Hızla gelişen ve büyüyen bir teknoloji çağında yaşıyoruz. Bu da beraberinde internetin her gün hayatlarımıza daha da fazla entegre olması durumunu getiriyor. İnternete artan bağımlılık ve ihtiyaç ise siber saldırganlar için daha fazla bir saldırı alanı olduğu anlamına geliyor. Bu yazıda sizlere olası bir siber saldırı sırasında ve sonrasında saldırıyı ele alma, alınacak olan aksiyon ve olayları etkin bir şekilde yürütülmesi gibi aşamaların bulunduğu “Incident Response” durumu içerisinde yer alan 4 Metric ile ilgili bir yazı düzenledim. Bu Metric’ler nelerdir, ne işe yarar ve nasıl kullanırız bunlara değineceğim.

**1. Mean time to detect (MTTD)**

Bu Metric ekibimizin olası bir güvenlik olayını tespit etmesi için ihtiyaç duymuş olduğu ortalama bir süre olarak belirtilebilir. Burada MTTD’yi ölçebilmemiz için, öncelikle ekipte belirli bir süre zarfında olan olayların tespit edilmesi ne kadar zaman alıyor? Önce bu zamanlar hesaplanır ve toplanır. Daha sonrasında ise toplanan bu zaman, önceden belirlenmiş süre zarfında meydana gelen olay sayısına bölünür. Bu Metric genelde ekipler arasındaki etkinliğin karşılaştırılması veya mevcut ekibin olayları izleme durumunu değerlendirmek için kullanılabilir.

SANS 2019 Olay Müdehalesi anketine göre, kuruluşların %52,6’sının MTTD’si 24 saatten kısayken, %81,4’ünün MTTD’si 30 gün veya daha az olduğu tespit edildi. SOC, kurum içi veya bulut kaynakların 7/24 gerçek zamanlı izlenmesini sağladığından dolayı ekibin yeteneklerini genişlemesinde önemli rol almaktadır. Bu, bir saldırının olup olmadığını, ne zaman ve nerede meydana geldiğini görmemize de yardımcı olarak MTTD'yi de büyük ölçüde azaltmaktadır.

## 2. Mean time to acknowledge (MTTA)

## Bu Metric ise alarmın meydana geldiği zaman ve bu alarma BT personelinin verdiği yanıtın zamandır. Bir diğer anlatım ile personel alarm meydana geldikten ne kadar süre sonra bu alarma yanıt vermiş bu arada geçen süre olarak tanımlanmaktadır. MTTD bizlere bir olayın tespit etme süresi hakkında bilgi verirken, MTTA ise sorunu fark etmenin ve bu sorun üzerinde çalışmaya başlamanın ne kadar sürdüğüne odaklanmaktadır.

## 3. Mean time to recovery (MTTR)

## Bu Metric’te ise çalışanların saldırıdan etkilenmiş bir sistemi tekrardan çalıştırılabilir hale getirmesi için arada geçen süredir. Daha basit bir ifadeyle anlatmak gerekirse güvenlik açığı keşfedildikten sonra kapatılması için geçen süredir. MTTR bize Incident Response ekibinin ve bu saldırıdan etkilenen müşterilerin normale ne kadar hızlı bir şekilde döndürüleceği hakkında bilgi vermektedir. Dolayısıyla bu Metric’teki düşük performans hizmet verilen kuruluş için daha yüksek ihlal maaliyetleri anlamına gelebilmektedir.

## 4. Mean time to contain (MTTC)

Bu Metric ise kuruluşunuzun tüm bu olaylara karşı ne kadar iyi bir şekilde yanıt verdiğine bütünsel bir bakış açısı getirmek için MTTD, MTTA ve MTTR’yi bir araya getirir. MTTC Incident Response ekibinin bir olayı tespit etmesinin, daha sonra o olayı kabul etmesinin ve bu saldırının daha fazla zarar vermesini etkili bir şekilde önlenmesinin ne kadar sürdüğüne odaklanmaktadır.