**Malware Data Science~Kötü Amaçlı Yazılım Veri Bilimi (Saldırı Algılama ve İlişkilendirme - Attack Detection and Attribution )**

Güvenlik bilgileriniz ve olay yönetimi (SIEM) yazılımınız (security information and event management )muhtemelen verilerinizde ki şüpheli eğilimleri belirlemek için veri bilimini kullanır.

\*Data Science  Veri bilimi nedir ?

veri bilimi , istatistikleri , matematiği ve sanatsal istatistikleri anlamamıza ve bu veriler hakkında tahminlerde bulunmamıza olanak tanıyan, büyüyen bir algoritmik araçlar kümesidir. Daha spesifik tanımlar var, ancak genel olarak veri biliminin üç alt bileşeni vardır: makine öğrenimi machine learning , data mining veri madenciliği ve data visualization veri görselleştirme

Güvenlik bağlamında, makine öğrenimi algoritmaları yeni tehditleri tespit etmek için eğitim verilerinden öğrenir. training data

veri madenciliği algoritmaları kuruluşlarımızı hedef alan saldırı kampanyalarını ayırt etmemize yardımcı olabilecek ilginç modeller (tehdit aktörleri arasındaki ilişkiler gibi) için güvenlik verilerini arar.

son olarak veri görselleştirme insanların ilginç ve şüpheli eğilimleri fark etmelerini kolaylaştırmak için steril tablo şeklindeki verileri grafik formata dönüştürür.

\*Veri Bilimi Güvenlik için neden önemli ?

[ww.av-test.org](http://ww.av-test.org)/en/statistics/malware den kötü amaçlı malware sayılarının istatistikerine bakılabilir.

malware de manuel tespit teknikleri imzalar gibi atık her şeyi algılamak için kolaylık sağlayabilir.

\*Veri Bilimini Malware'e uygulamak:

fidye yazılımı e-posta ekleirnden kullanıcıların makinelerine ardından verilerini şifreleyip kilit için para

Kötü amaçlı yazılım veri bilimini anladığınızda, veri bilimini ağ saldırılarını, kimlik avı e-postalarını veya şüpheli kullanıcı davranışlarını tespit etme gibi diğer güvenlik alanlarına uygulamak için daha donanımlı olacaksınız. Aslında, bu kitapta öğreneceğiniz hemen hemen tüm teknikler, yalnızca kötü amaçlı yazılım için değil, genel olarak veri bilimi algılama ve istihbarat sistemleri oluşturmak için geçerlidir.

Kitaptaki kodları malware data science.comdan indirebilirsin.