Splunk Nedir?

**Splunk**, büyük veri analitiği ve günlük (log) verisi analizi için kullanılan bir yazılım platformudur. Özellikle IT (bilgi teknolojileri) altyapıları, güvenlik olayları, uygulama performansı ve sistem izleme gibi alanlarda yoğun olarak kullanılır. Splunk, veriyi toplar, indexler (dizinler), analiz eder ve kullanıcıların görsel raporlar, panolar (dashboards) ve uyarılar oluşturmasına olanak tanır. Bu eylemler için SPL isimli SQL benzeri sorgu dilini kullanır. Siber güvenlikte SIEM, Kubernetes gibi dağıtık mimarı orkestrasyonları ve genel sunucu log trafiği analizi için sıklıkla tercih edilir.

Bu Proje için kullanım:

Veri Ekleme

1. Splunk’ı açın
2. Şu rotayı takip edin:

Dashboard -> Settings -> Add Data -> Upload Data

1. CSV Dosyasını burada yükleyin ve next diyerek devam edin. İşlem kolaylığı açısından index(ayrıştırma yapma alanı)’imizi ayrı bir isimle açmanız iyi bir tercih olacaktır.
2. Search Kısmına gelelim ve şu kodu yazalım. Bizim CSV dosyamız için en iyi çözümü sunacaktır.

Bilinmesi Gereken bazı komutlar:

Index= ayrıştırıcı kategorimiz

Eval= Veri manipülasyonu işlemi yapacağımızı bildiren komut.

Replace= x hücresindeki y verisini z ile değiştirir.

Field= Kabaca SQL’deki Column isimleri olarak düşünülebilir. Verileri tutan başlık olarak özetleyebiliriz.

Rename= bir Field’ı yeniden isimlendirmek için

regEX: Splunkta Regülasyon veri yönetim modellerini kullanmanızı sağlar. ^(bununla başlıyorsa), /s (boşluk ifadeleri) gibi ifadeleri barındırır.

İsnull(): eğer hücre boşsa

Mvindex(): hücredeki verinin değeri üzerinde gezin. Eğer veri TEXT tipinde ise bu değer her bir kelime olur.

Split(): Seperatörden sonra iki farklı parçaya ayır.

Trim(): özel bir kelimeden sonra verinin diğer kısmını sil.

Lower(): verileri küçük harf yap.

Case(): verilerin büyük yada küçük harf barındırmalarını önemseme.

Like(): SQL’deki Like ile aynıdır (Şu harf ile başlayan veriler vb). %’ler veya RegEX ifadeleri ile zenginleştirilmelidir.

Table: tablo haline getir

index="dataset" # Dataset Ayrıştırıcısında ara

| foreach \* [eval <<FIELD>> = replace('<<FIELD>>', ":", "")] # “:” ile başlayan hücrelerden “:”ü temizle. (CSV Dosyasının ayrıştırılmadan gelmeyişinden dolayı ihtiyacımız var.)

| eval Fiyat = replace(Fiyat, ",.\*", "") Sadece Fiyat Field’ında “,”den sonrasını sil. (CSV Dosyasının ayrıştırılmadan gelmeyişinden dolayı ihtiyacımız var.)

| rename #bu fonkisyon: Uygunsuz isimdeki Tüm Field’lardaki verileri yeniden adlandırır.

"A\_\_\_\_rl\_\_k" as Agirlik,

"Ekran \_\_\_\_z\_\_n\_\_rl" as Ekran\_Cozunurlugu,

"Ekran Kart\_\_ Haf\_\_zas" as Ekran\_Karti\_Hafizasi,

"Ekran Kart\_\_ Modeli" as Ekran\_Karti\_Modeli,

"Ekran Kart" as Ekran\_Kart,

"Ekran Boyutu" as Ekran\_Boyutu,

"Ekran Kart\_\_ Tipi" as Ekran\_Karti\_Tipi,

"Ekran Yenileme H\_\_z" as Ekran\_Yenileme\_Hizi,

lemci as Islemci,

"lemci \_\_ekirdek Say\_\_s" as Islemci\_Cekirdek\_Sayisi,

"lemci \_\_nbelle\_\_i" as Islemci\_Onbellegi,

"lemci H\_\_z" as Islemci\_Hizi,

"lemci Modeli" as Islemci\_Modeli,

"lemci Nesli" as Islemci\_Nesli,

"lemci T\_\_r" as Islemci\_Turu,

"letim Sistemi" as Isletim\_Sistemi,

"Pil G\_\_c" as Pil\_Gucu,

"r\_\_n Ad" as Urun\_Ad,

"r\_\_n URL" as Urun\_URL,

"RAM T\_\_r" as Ram\_Turu,

"z\_\_n\_\_rl\_\_k Format" as Cozunurluk\_Format,

"RAM Frekans" as RAM\_Frekans,

"Panel Tipi" as Panel\_Tipi

| foreach \* [eval <<FIELD>> = replace(<<FIELD>>, "^[\x{00A0}\s]+", "")] # ASCII değeri ve regEX kullanarak hücrelerin başındaki gereksiz boşluğu temizle. (CSV Dosyasının ayrıştırılmadan gelmeyişinden dolayı ihtiyacımız var.)

| eval Agirlik=lower(trim(Agirlik)) | eval Agirlik=case( like(Agirlik, "%kg"), tonumber(replace(Agirlik, "[^0-9.]", "")), like(Agirlik, "%gr"), tonumber(replace(Agirlik, "[^0-9.]", "")) / 1000, 1=1, null() ) #Ağırlığı numeric bir değer yapabilmek için kg ve gr değerlerini sil. Gram’ı, Kilogram cinsinden yaz.

| eval Marka=mvindex(split(Urun\_Ad, " "), 0) #Markayı bulabilmek için Ürün Adının ilk kelimesini al

| eval Seri=if(isnull(Seri), mvindex(split(Urun\_Ad, " "), 0)." ".mvindex(split(Urun\_Ad, " "), 1), Seri) #Ürünün serisini bulabilmek için Ürün Adının ilk iki kelimesini al.

| table #Bu Kod ise alttaki verilerden bir tablo taslağı oluşturmamızı sağlar.

"Urun\_Ad", "Marka", "Seri", "Urun\_URL", "SSD", "Islemci\_Turu", "Islemci\_Nesli", "Islemci\_Modeli", "Islemci\_Hizi", "Islemci\_Cekirdek\_Sayisi", "Ekran\_Kart", "Ekran\_Karti\_Hafizasi", "Ekran\_Karti\_Modeli", "Ekran\_Karti\_Tipi", "RAM", "Ram\_Turu", "RAM\_Frekans", "Ekran\_Boyutu", "Ekran\_Cozunurlugu", "Cozunurluk\_Format", "Panel\_Tipi", "Ekran\_Yenileme\_Hizi", "Isletim\_Sistemi", "Pil\_Gucu", "Agirlik", "Fiyat"

1. Veri Modeli olarak yaratmak

Ana Menüden 4. Maddedeki Search’ü çalıştırdıktan sonra şu yolu takip edin.

Create View Model -> Done -> Tablonuza isim verin.

1. Veri Tablosu oluşturduktan sonra görsel grafikler oluşturabilirsiniz bunuda DataSet Tablonuzun ekranındayken.

Visualize with Pivot’a tıkladıktan sonra istediğiniz grafiği seçip istediğiniz Axis değerlerini seçtikten sonra tamamlayabilirsiniz.

1. Tablonun son durumunu CSV gibi formatlarda dışarı aktarabilmek için