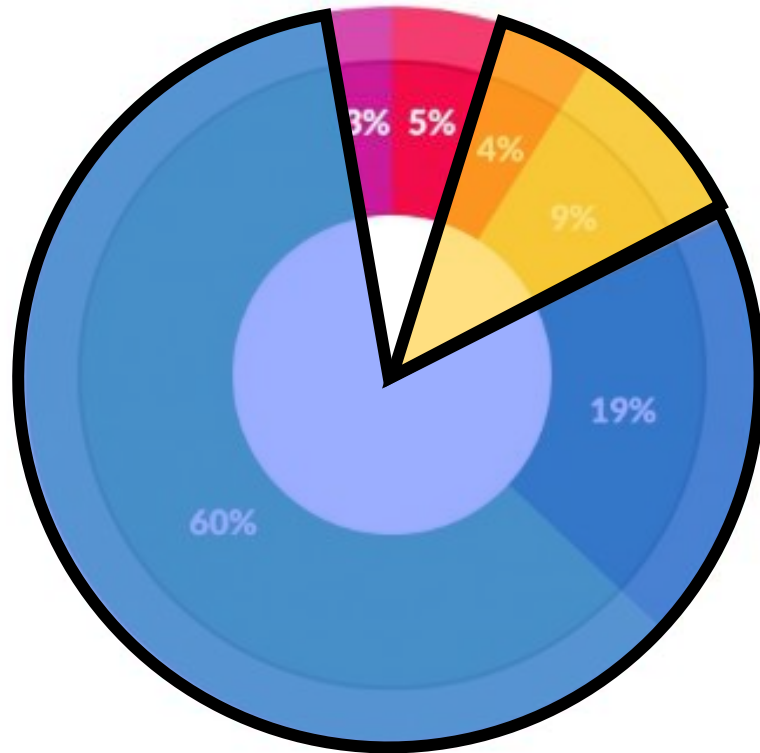
What data scientists spend the most time doing

- Building training sets: 3%
- Cleaning and organizing data: 60%
- Collecting data sets; 19%
- Mining data for patterns: 9%
- Refining algorithms: 4%
- Other: 5%

“Cleaning Big Data: Most Time-Consuming, Least Enjoyable Data Science Task, Survey Says”, Forbes Mar 23, 2016

What Data Scientists Really Do

Data Preparation accounts for about 80% of the work of data scientists



What data scientists spend the most time doing

- Building training sets: 3%
- Cleaning and organizing data: 60%
- Collecting data sets; 19%
- Mining data for patterns: 9%
- Refining algorithms: 4%
- Other: 5%

“Cleaning Big Data: Most Time-Consuming, Least Enjoyable Data Science Task, Survey Says”, Forbes Mar 23, 2016

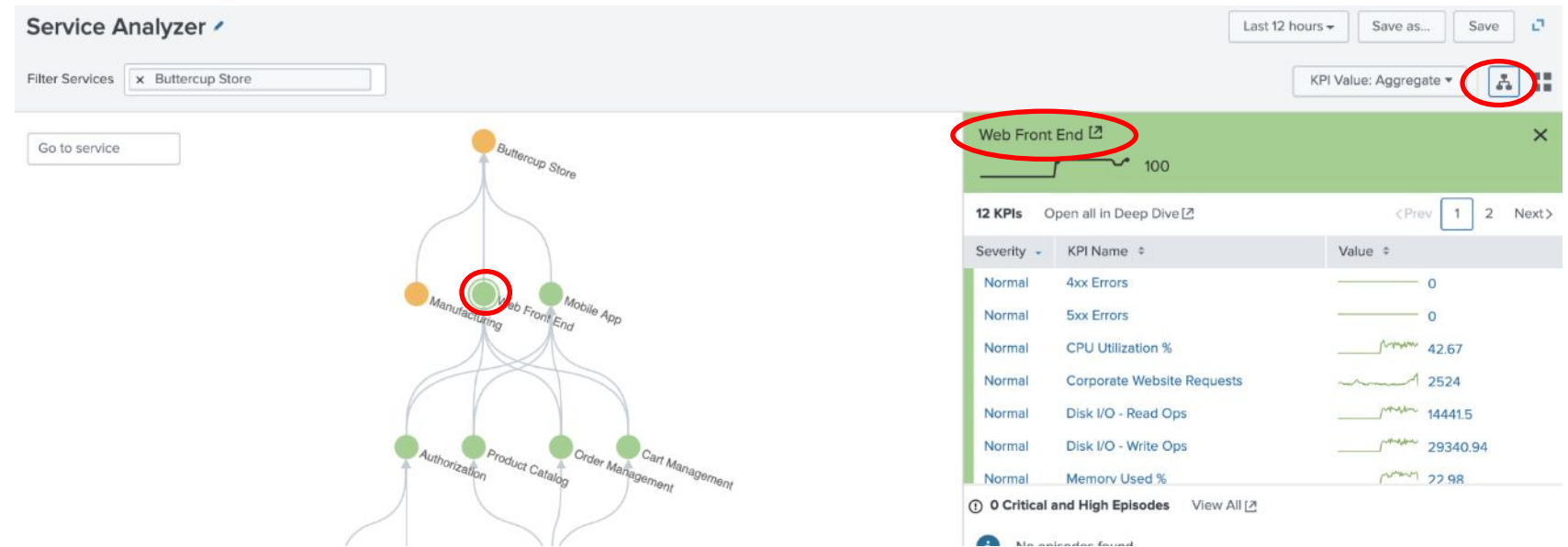
Machine Learning Use Case

- ▶ There have been lots of social media comments regarding Buttercup' website availability, especially during the evenings.
- ▶ Luckily the website data is being ingested by Splunk, this sourcetype is called 'access_combined' and contains lots of information.
- ▶ The objective of this exercise to is utilise Splunk ITSI machine learning capabilities to identify normal behaviour for web response time.
- ▶ We will also look to see if the application servers supporting the website are functioning equally.

Machine Learning Lab

The Corporate Website Request KPI has no thresholding for alerting. In this lab we will configure machine learning to understand what normal looks like and alert us when the KPI falls outside this range.

- ▶ Go to the 'default' service analyzer view and expand the tree view
- ▶ Click 'Web Front End' service
- ▶ Select the 'Web Front End' link



The screenshot shows the Service Analyzer interface. The top navigation bar includes 'Service Analyzer', a filter for 'Buttercup Store', and a 'KPI Value: Aggregate' dropdown menu. The main area displays a hierarchical tree view of services. The 'Web Front End' service is highlighted with a red circle. To the right, a panel titled 'Web Front End' shows a list of 12 KPIs. The 'Corporate Website Requests' KPI is highlighted with a red circle. Below the KPI list, there are 0 Critical and High Episodes.

Severity	KPI Name	Value
Normal	4xx Errors	0
Normal	5xx Errors	0
Normal	CPU Utilization %	42.67
Normal	Corporate Website Requests	2524
Normal	Disk I/O - Read Ops	14441.5
Normal	Disk I/O - Write Ops	29340.94
Normal	Memory Used %	22.98

Machine Learning Lab

We need to instruct ITSI to use a template for thresholding, we will be using the adaptive standard deviation 3 hour working week template.

- ▶ Select the 'Corporate Website Requests' KPI

The screenshot displays the ITSI console interface for configuring a KPI. The top navigation bar includes 'Web Front End' and 'Service description'. Below this, there are tabs for 'Entities', 'KPIs', 'Service Dependencies', 'Settings', and 'Predictive Analytics'. The 'KPIs' tab is active, showing a list of KPIs on the left sidebar. The 'Corporate Website Requests' KPI is highlighted with a red oval. The main panel shows the configuration for 'Corporate Website Requests', including a 'KPI description' and a 'Thresholding' section. The 'Thresholding' section has a dropdown menu for 'Search and Calculate' and a 'Thresholding' section with the following options:

- Use Thresholding Template (Selected a thresholding te...)
- Set Custom Thresholds
- Enable Time Policies?
- Enable Adaptive Thresholding?
- Enable KPI Alerting?

Machine Learning Lab

- ▶ Select 'use Thresholding Template' button
- ▶ Review the different options
- ▶ Select '3-hour blocks work week' (adaptive/stdev)

▶ Click 'Apply' button

Apply Threshold Template ✕

All existing threshold settings will be discarded. Are you sure you want to apply template?

Cancel Apply

Entities | **KPIs** | Service Dependencies | Settings | Predictive Analytics

KPIs Clone New ▾

4xx Errors

5xx Errors

Bytes in

Bytes out

Corporate Website Requests

CPU Utilization %

Disk I/O - Read Ops

Disk I/O - Write Ops

Memory Used %

Network Throughput - Inbound

Corporate Website Requests ✎

KPI description ✎

> Search and Calculate

Thresholding

Use Thresholding Template 3-hour blocks work we... ▾ Edit Template [↗](#)

Set Custom Threshold

Enable Time Policies?

Adaptive Thresholding rule

Enable KPI Alerting?

Training window? 7 days ▾

thresholding for the KPI base

Preview Aggregate

Thursday Monday

3-hour blocks work week (adaptive/quantile)

3-hour blocks work week (adaptive/range)

3-hour blocks work week (adaptive/stdev)

3-hour blocks work week (static)

AM, PM (adaptive/quantile)

AM, PM (adaptive/range)

AM, PM (adaptive/stdev)

Machine Learning Lab

The built-in machine learning has configured thresholds, this is broken into 1-hour time ranges. However we want to use historical data to apply some adaptive thresholding.

- ▶ Open the 'Configuration Thresholds for Time Policies' box
- ▶ Review different times
 - Choose 'Weekdays, 9am-12am'
- ▶ Click 'Apply Adaptive Thresholding' button
 - Wait 30 Seconds
- ▶ Notice threshold
- ▶ Click 'Save' button

Configure Thresholds for Time Policies

Weekdays, 7 AM

Weekdays, 7 PM

Weekdays, 8 AM

Weekdays, 8 PM

Weekdays, 9 AM

Weekdays, 9 PM

Weekends

Default

Aggregate Threshold Values

Policy type?

Standard deviation

Thresholds are computed from data. Parameter associated with the labels is the number of standard deviations away from the mean. A value of 0 would equal the mean of the data. 1 would be a single standard deviation away from the mean.

Critical 2 σ

Medium 1 σ

Normal -1 σ

Medium -2 σ

View data for Last Tuesday: 21:00 - 22:00

Apply Adaptive Thresholding

Machine Learning Lab

Internal SLAs do not apply on weekends, tracking is still necessary, but management wants deliberately higher values.

We will now modify the new adaptive thresholds to increase the weekend ranges, this will result in a custom template.

- ▶ Click on '*Thresholding*' arrow
- ▶ Review the preview window
 - Note weekend range
- ▶ Click '*Set Custom Threshold*'

Thresholding

Use Thresholding Template 1-hour blocks work week (adaptive... [Edit Template](#)

Set Custom Thresholds

Enable Time Policies: Yes No Enable Adaptive Thresholding?: Yes No Training window?: 7 days

Adaptive Thresholding runs everyday around midnight and updates the thresholding for the KPI based on the settings below. Once updated, old thresholds cannot be recovered.

Treat Gaps in Data as: Unknown

Preview Aggregate Thresholds



Machine Learning Lab

We will now modify the new adaptive thresholds to increase the weekend ranges, this will result in a custom template.

- ▶ Expand '*Configure Thresholds for Time Policies*'
- ▶ Click '*Weekends*'
- ▶ Move all sliders as show
- ▶ Click '*Apply Adaptive Thresholding*'

~ Configure Thresholds for Time Policies

Weekdays, 7 AM

Weekdays, 7 PM

Weekdays, 8 AM

Weekdays, 8 PM

Weekdays, 9 AM

Weekdays, 9 PM

Weekends

Default

Policy type?

Standard deviation ▾

Thresholds are computed from data. Parameter associated with the labels is the number of standard deviations away from the mean. A value of 0 would equal the mean of the data. 1 would be a single standard deviation away from the mean.

View data for Saturday: 23:00 - 23:59 ▾ ⚙

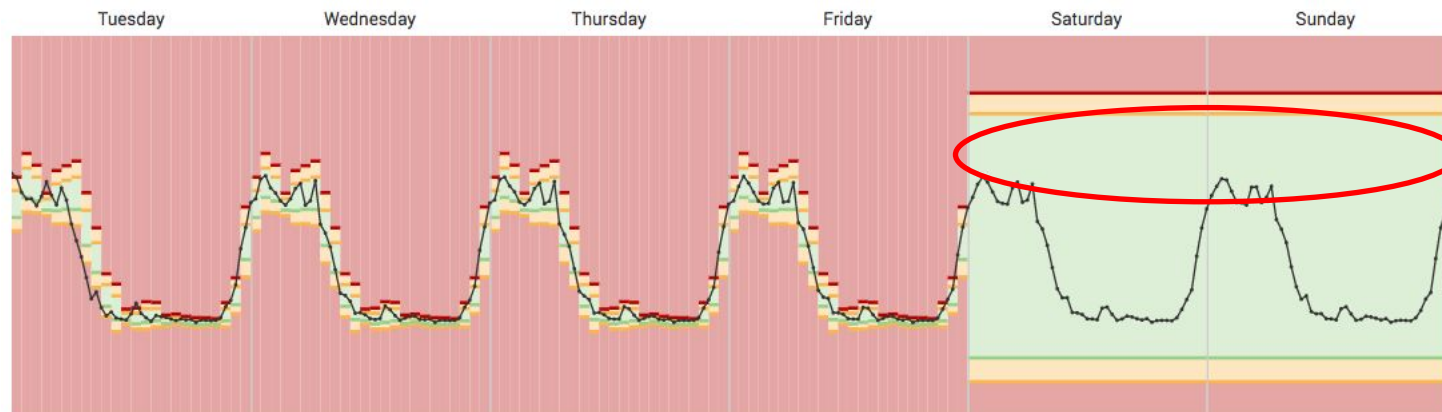
Critical ▾	2	σ	×
Medium ▾	1	σ	×
Normal ▾	-1	σ	×
Medium ▾	-2	σ	×

+ Add Threshold

Machine Learning Lab

The preview aggregate threshold window now shows that during the weekend we will not receive an warning alert for the website response time KPI.

Preview Aggregate Thresholds



▶ Click 'Save' button

Deep Dive Use Case

- ▶ Typically when organisations have outages they create a war room to identify the root cause as quickly as possible, this involves bringing together many business & technical stake holders at great expense.
- ▶ The deep dive capabilities within ITSI brings together multiple data sources into a single visualization. The correlation of data streams enable quick identification of root cause and effect on the business.
- ▶ In this lab we will build a deep dive visualization for the new On-Prem Database service, this will bring business and technical KPIs together with raw event data.
- ▶ *Extra – Once this lab is completed review the comparisons options.*

Deep Dive Lab

- ▶ Navigate to the '*Default Service Analyzer*' view
- ▶ Toggle to '*Tree View*' mode
- ▶ Click '*On-Prem Database*' service
- ▶ Click '*Open all in deep dive*'

The screenshot displays the Service Analyzer interface. At the top, the title is 'Service Analyzer'. Below it, there is a 'Filter Services' input field containing 'Buttercup Store'. To the right, there are buttons for 'Last 12 hours', 'Save as...', 'Save', and a refresh icon. A 'KPI Value: Aggregate' dropdown menu is also visible, with a red circle around its icon. Below the filter, there is a 'Go to service' button. The main area shows a hierarchical tree view of services. The 'On-Prem Database' service is highlighted with a red circle. To the right, a panel titled 'On-Prem Database' shows a line graph with a value of 70. Below the graph, there is a section for '8 KPIs' with a red circle around the text 'Open all in Deep Dive'. A table lists the KPIs with their severity, names, and values.

Severity	KPI Name	Value
Normal	CPU Utilization %	58.01
Normal	Disk I/O - Read Ops	3194.38
Normal	Disk I/O - Write Ops	2508.36
Normal	Disk Space Used %	71.71
Normal	Memory Used %	79.78
Normal	Network Throughput - Inbound	4.57
Normal	Network Throughput - Outbound	13.96

Below the table, there is a section for '0 Critical and High Episodes' with a 'View All' link. A message icon indicates 'No episodes found.'

Deep Dive Lab

This deep dive view is used to bring all the relevant data to run an efficient war room, we can add/remove swim lanes to make the visualization even more useful.

- ▶ Select the three swim lanes
- ▶ Bulk Actions > Delete



Deep Dive Lab

To understand the impact we need to add some business KPI to this deep dive, this will speed up investigations and diagnosis.

- ▶ Either navigate up the service tree or change focus to '*Buttercup Store*'
- ▶ Click + on the following KPIs;
 - Revenue
 - Revenue per Order
 - Successful Checkouts
- ▶ Move lanes as per image



Deep Dive Lab

To enable investigation into anomalous activity in your KPIs we can drill down on KPIs to gain deeper insights.

- ▶ Select 'Disk Space used %'
- ▶ Select the COG icon next to Disk Space used %
- ▶ Select Lane Overlay options
- ▶ Select Enable Overlays 'Yes'

The screenshot shows a Splunk dashboard with several KPI cards. The 'Disk Space Used %' KPI card is highlighted with a red circle around its settings icon. A context menu is open over this KPI, listing options: Edit Lane, Graph Rendering Options, Lane Overlay Options, Threshold Options, Edit KPI, Delete Lane, and Open in Search. The 'Lane Overlay Options' dialog box is also open, showing the following settings:

- Enable Overlays: **Yes** (circled in red)
- Overlay Type: Entity
- Graph Color: Automatic
- Overlay Selection Mode: Static

Selection	Entity_Title	Alert_Level	sparkline
<input checked="" type="checkbox"/>	mysql-01	Normal	
<input checked="" type="checkbox"/>	mysql-02	Normal	
<input checked="" type="checkbox"/>	mysql-03	Normal	
<input type="checkbox"/>	mysql-04	Normal	

Selected Entities

mysql-01	x
mysql-02	x
mysql-03	x

At the bottom of the dialog, the 'Save' button is circled in red.

Deep Dive Lab

- ▶ Hover over one of the lines from 'Disk Space Use %'. Notice the drill down possibility to the Splunk App for Infrastructure



Deep Dive Lab

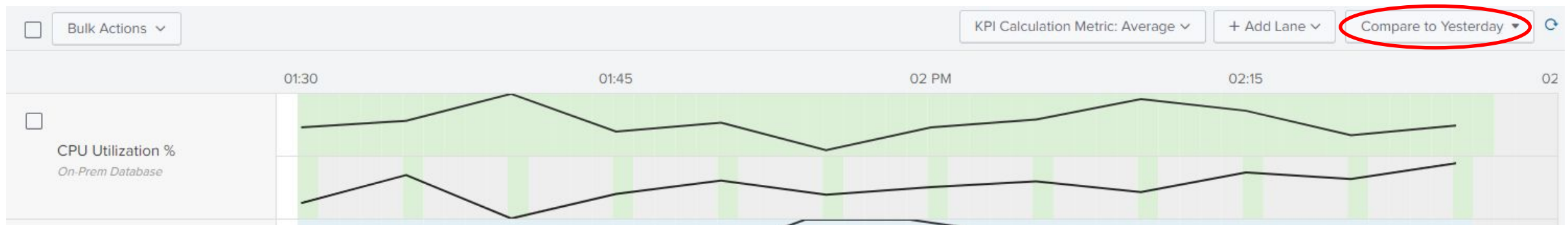
- ▶ Select 'Add Lane'
- ▶ Click 'Add Event Lane'
- ▶ Input 'Database Service Errors'
Title
- ▶ Event Search:
 - `'sourcetype="stream:mysql" status>200'`
- ▶ Click 'Create Lane'

The screenshot shows a Splunk dashboard configuration interface. At the top, there is a 'KPI Calculation Metric: Average' dropdown, a '+ Add Lane' button (circled in red), and a 'Compare to ...' dropdown. Below this, a time range from 10 AM to 10:30 is visible. A dropdown menu is open, showing three options: 'Add Metric Lane', 'Add KPI Lane', and 'Add Event Lane' (circled in red). Below the menu is the 'Add Event Lane' dialog box. It has a title field with 'Database Errors', a subtitle field with 'optional', a 'Graph Color' dropdown set to 'Automatic', and 'Lane Size' buttons for 'Small', 'Medium', and 'Large'. The 'Event Search' field contains the query `'sourcetype="stream:mysql" status>200'` (circled in red). Below the search field is a 'Run Search' button. At the bottom right of the dialog are 'Cancel' and 'Create Lane' buttons (circled in red).

Deep Dive Lab

▶ Extra

- Investigate blue event lane
- Compare to yesterday

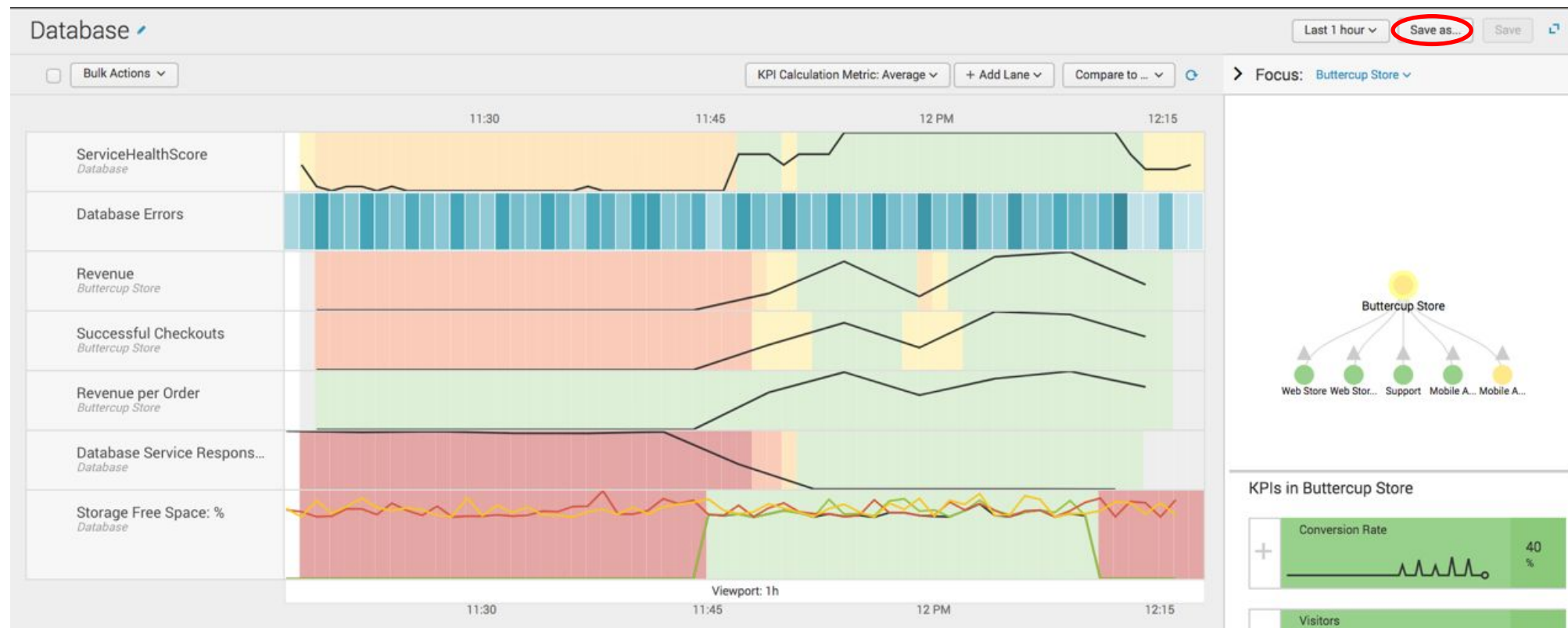


▶ *Note: adjust the Time-Picker to only show the last 60 minutes.*

Deep Dive Lab

Once you have finished investigating the Deep Dive dashboard

- ▶ make sure you click 'Save As'
- ▶ And save 'Database Deep Dive – <Your Initials>'



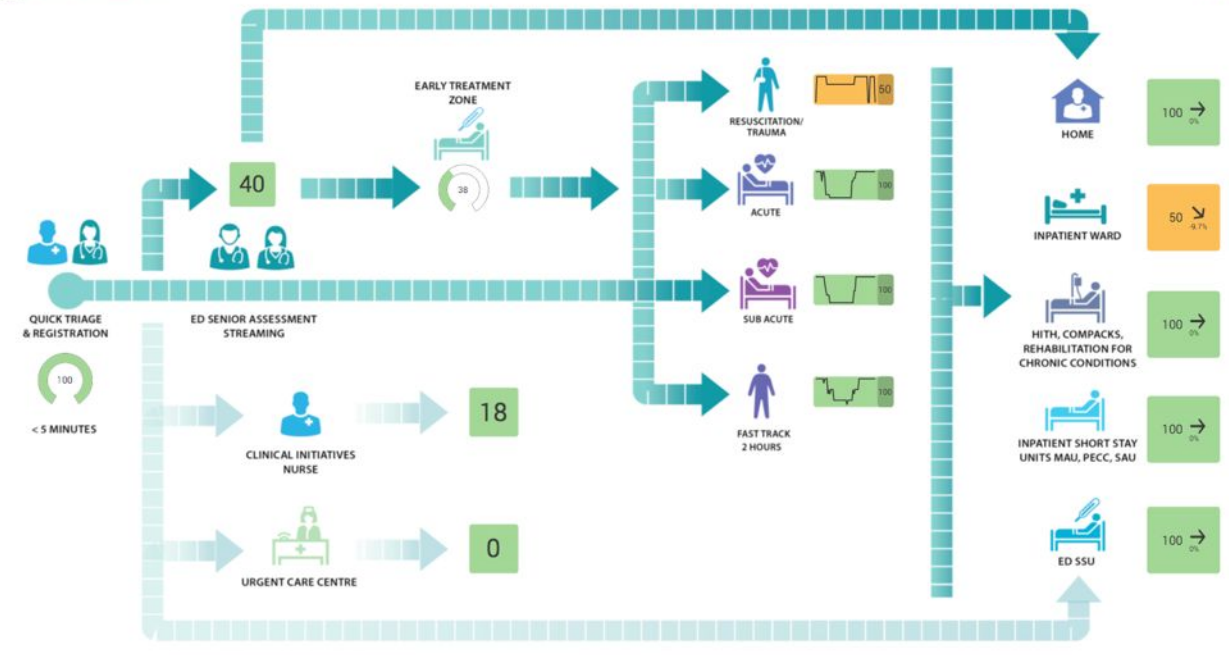
When to use Glass Tables

- ▶ Executive overview and business metrics
 - ▶ Highly complex and valuable services
 - ▶ Services that fail often or result in War Rooms
 - ▶ Services that have recurring outages
 - ▶ Main use case to stream-line root cause investigation
 - ▶ When you want to link to Splunk Enterprise or other tools
- ▶ *Note : It is best practice to import a background with most of your graphical design, and then drag KPIs onto the canvas.*

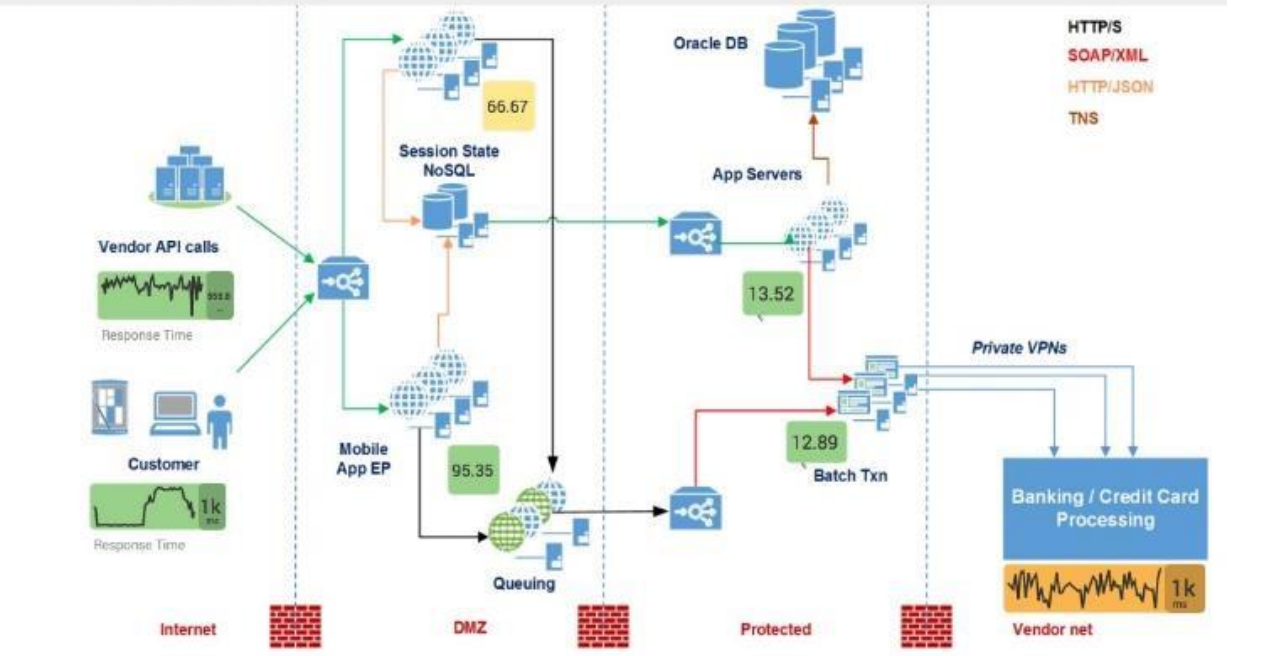
Current Operational Health



HEALTHCARE SERVICE INTELLIGENCE



On Line Transaction Service



National Park Visitor Services




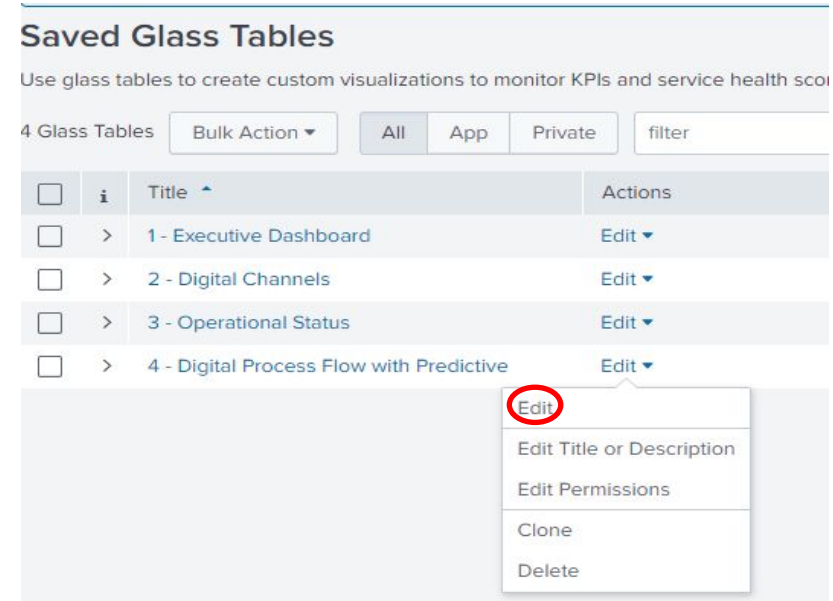
Glass Table Use Case

- ▶ The business leaders would like a high-level dashboard showing the key functions and services of the organisation.
- ▶ The objective of this exercise is to complete the existing IT operations dashboard (Digital Transaction Flow) with the new On-Prem Database service healthscore, including a drill down to a deep dive.
- ▶ Second part of this lab is to create a business focus dashboard;
 - Import your group logo
 - Include several KPIs that only relate to the business
 - Keep technical KPIs to a minimum
 - Link existing dashboard to one of the services

Glass Table Lab

- ▶ Select *Glass Table menu*
- ▶ Edit '4. Digital Transaction Flow'

- ▶ Click  icon to fit to page
- ▶ Note the tool pallet icons
- ▶ KPIs can be dragged onto canvas
- ▶ Configuration panel on right



Glass Table Lab

- ▶ Expand 'On-Prem Database'
- ▶ Drag 'ServiceHealthScore' onto the canvas

- ▶ Configure attributes;

- Label Box = Off
 - *Scroll down the dialog box*
- Drilldown = On
- Select 'Saved Deep Dive'
 - Select 'On-Prem Database DD'
- Change visualisation type
 - Single Value

- ▶ Click Update

The screenshot shows a dashboard titled "4 - Digital Process Flow with Predictive". The main canvas displays a process flow diagram with various components like "Web Store", "Manufacturing", "External APIs", "Web Front End", "Cart Management", "Order Management", "Product Catalog", "Mobile App", "Authorization", "Cloud Database", and "On-Prem Database". Each component has a health score indicator (e.g., 100, 11, 70, 99, 100, 100, 100, 70, 70, 471, 35, 70, 70).

On the left, a "Services" sidebar lists various services, with "ServiceHealthScore" under "On-Prem Database (10)" circled in red. A "filter" input is also visible.

On the right, a "Configurations" panel is open, showing settings for the selected KPI: "ServiceHealthScore". The "Label Box" is set to "On" (circled in red), and the "Label" is "ServiceHealthScore". A red arrow points to the "Label Box" setting. The "Update" button is highlighted in green.

At the bottom of the canvas, a "Legend" box is circled in red.

Glass Table Lab

▶ Move Database healthscore next to the Database icon (green box)

▶ On the right-hand panel

▶ Configure attributes;

- Width = 180

- Height = 180

▶ Click Update

▶ Click Save

The screenshot shows a digital process flow dashboard titled "4 - Digital Process Flow with Predictive". The dashboard displays a flowchart with various services and their health scores. The configuration panel on the right is open, showing the configuration for the "ServiceHealthScore" KPI. The "Width" and "Height" fields are both set to 180 and are circled in red. The "Label Box" and "Abbreviation" options are set to "On". The "Use KPI Summary" option is set to "Yes". The "Search" field contains the text "get_full_summary_kpi".

Services

- filter
- Manufacturing (1)
- > NTP (2)
- On-Prem Database (10)
 - ServiceHealthScore
 - CPU Utilization %
 - Database Queries
 - Database Response Time
 - Disk I/O - Read Ops
 - Disk I/O - Write Ops
 - Disk Space Used %
 - Memory Used %
 - Network Throughput - L...
 - Network Throughput - O...
- > Order Management (21)
- > Product Catalog (21)
- > Shared Database Environ...

Configurations

KPI: ServiceHealthScore
Service: On-Prem Database
[Edit KPI](#)

Position

Layer

Width

Height

Label Box On Off

Abbreviation? On Off

Digit

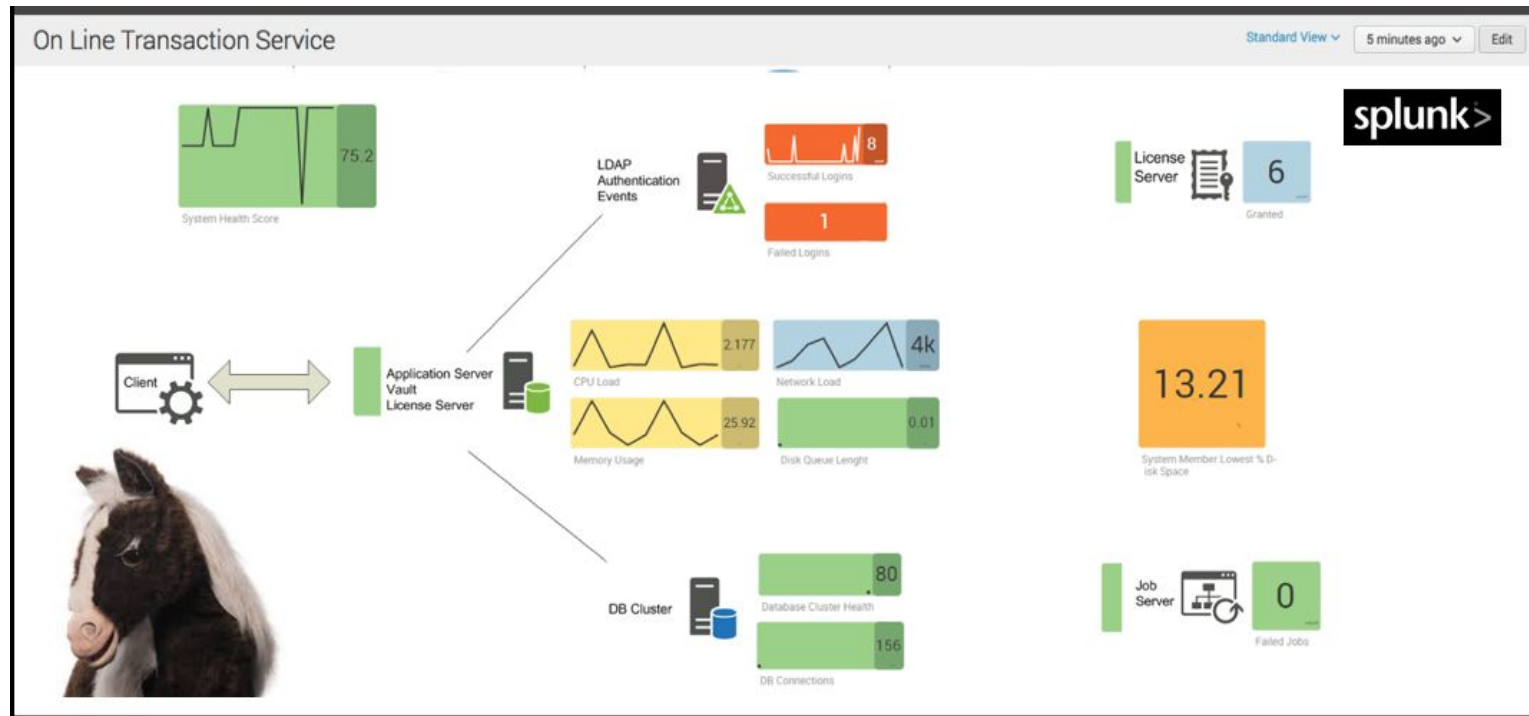
Precision

Use KPI Summary? Yes No

Search?

Glass Table Lab (Extra)

- ▶ Now it's your turn...you have 10 minutes
- ▶ Google and import your company logo
- ▶ Drop onto canvas;
 - Couple of icons
 - Link them
 - Business health scores
- ▶ Rename to reflect your business, be creative!



Machine Learning: Predictive Analytics

(or Imminent Outage Prediction)

What's Imminent Outage Prediction?

- ▶ Using historical data from KPIs for a service and some clever ML algorithms, you can sometimes **predict an outage** 20-30 minutes before it happens!
- ▶ Works best when a service has 5+ good KPIs and 1+ week of historical data
- ▶ The algorithm looks for recognizable/predictable KPI behavior, which comes before the service's aggregate health score changes.
 - For example: before the last outage, CPU usage went up AND garbage collection times increased AND session counts dropped...

Workshop Use Case

- ▶ The IT operations team are struggling to resolve issues with the company manufacturing service, typically outages are reported via customers contacting the service desk to complain.
- ▶ They would like to use machine learning to predict health score degradation 30 minutes before it causes a service outage.
- ▶ The objective of this lab will be to use the '**Manufacturing**' health score to build a predictive algorithm model to predict future issues.

Predictive Analytics Lab

We need to use machine learning to build a model for the Manufacturing service. This model will be used in the second part of this lab.

- ▶ Select '*configure*' menu
- ▶ Pick '*Services*' item
- ▶ Click edit '*Manufacturing*' service
- ▶ Select '*Edit*' menu

The screenshot shows the IT Service Intelligence interface. The top navigation bar includes 'Service Analyzer', 'Episode Review', 'Glass Tables', 'Deep Dives', 'Multi-KPI Alerts', 'Dashboards', 'Search', 'Configure', and 'Product Tour'. The 'Configure' menu is circled in red. Below the navigation bar, the 'Services' section is displayed. A table lists 10 services, including 'Manufacturing'. The 'Edit' dropdown menu for the 'Manufacturing' service is circled in red, and the 'Edit' option within that menu is highlighted.

	Name	Actions	Status	Service Template	Entity Rules	KPIs	Health	Team
<input type="checkbox"/>	> Authorization	Edit	Enabled	Not linked	4	14	View Health	Global
<input type="checkbox"/>	> Buttercup Store	Edit	Enabled	Not linked	0	21	View Health	Global
<input type="checkbox"/>	> Cart Management	Edit	Enabled	Synced with Cloud-Based Services	4	20	View Health	Global
<input type="checkbox"/>	> Cloud Databases	Edit	Enabled	Not linked	2	8	View Health	Global
<input type="checkbox"/>	> External Authentication Services	Edit	Enabled	Not linked	0	3	View Health	Global
<input type="checkbox"/>	> Manufacturing	Edit	Enabled	Not linked	1	7	View Health	Global
<input type="checkbox"/>	> Mobile App	Edit	Enabled	Not linked	0	3	View Health	Global
<input type="checkbox"/>	> Order Management	Edit	Enabled	Synced with Cloud-Based Services	3	20	View Health	Global
<input type="checkbox"/>	> Product Catalog	Edit	Enabled	Synced with Cloud-Based Services	3	20	View Health	Global
<input type="checkbox"/>	> Web Front End	Edit	Enabled	Not linked	4	12	View Health	Global

Predictive Analytics Lab

ITSI Predictive Analytics uses machine learning algorithms to predict the future health score of your service. This screen we will train and test different machine learning algorithms to determine which one will give the most accurate prediction.

- ▶ Select '*Predictive Analytics*'
 - ▶ Time = 14 Days
 - ▶ Algorithm Type = Regression
 - ▶ Algorithm = Linear Regression
 - ▶ Click 'Train' button
-
- ▶ Once the model has run, investigate below.
 - ▶ Click 'Save'

The screenshot shows the ITSI Predictive Analytics interface for a 'Manufacturing' service. The 'Predictive Analytics' tab is selected and circled in red. The 'Time Period' is set to 'Last 14 days', 'Algorithm Type' is 'Regression', and 'Algorithm' is 'Linear Regression', all circled in red. The 'Split for Training/Test' is 70/30, and the 'Train' button is circled in red. Below the settings is a line chart titled 'Service Health Score and KPIs over time' showing various metrics over a 24-hour period. The chart includes a legend with the following items: Manufacturing Availability, Manufacturing Cycle Time, Manufacturing Overall Equipment Effectiveness, Manufacturing Performance, Manufacturing Quality, Manufacturing ServiceHealthScore, Manufacturing Total Acceptable Units, and Manufacturing Total Units Produced. The chart shows a repeating pattern of peaks and troughs over time. At the bottom right, there are 'Cancel' and 'Save' buttons.

Predictive Analytics Lab

- ▶ Repeat the previous steps for the other two algorithms over 14-day period.
- ▶ Random Forest Regressor
- ▶ Click '*Train*' button
- ▶ Remember 'Save' button !

- ▶ Gradient Boosting Regressor
- ▶ Click '*Train*' button
- ▶ Remember 'Save' button !

Manufacturing / Service description

Entities KPIs Service Dependencies Settings **Predictive Analytics**

ITSI Predictive Analytics uses machine learning algorithms to predict the future health score of your service. You can train and test different machine learning algorithms to determine which one will give the most accurate prediction. Expand the INSTRUCTIONS section to get started.

> INSTRUCTIONS

Time Period Algorithm Type Algorithm

Model created. See Test a Model below for details.

- Linear Regression
- Random Forest Regressor
- Gradient Boosting Regressor

Service Health Score and KPIs over time

100
40
90
1

2:00 PM Mon Apr 6 2020 4:00 PM 6:00 PM 8:00 PM 10:00 PM 12:00 AM Tue Apr 7 2:00 AM 4:00 AM 6:00 AM 8:00 AM 10:00 AM 12:00 PM

Manufacturing: Availability
Manufacturing: Cycle Time
Manufacturing: On-time Effectiveness
Manufacturing: Performance
Manufacturing: Quality
Manufacturing: ServiceHealthScore
Manufacturing: Total Acceptable Units
Manufacturing: Total Units Produced

Predictive Analytics Lab

In this lab we are going to review the predictive analytics value for the **Manufacturing** service using the recommended model.

- ▶ Select *Dashboards > Predictive Analytics*
- ▶ Select the 'Manufacturing' service
- ▶ Select the recommended algorithm model

Predictive Analytics

ITSI Predictive Analytics uses machine learning to predict the health score value of a selected service. The models use historical KPI and service health score data to approximate what a service's health might look like in 30 minutes. [Learn more](#)

Service ? Model ?

Manufacturing RandomForestRegressor

Predicted Service Health Score in 30 Minutes

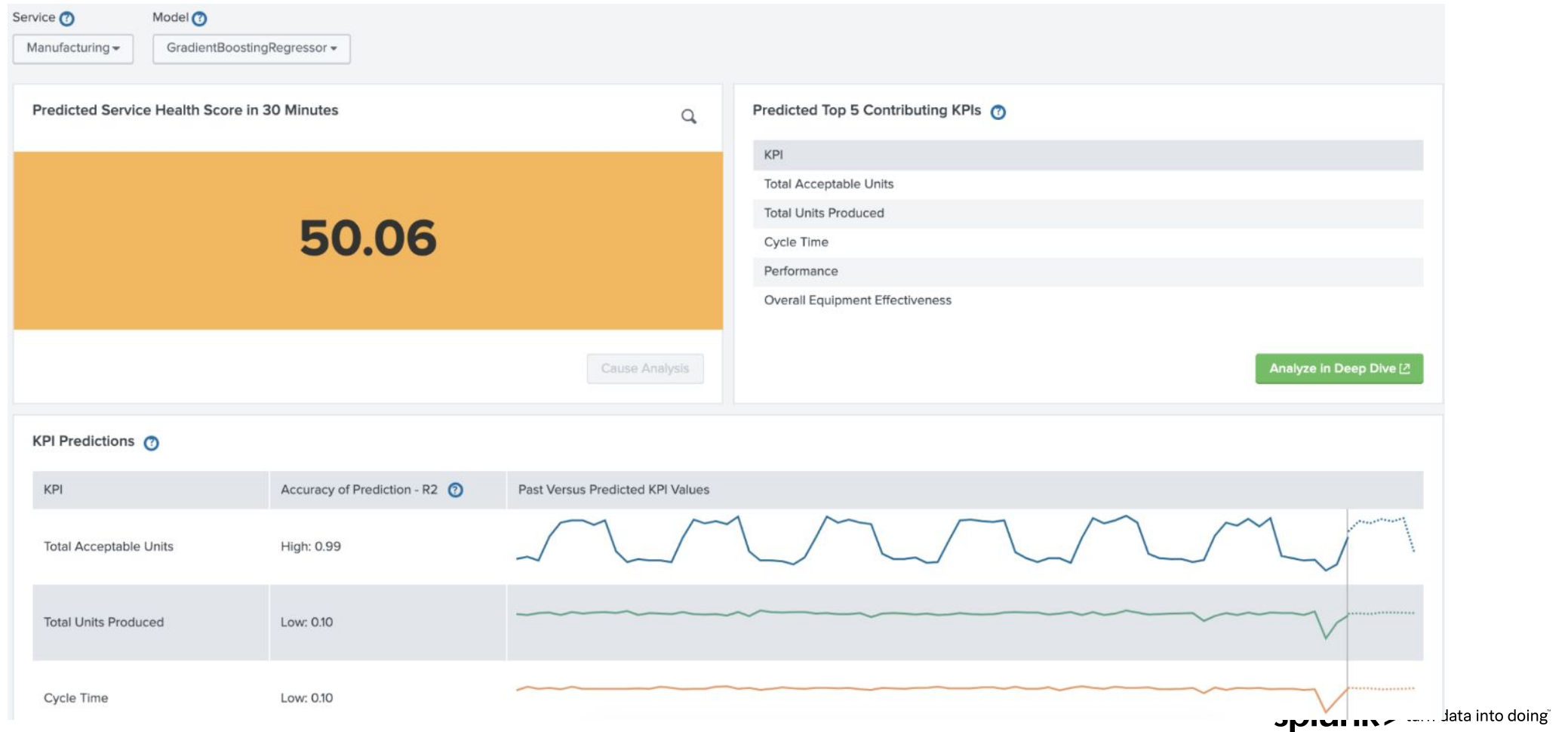
50.00

Cause Analysis

Predictive Analytics Lab

Once we have selected a model ITSI will calculate the future healthscore

- ▶ Click 'Cause Analysis' button to review the suggested KPIs



Predictive Analytics Lab

- ▶ Click the spyglass to review the SPL
- ▶ This SPL is already being used in our glass table

The screenshot displays the Splunk Predictive Analytics interface. At the top, the 'Service' is set to 'Manufacturing' and the 'Model' is 'GradientBoostingRegressor'. A search bar contains the SPL: ``itsi_predict_one_number(4bf1f146-3b89-4ae7-b8f3-32f536357bc4,health_score,app :itsi_predict_4bf1f146_3b89_4ae7_b8f3_32f536357bc4_GradientBoostingRegressor_041e77dd3c5e000bee811489_1585923875029)``. Below the search bar, a table shows the results of the search, with one event displayed: `health_score: 48.70154986843101` and `_time: 2020-04-03 14:50:00`. To the right, a 'Predicted Top 5 Contributing KPIs' section lists 'Total Acceptable Units' and 'Total Units Produced'. At the bottom, a visualization shows two line graphs: 'Total Units Produced' (green line) and 'Cycle Time' (orange line), both with a 'Low: 0.10' threshold indicated by a vertical dashed line.

Predictive Analytics Lab

- ▶ Select 'Glass Tables > Digital Transaction Flow with Predictive'
- ▶ Click 'Edit' button
- ▶ Review the 'Database Future Health-Score attributes'

The screenshot displays the Splunk interface for '4 - Digital Process Flow with Predictive'. The main visualization is a flow diagram showing the following components and their health scores:

- Web Store: Revenue 3k, Conversion Rate 31%
- Manufacturing: Current 100, Health 50 (circled in red)
- Mobile App: Revenue 1k, Conversion Rate 28%
- External APIs: Health 100
- Web Front End: Health 100
- Mobile App: Health 100
- Cart Management: Health 100
- Order Management: Health 100
- Product Catalog: Health 100
- Authorization: Health 100
- Cloud Databases: Health 100
- On-Prem Databases: Health 100

The 'Configurations' panel on the right shows the following settings:

- Ad hoc Search
- Search Type: Ad hoc, Data Model
- Search: `itsi_predict_one_number(4bf1f146-3b89-4ae7-b8f3-22f536357bc4,health_score,app:itsi_predict_4bff1f146_3b89_4ae7_b8f3_32f536357bc4_GradientBoostingRegressor_a4eccbb2904ed344cd69760e_1565717593771)` (circled in red)
- Run Search
- Earliest Time: 60 minutes ago
- Threshold Field: health_score
- Thresholds: On, Off

Event Analytics Lab

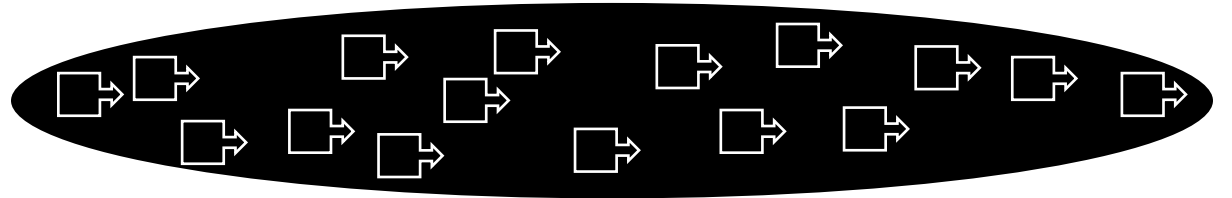
- ▶ The database team has expressed frustration with alerts originating from Nagios. The high volume of alerts is leading to alert fatigue and they lack the contextual information necessary to make them actionable.
- ▶ While the plan is to consolidate monitoring tools, they have asked if we can provide immediate relief using ITSI to group events together and reduce noise.
- ▶ Also, with hundreds of database instances to manage, tracking which alerts are associated to critical systems vs non-critical systems is tribal knowledge for the database team. They love the service tree view in ITSI and asked if it's possible to see the services affected by an alert.
- ▶ Interestingly enough, you heard the same challenges expressed by the web team who uses New Relic to monitor the application code.

Event Analytics Lab

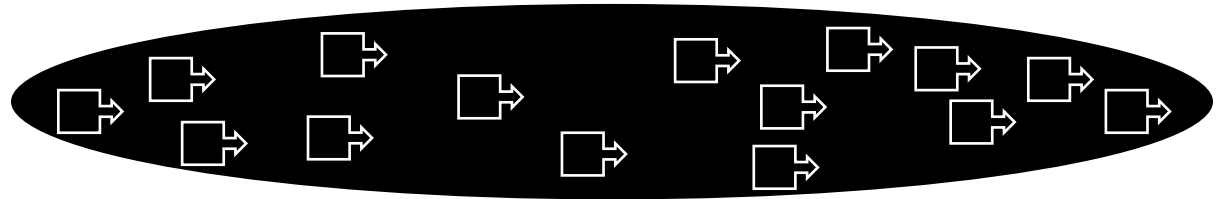
- ▶ Often, each team or layer of the stack has their own monitoring tools producing their own alerts. Each tool creating a silo of information that other teams don't get insight.

**Silo
Views**

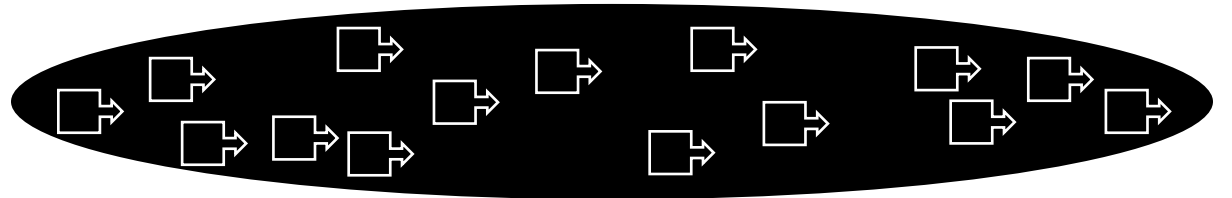
Applications



Servers



Databases



Event Analytics Lab

- ▶ If we can cluster events by time, we can immediately reduce noise. The two database events in orange happened around the same time and therefore, may very well be related to the same incident



Applications



Servers



Databases



Event Analytics Lab

- ▶ The three events in green occurred later after a pause in the flow of events. Probably a different issue all together. So grouping events together by time is a very powerful noise reduction technique.

Silo Views

Applications



Servers



Databases



Event Analytics Lab

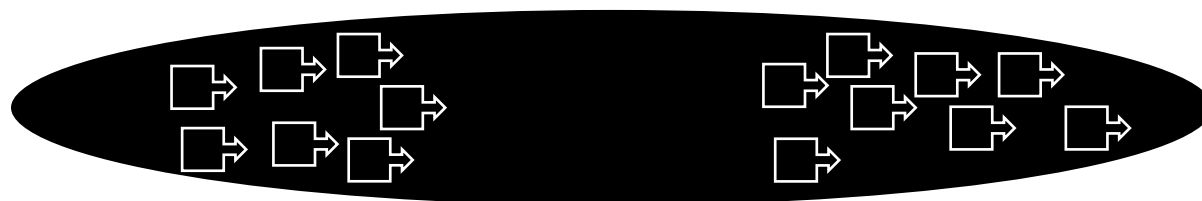
- ▶ We can extend the power of grouping beyond just time to further reduce noise. What if all of the events in orange we associated to the same database instance. Same timeframe... Same instance... that's probably all a related incident.

**Silo
Views**

Applications



Servers



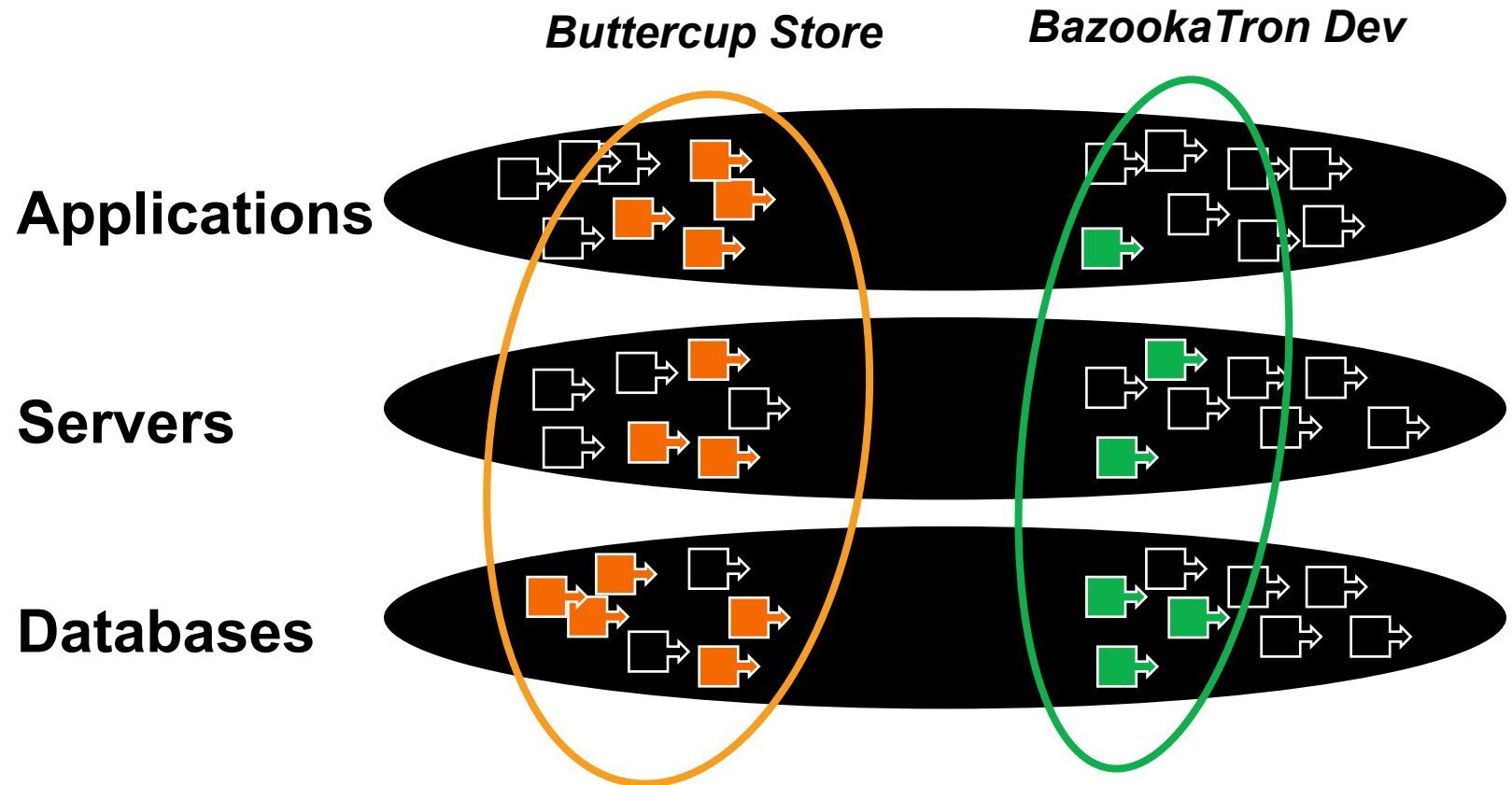
Databases



Event Analytics Lab

- ▶ We can extend the grouping across siloed monitoring tools, and across layers of the stack. What if I told you that all the events in orange were associated with machines that run the Buttercup Store.

**Silo
Views**



A quick terminology check

- ▶ **Alert** - Describes a state change for a target entity
 - Examples of different alerts:: Server42 is down, Filesystem is full
- ▶ **Alarm** - Specific alert for a target entity, can change severity/state over time
 - Example of single alarm: Server42 is “down”, then later “up”
- ▶ **Time-series data or Events**- The stuff that Splunk indexes
 - Includes traditional alerts & alarms, as well as logged data, metrics, wire data and more
- ▶ **Notable Event** - An actionable message (Splunk ITSI & Splunk ES)
 - Intended specifically for humans in Operations
- ▶ **Episode** - a group of Notable Events
- ▶ **Incident** - Unplanned interruption of an IT or business service
 - ServiceNow, Remedy

Event Analytics Lab

In this exercise we will group the database teams Nagios events together based on time and associate them to a service

Clean and prepare “raw” alert events

- SPL

Create Notable Events from alerts

- Correlation Search

Apply Service Context & Configure Event Grouping

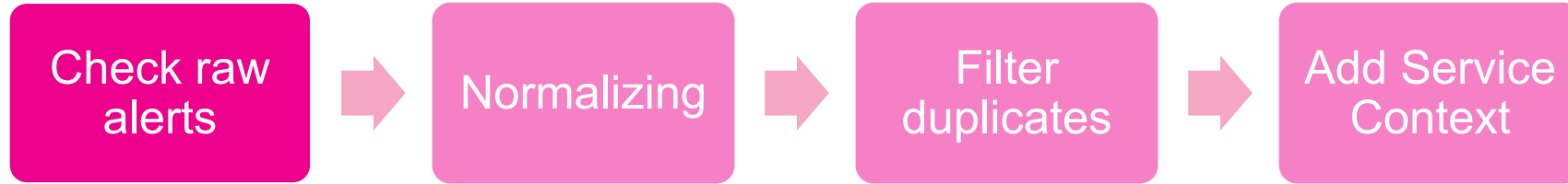
- Notable Event Aggregation Policies

Review episodes

i	Time	Event
>	09/04/2020 11:49:52.652	2020-04-09 11:49:52.652510 src_host="mysql-02" omd_site="SJC" perfdata="SERVICEPERFDATA" name="check_disk" severity="OK" attempt="1" statetype="SOFT" executiontime="0.0" latency="0.0" reason="Disk Space utilization 51.18 is below threshold" results="Disk Space status ok" host= mysql-02 source = nagios sourcetype = nagios
>	09/04/2020 11:48:52.592	2020-04-09 11:48:52.592363 src_host="mysql-02" omd_site="SJC" perfdata="SERVICEPERFDATA" name="check_disk" severity="WARNING" attempt="3" statetype="HARD" executiontime="0.0" latency="0.0" reason="Disk Space utilization 96.3 is above threshold" results="Disk Space status warn" host= mysql-02 source = nagios sourcetype = nagios
>	09/04/2020 11:47:52.527	2020-04-09 11:47:52.527797 src_host="mysql-02" omd_site="SJC" perfdata="SERVICEPERFDATA" name="check_disk" severity="WARNING" attempt="1" statetype="SOFT" executiontime="0.0" latency="0.0" reason="Disk Space utilization 93.89 is above threshold" results="Disk Space status warn" host= mysql-02 source = nagios sourcetype = nagios

< Prev 1 2 3 4 5 6 7 8 9 10 Next >

EA Lab Step 1 : Clean and prepare “raw” alert events



| `index=itsidemo sourcetype=nagios perfdatas=SERVICEPERFDATA`

Service Analyzer | Episode Review | Close Tables | Deep Dives | Multi-KPI Alerts | **Dashboards** | Search | Configure | Product Tour | IT Service Intelligence

S4N ITSI - Adding Nagios Events into ITSI

- Event Analytics Audit
- Event Analytics Monitoring
- Predictive Analytics
- ITSI Health Check
- S4N ITSI - Adding Nagios Events into ITSI

Step 1 - Raw Nagios Alerts

The first step to helping the database team achieve their goal is to ingest the raw alert events in. Prior to the workshop, we took the time to onboard the Nagios alerts the extracted fields.

SPL

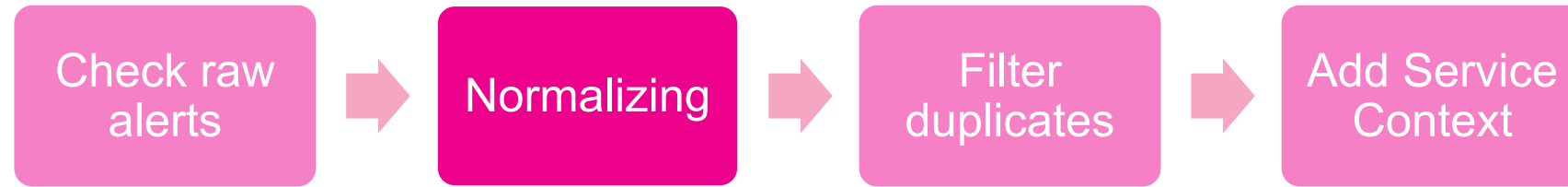
```
index=itsidemo sourcetype=nagios perfdatas=SERVICEPERFDATA
```

i	Time	Event
>	09/04/2020 11:49:52.652	2020-04-09 11:49:52.652510 src_host="mysql-02" omd_site="SJC" perfdatas="SERVICEPERFDATA" name="check_disk" severity="OK" attempt="1" statetype="SOFT" executiontime="0.0" latency="0.0" reason="Disk Space utilization 51.18 is below threshold" results="Disk Space status ok" host = mysql-02 source = nagios sourcetype = nagios
>	09/04/2020 11:48:52.592	2020-04-09 11:48:52.592363 src_host="mysql-02" omd_site="SJC" perfdatas="SERVICEPERFDATA" name="check_disk" severity="WARNING" attempt="3" statetype="HARD" executiontime="0.0" latency="0.0" reason="Disk Space utilization 96.3 is above threshold" results="Disk Space status warn" host = mysql-02 source = nagios sourcetype = nagios
>	09/04/2020 11:47:52.527	2020-04-09 11:47:52.527797 src_host="mysql-02" omd_site="SJC" perfdatas="SERVICEPERFDATA" name="check_disk" severity="WARNING" attempt="1" statetype="SOFT" executiontime="0.0" latency="0.0" reason="Disk Space utilization 93.89 is above threshold" results="Disk Space status warn" host = mysql-02 source = nagios sourcetype = nagios

< Prev 1 2 3 4 5 6 7 8 9 10 Next >

After you have finished reviewing the raw Nagios events. **Click here** to proceed to Step 2 - Add Normalized Fields

EA Lab Step 2 : Add Normalized Fields



Goal: Normalize the data to make it possible to correlate data from different

SOURCES

```

| eval norm_severity=case(severity=="CRITICAL",6,severity=="WARNING",4, severity="OK", 2)
| eval norm_instance= src_host
| eval norm_test=name
  
```

Step 2 - Add Normalized Fields

While each monitoring tool will express events differently, they all communicate the same fundamental information. Such as, how severe is the event? To which machine is the event associated? What type of check or test was performed? To facilitate the grouping of multiple events from multiple monitoring tools, we must normalize this key information so that a common set of field names and values is used. The SPL below creates these normalized severity, instance, and test fields.

SPL

```

index=itsidememo sourcetype=nagios perfdata=SERVICEPERFDATA
| eval norm_severity=case(severity=="CRITICAL",6,severity=="WARNING",4, severity="OK", 2)
| eval norm_instance=src_host
| eval norm_test=name
  
```

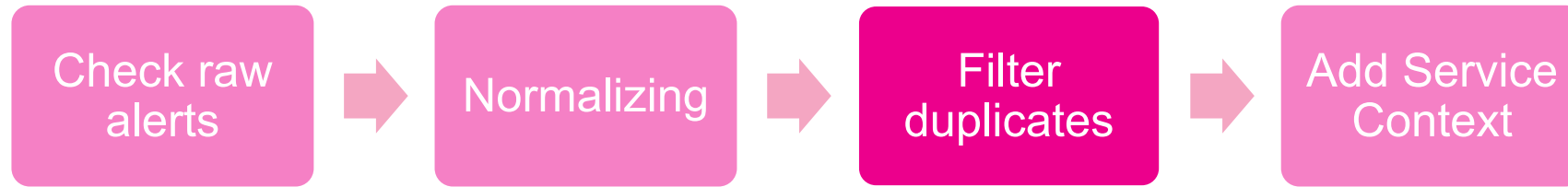
_time	name	severity	norm_severity	norm_instance	norm_test	total
2020-04-15 10:02:27.773	check_disk	OK	2	mysql-02	check_disk	1
2020-04-15 10:01:27.710	check_disk	WARNING	4	mysql-02	check_disk	1
2020-04-15 09:56:27.396	check_disk	OK	2	mysql-02	check_disk	1
2020-04-15 09:55:27.334	check_disk	WARNING	4	mysql-02	check_disk	1
2020-04-15 09:51:27.088	check_disk	OK	2	mysql-02	check_disk	1

594 157

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

After you have finished reviewing the new normalized fields, click here to proceed to Step 3 - Deduplicate events

EA Lab Step 3 : Deduplicate events



Goal: Removing duplicated events

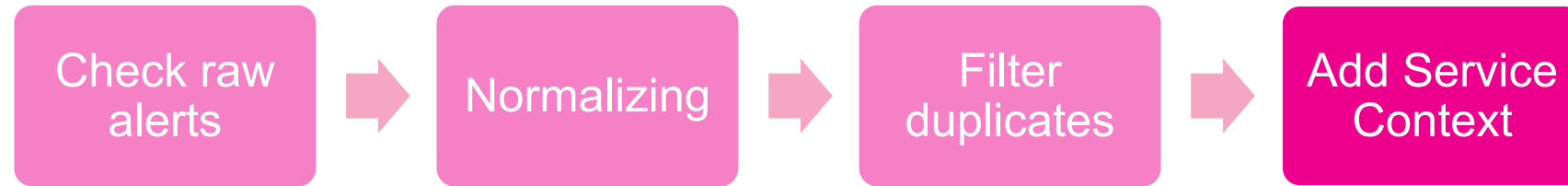
`| dedup consecutive=true src_host severity name`

_time ↕	name ↕	norm_instance ↕	severity ↕	norm_severity ↕	total ↕
2020-04-15 10:02:27.773	check_disk	mysql-02	OK	2	1
2020-04-15 10:01:27.710	check_disk	mysql-02	WARNING	4	1
2020-04-15 09:56:27.396	check_disk	mysql-02	OK	2	1
2020-04-15 09:55:27.334	check_disk	mysql-02	WARNING	4	1
2020-04-15 09:51:27.088	check_disk	mysql-02	OK	2	1
				102	34

« Prev 1 2 3 4 5 6 7 Next »

Finally, after you have finished reviewing the deduplicated events, click here to proceed to Step 4 - Add Service Context

EA Lab Step 4 - Add Service Context



Goal: Add Service Context makes correlation possible for different alerts in a service

```

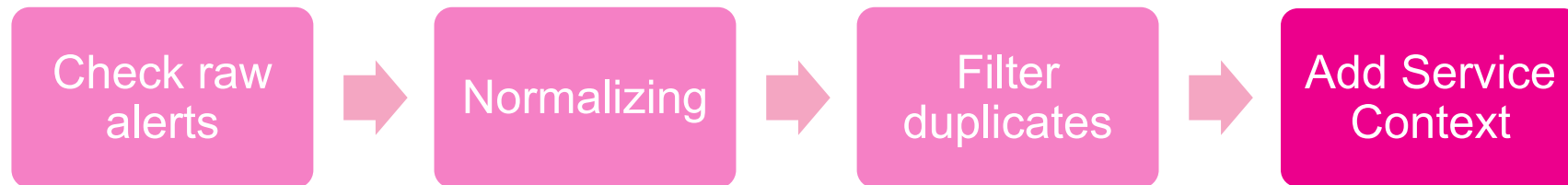
| `apply_entity_lookup(host)`
| `get_service_name(serviceid,service_name)`
  
```

▶ Click on the magnifying glass

_time ↕	name ↕	norm_instance ↕	severity ↕	norm_severity ↕	service_name ↕
2020-04-15 10:02:27.773	check_disk	mysql-02	OK	2	On-Prem Database
2020-04-15 10:01:27.710	check_disk	mysql-02	WARNING	4	On-Prem Database
2020-04-15 09:56:27.396	check_disk	mysql-02	OK	2	On-Prem Database
2020-04-15 09:55:27.334	check_disk	mysql-02	WARNING	4	On-Prem Database
2020-04-15 09:51:27.088	check_disk	mysql-02	OK	2	On-Prem Database

< Prev 1 Open in Search 6 7 Next >

🔍 ⬇️ ⓘ 🔄 a minute ago



▶ Select the SPL Query and copy to clipboard, we will need it in the next chapter

New Search

```
index=itsidemo sourcetype=nagios perfdata=SERVICEPERFDATA
| eval norm_severity=case(severity=="CRITICAL",6,severity=="WARNING",4, severity="OK", 2)
| eval norm_instance= src_host
| eval norm_test=name
| dedup consecutive=true src_host severity name
| eval entity_title=norm_instance
| `apply_entity_lookup(host)`
| `get_service_name(serviceid,service_name)`
| table _time, name, norm_instance, severity, norm_severity, service_name
```

✓ 34 events (14/04/2020 15:00:00.000 to 15/04/2020 15:27:32.000) No Event Sampling

Events Patterns **Statistics (34)** Visualization

20 Per Page Format Preview

_time	name	norm_instance	severity	norm_severity	service_name
2020-04-15 10:02:27.773	check_disk	mysql-02	OK	2	On-Prem Database
2020-04-15 10:01:27.710	check_disk	mysql-02	WARNING	4	On-Prem Database
2020-04-15 09:56:27.396	check_disk	mysql-02	OK	2	On-Prem Database
2020-04-15 09:55:27.334	check_disk	mysql-02	WARNING	4	On-Prem Database

Event Analytics Lab

In this exercise we will group the database teams Nagios events together based on time and associate them to a service

Clean and prepare “raw” alert events

- SPL

Create Notable Events from alerts

- Correlation Search

Apply Service Context & Configure Event Grouping

- Notable Event Aggregation Policies

Review episodes

Search Properties

Search Name ^{*}

Description [?]

Search Type Data Model Ad hoc

Search ^{*}

```
index=itsidemo sourcetype=nagios perfddata=SERVICEPERFDATA
| eval
norm_severity=case(severity=="CRITICAL",6,severity=="WARNING",
4, severity="OK", 2)
| eval norm_instance= src_host
| eval norm_test=name
| dedup consecutive=true src_host severity name
| eval entity_title=norm_instance
| `apply_entity_lookup(host)`
`get_service_name(serviceid,service_name)
| table _time, name, norm_instance, severity, norm_severity,
service_name
```

Run Search [🔗](#)

Time range

Association

Service

Entity Lookup Field [?]

Schedule

Event Analytics Lab

- ▶ Navigate to Configure -> Correlation Searches
- ▶ Create New Search -> Create Correlation Search

The screenshot displays the Splunk IT Service Intelligence (ITSI) interface. The top navigation bar includes links for Service Analyzer, Episode Review, Glass Tables, Deep Dives, Multi-KPI Alerts, Dashboards, Search, **Configure**, and Product Tour. The **Configure** menu is open, showing a list of options: Services, Entities, Service Templates, **Correlation Searches** (highlighted with a red circle), KPI Base Searches, KPI Threshold Templates, Backup/Restore, Maintenance Windows, Notable Event Aggregation Policies, Hybrid Action Dispatching, and Teams. On the right side of the interface, there is a green **Create New Search** button (also highlighted with a red circle) and an 'Explore Content' button. Below the navigation bar, the 'Correlation Searches' section is visible, featuring a table with columns for Bulk Action, filter, Title, and Actions. The table lists several correlation searches, such as 'Active Directory', 'Bidirectional Ticketing', and various 'Episode Monitoring' searches. A pagination control shows '1' of 2 pages.

Bulk Action	filter	Title	Actions
<input type="checkbox"/>		> Active Directory	Edit
<input type="checkbox"/>		> Bidirectional Ticketing	Edit
<input type="checkbox"/>		> Episode Monitoring - All Services and KPIs Return to Normal	Edit
<input type="checkbox"/>		> Episode Monitoring - Concentration of High and Critical Notable Ev...	Edit
<input type="checkbox"/>		> Episode Monitoring - Critical Notable Event added to Episode (Rec...	Edit
<input type="checkbox"/>		> Episode Monitoring - Episode Risk Well Above Historical Average	Edit

Event Analytics Lab: correlation search

▶ Name your search

▶ *Paste the SPL in search:*

```
index=itsidemo sourcetype=nagios perfddata=SERVICEPERFDATA
| eval norm_severity=case(severity=="CRITICAL",6,severity=="WARNING",4, severity="OK", 2)
| eval norm_instance= src_host
| eval norm_test=name
| dedup consecutive=true src_host severity name
| eval entity_title=norm_instance
| `apply_entity_lookup(host)`
| `get_service_name(serviceid,service_name)`
| table _time, name, norm_instance, severity, norm_severity, service_name
```

▶ *Time range: Last 5 minutes (select 'relative' in time picker)*

▶ *Run Every: 5 minutes*

▶ *Entity Lookup Field: host to link with the Service Context*

▶ *Scroll down*

Search Properties

Search Name ^{*} Nagios Correlation Search

Description [?] optional

Search Type Data Model Ad hoc

Search ^{*}

```
index=itsidemo sourcetype=nagios perfddata=SERVICEPERFDATA
| eval
norm_severity=case(severity=="CRITICAL",6,severity=="WARNING",
,4, severity="OK", 2)
| eval norm_instance= src_host
| eval norm_test=name
| dedup consecutive=true src_host severity name
| eval entity_title=norm_instance
| `apply_entity_lookup(host)`
| `get_service_name(serviceid,service_name)`
| table _time, name, norm_instance, severity, norm_severity,
service_name
```

Run Search [↗](#)

Time range Last 5 minutes ▼

Association

Service Select service(s)

Entity Lookup Field [?] host

Schedule

Event Analytics Lab: correlation search

- ▶ *Populate Notable Event Title*
Nagios alert from %norm_instance%
- ▶ *Populate Notable Event Desc.*
Nagios alert from %norm_instance%. %norm_test (%severity%)
- ▶ *Severity: Advanced Mode*
- ▶ *Severity: %norm_severity%*
- ▶ *Save*

Notable Events

Notable Event Title ? Nagios alert from %norm_instance%

Notable Event Description ? Nagios alert from %norm_instance%. %norm_test (%severity%)

Owner ? unassigned ▼ Advanced Mode
In advanced mode, use tokens like %fieldname% to use result field values to set owner.

Severity ? %norm_severity% Simple Mode
In advanced mode, use tokens like %fieldname% to use result field values to set severity.

Status ? New ▼ Advanced Mode
In advanced mode, use tokens like %fieldname% to use result field values to set status.

Drilldown Search Name ?

Drilldown Search ?

Drilldown earliest offset ? Last 5 minutes ▼

Drilldown latest offset ? Next 5 minutes ▼

Notable Event Identifier Fields ? source
Set of fields used together to determine if a notable event is unique or not.

Drilldown Website Name ?

Drilldown Website URL ?

> Advanced Options

Cancel Save

Policies

In this exercise we will group the database teams Nagios events together based on time and associate them to a service

Clean and prepare “raw” alert events

- SPL

Create Notable Events from alerts

- Correlation Search

Apply Service Context & Configure Event Grouping

- Notable Event Aggregation Policies

Review episodes

The screenshot shows the configuration interface for a 'Service Issues' policy. It includes sections for 'Filtering Criteria' and 'Break episode?'. The 'Filtering Criteria' section has two rules: 'severity greater than Normal' and 'service_name matches *'. The 'Break episode?' section has two conditions: 'If this episode existed for 36000 second(s)' and 'If the flow of events into the episode paused for 3600 second(s)'. There are also sections for 'Smart Mode grouping' and 'Split events by field?' with 'service_name' selected.

Service Issues [/](#)
Notable Event Aggregation Policy description [/](#)

Filtering Criteria Action Rules

Filtering Criteria
Create filtering criteria to group notable events into episodes.

▼ Include the events if?

severity greater than ▼ Normal ×

service_name matches ▼ * ×

+ Add Rule (AND)

+ Add Rule (OR)

> Smart Mode grouping

▼ Split events by field?

Split events into multiple episodes by

service_name ×

▼ Break episode?

> If this episode existed for 36000 second(s) ×

> If the flow of events into the episode paused for 3600 second(s) ×

+ Add Breaking Condition (OR)

> Episode information

Event Analytics Lab: Notable Event Aggregation Policies

- ▶ Navigate to Configure -> Notable Event Aggregation Policies
- ▶ Edit "Service Issues" policy

The screenshot shows the Splunk Enterprise interface for configuring Notable Event Aggregation Policies. The page title is "Notable Event Aggregation Policies" and it includes a subtitle: "Use notable event aggregation policies to group similar notable events in the Episode Review." There are 11 policies listed in a table, each with a checkbox, a title, an "Edit" link, and a status toggle. The "Service Issues" policy is selected, and its "Edit" dropdown menu is open, showing options: "Edit", "Edit Title or Description", "Edit Permissions", "Clone", and "Delete". The "Edit" option is circled in red.

<input type="checkbox"/>	i	Title ^	Actions	Status
<input type="checkbox"/>	>	Application Alerts	Edit ▼	Enabled
<input type="checkbox"/>	>	Default Policy	Edit ▼	Enabled
<input type="checkbox"/>	>	Default SNMP Policy	Edit ▼	Disabled
<input type="checkbox"/>	>	Episodes by Alert Group	Edit ▼	Disabled
<input type="checkbox"/>	>	Episodes by ITSI Service	Edit ▼	Disabled
<input type="checkbox"/>	>	Infrastructure Alerts	Edit ▼	Enabled
<input type="checkbox"/>	>	KPI Alerting Policy	Edit ▼	Enabled
<input type="checkbox"/>	>	Multi-Episode Problem	Edit ▼	Disabled
<input type="checkbox"/>	>	Normalized Policy (Splunk App for Infrastructure)	Edit ▼	Enabled
<input type="checkbox"/>	>	Service Issues	Edit ▼	Enabled
<input type="checkbox"/>	>	User Account Management	Edit ▼	Enabled

Event Analytics Lab: Notable Event Aggregation Policies

- ▶ Review “Include the events if” configuration
- ▶ Review “Split events by field” configuration
- ▶ Review “Break episode” configuration
- ▶ Modify the “Break episode” configuration
 - If the flow of events paused for 3600 seconds

The screenshot shows the configuration interface for a 'Service Issues' policy. It is divided into several sections:

- Service Issues**: The main title of the policy.
- Filtering Criteria**: A section with a description 'Create filtering criteria to group notable events into episodes.' It contains a dropdown 'Include the events if?' with two rules:
 - severity greater than Normal
 - service_nam matches *Buttons for '+ Add Rule (AND)' and '+ Add Rule (OR)' are present.
- Smart Mode grouping**: A section with a dropdown 'Split events by field?' containing 'service_name'.
- Break episode?**: A section with two conditions:
 - If this episode existed for 36000 second(s)
 - If the flow of events into the episode paused for 3600 second(s)Buttons for '+ Add Breaking Condition (OR)' are present.
- Episode information**: A section at the bottom of the configuration.

Event Analytics Lab: Notable Event Aggregation Policies

- ▶ You can see in the preview results how ITSI is now grouping events together based on your configurations.

▶ Preview Results

Service Issues [Notable Event Aggregation Policy description](#)

Filtering Criteria Action Rules

Filtering Criteria
Create filtering criteria to group notable events into episodes.

▼ Include the events if?

- severity greater than Normal
- service_name matches *

+ Add Rule (AND)
+ Add Rule (OR)

> Smart Mode grouping

▼ Split events by field?

Split events into multiple episodes by
service_name

▼ Break episode?

- > If this episode existed for 36000 second(s)
- > If the flow of events into the episode paused for 3600 second(s)

+ Add Breaking Condition (OR)

> Episode Information

Preview with the Last 24 hours

i	Count	Title	Description	Severity	Owner	Status
>	13	Web Front End issue	Possible issue with Web Front End or upstream service	Medium	unassigned	New
>	140	Web Front End issue	Possible issue with Web Front End or upstream service	Medium	unassigned	New
>	2	On-Prem Database issue	Possible issue with On-Prem Database or upstream service	Low	unassigned	New
>	50	Web Front End issue	Possible issue with Web Front End or upstream service	Medium	unassigned	New
>	151	Authorization issue	Possible issue with Authorization or upstream service	Medium	unassigned	New
>	15	Authorization issue	Possible issue with Authorization or upstream service	Medium	unassigned	New
>	2	On-Prem Database issue	Possible issue with On-Prem Database or upstream service	Low	unassigned	New
>	2	Authorization issue	Possible issue with Authorization or upstream service	Medium	unassigned	New
>	1	On-Prem Database issue	Possible issue with On-Prem Database or upstream service	Critical	unassigned	New
>	61	Authorization issue	Possible issue with Authorization or upstream service	Medium	unassigned	New

Preview results

Cancel Save

▶ Click Cancel

Event Analytics Lab

In this exercise we will group the database teams Nagios events together based on time and associate them to a service

Clean and prepare “raw” alert events

- SPL

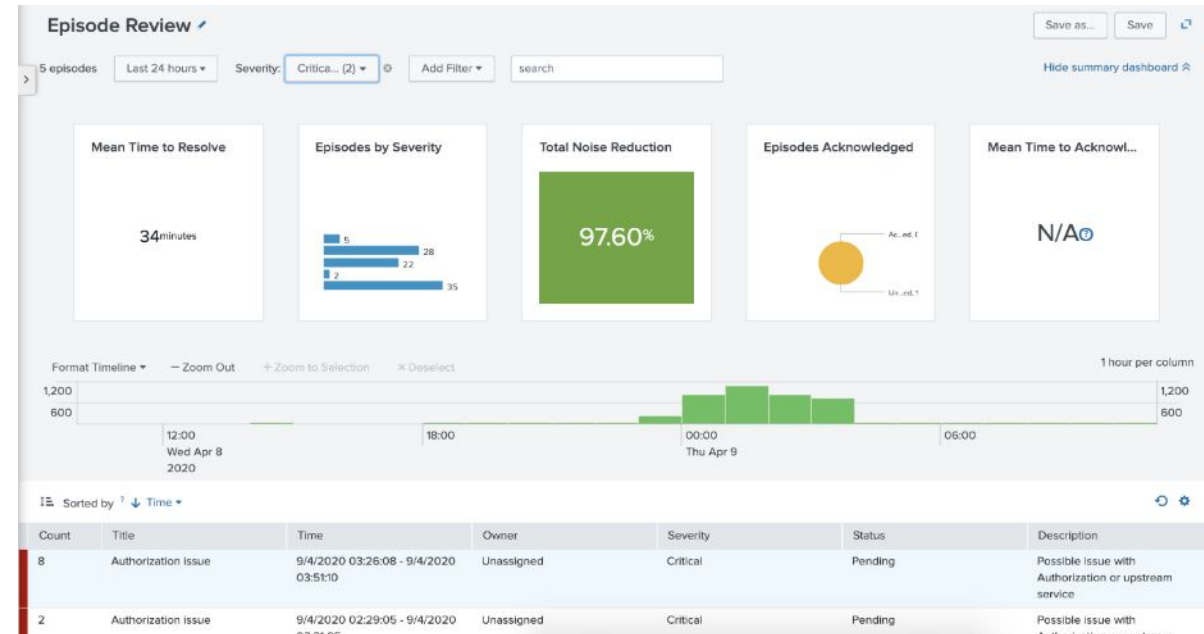
Create Notable Events from alerts

- Correlation Search

Apply Service Context & Configure Event Grouping

- Notable Event Aggregation Policies

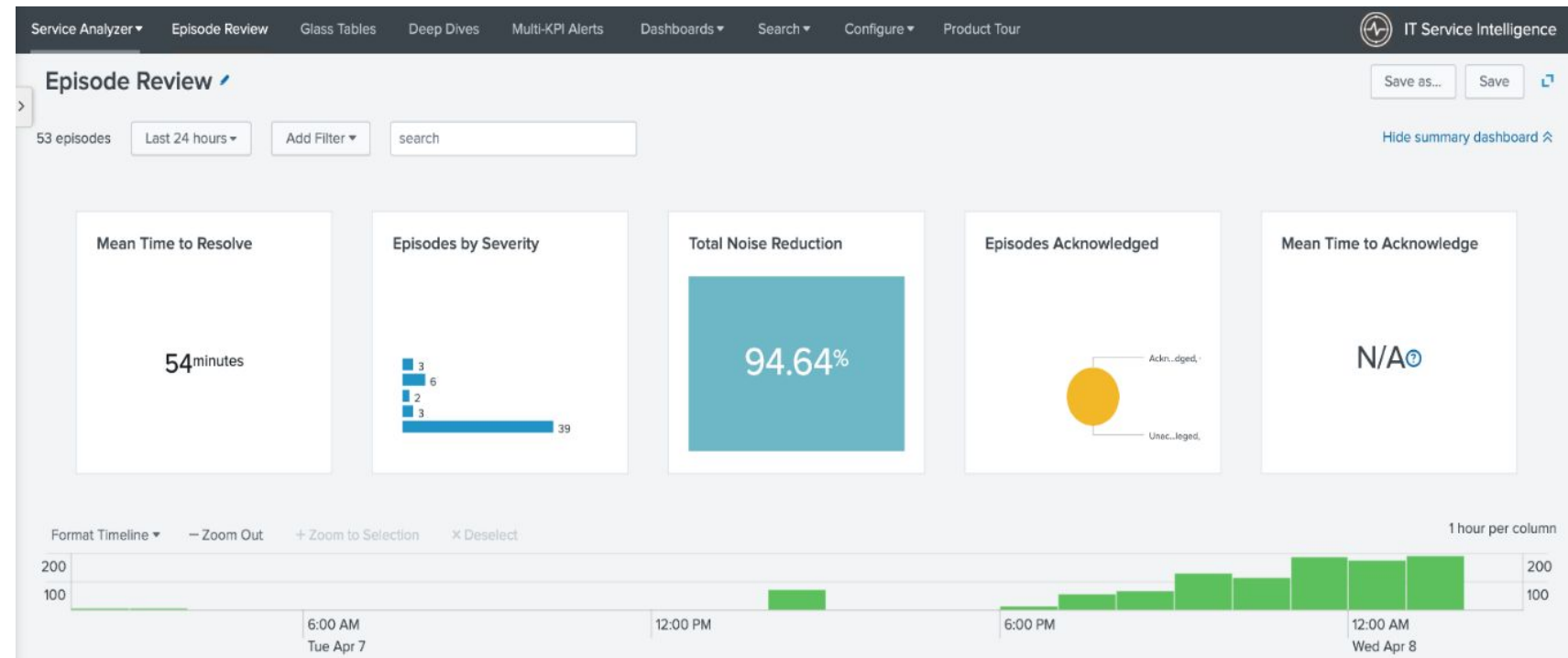
Review episodes



Event Analytics Lab: Episode View

When notable events are grouped by aggregation policies, the resulting groups are called episodes, you can think of an episode as an incident. The episode review page provides a great deal of information in a heads-up display and is like the cockpit view for Operations teams.

- ▶ Navigate to Episode Review
- ▶ Note the Noise Reduction



Event Analytics Lab: Episode View

- ▶ *Scroll down and review list*
- ▶ *Modify filter as shown*
 - *Critical & High only*

The screenshot displays the 'Episode Review' interface in Splunk. At the top, it shows '1 episode' and a time range of 'Last 24 hours'. The severity filter is currently set to 'Critical... (2)'. A search bar is visible on the right. Below the header, the interface is sorted by 'Time'. A table of episodes is shown, with the first episode highlighted: 'On-Prem Database issue' with an owner of 'Unassigned' and a severity of 'Seve'. A dropdown menu is open over the severity filter, showing a search bar and a list of severity levels: 'Critical', 'High', 'Info', 'Low', 'Medium', and 'Normal'. The 'Critical' and 'High' options are checked. The menu also includes 'Select All' and 'Clear All' buttons and shows '6 of 6 values'.

Event Analytics Lab: Episode View

- ▶ We will now review an episode to better understand the flow of events, and we will then ensure someone has ownership.

- ▶ Click on 'Authorization Issue' episode
- ▶ Review the details for each tab
- ▶ Add your name to the comments

- ▶ Change to 'In Progress'
- ▶ Review possible Actions

Format Timeline ▾ - Zoom Out + Zoom to Selection x Deselect 1 hour per column

1,200 600 12:00 Wed Apr 8 2020 18:00 00:00 Thu Apr 9 06:00

Sorted by ? ↓ Time ▾

Count	Event Type	Owner	Severity	Status
8	Authorization issue	Unassigned	Critical	Pending
2	Authorization issue	Unassigned	Critical	Pending
2	Authorization issue	Unassigned	Critical	Pending
1	Authorization issue	Unassigned	Critical	Pending
1	On-Prem Database issue	Unassigned	Critical	Pending

Authorization issue
9/4/2020 03:26:08 GMT+0000 (GMT) - 9/4/2020 03:51:10 GMT+0000 (GMT)
Possible issue with Authorization or upstream service
Notable Event Count: 8 Aggregation Policy: Service Issues

Impact Events Timeline Common Fields Similar Episodes **Comments** Activity All Events

IMPACTED SERVICES AND KPIS Analyze in Deep Dive

Authorization 100

SERVICE TOPOLOGY
View Full Topology

Focus: Authorization

Web Front End Mobile App Authorization



Next Steps

Somerford's Approach to ITSI

Sommerford's Glass Table Methodology

Project Phases

Initiation

- Kick-Off Call
- Pre-Workshop Planning
- ITSI Product Walkthrough

Analysis

- Service Identification Workshop
- Entity Strategy Workshop
- Service Decomposition Workshops

Data Onboarding & ITSI Installation

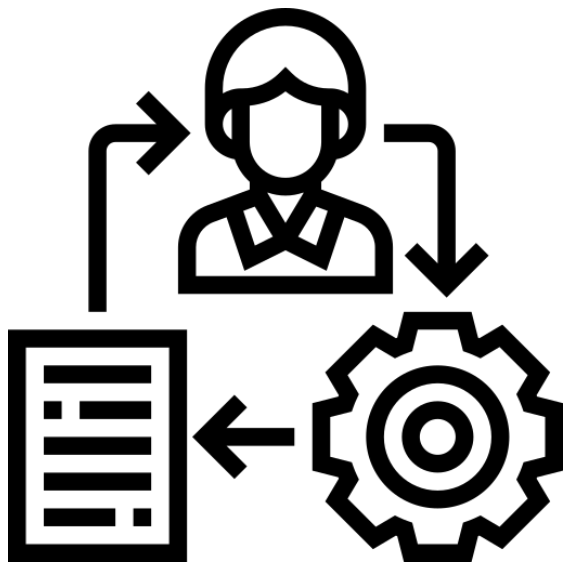
- ITSI Installation
- Data Onboarding
- Implement Entity Management Strategy

Delivery

- Delivery Planning
- ITSI Services Development
- Progress Review
- ITSI Service Review
- ITSI UI Development

Handover

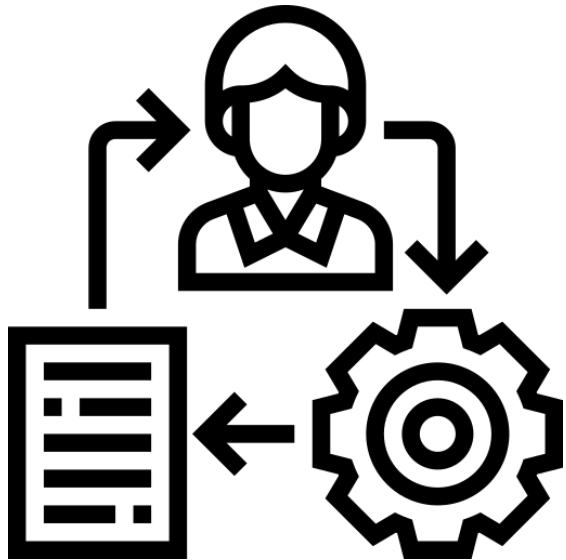
- Project Closeout
- Enablement
- BAU Transition
- Onboarding Users
- Follow-up Reviews



Service Identification

- Which business and technology services are candidates?
- Which services shall we do first?

Service Decomposition



- What are the business services to be monitored?
- What technology services make up those business services?
- What are the components of the technology services?
- What do you care about? What are the metrics?
- What are the KPIs?
- What data drives each KPI?

Thank You!

Please get in touch with us
if you have any questions.

paul.winchester@somerfordassociates.com



@Sommerford_Ltd



Sommerford Associates Limited