Gereksinimler

- MISP Gereksinimleri

MISP Gereksinimleri

MISP kullanım senaryosunu belirlerken, ilk adım kullanım amacını belirlemektir. Kullanıcı sayısı, alınan veri miktarı, kullanılan veri noktaları, olay sayısı, ilişkilendirme sayısı ve API kullanımı gibi faktörlerin hepsi göz önünde bulundurulmalıdır.

Donanım gereksinimleri oldukça düşüktür; genellikle 2+ çekirdekli ve 8-16 GB belleğe sahip bir web sunucusu yeterlidir, ancak daha fazlası her zaman tercih edilir. Gereksinimler veri kümesi ve kullanıcı sayısına bağlıdır.

Gereksinimleri Etkileyebilecek Bazı Önemli Hususlar:

- Verilerin yüksek oranda ilişkilendirilmesi, bellek ve hesaplama yoğunluğunu artırabilir. Bu durumda, ilişkilendirme oranını düşürmek veya bellek ve CPU kapasitesini artırmak düşünülebilir.
- Örnek sayısı ve ek dosyalar, doğrudan disk kullanımını etkiler.
- Eş zamanlı kullanıcı sayıları, bellek ve CPU kullanımını etkiler.
- Uzak *feedlerin* ve sunucuların önbelleğe alınması, sistemin bellek gereksinimlerini artırır.
- Günlük faaliyetlerin miktarı, veritabanı ve yerel günlük dosyalarının disk gereksinimlerini artırabilir.

Operasyonel Sunucular İçin Örnek Gereksinimler:

- Küçük paylaşım merkezleri ve uç nokta MISP'leri için 16 GB bellek ve 2 vCPU yaygındır.
- Büyük paylaşım toplulukları için 128 GB bellek ve 32 fiziksel CPU çekirdeği önerilir.
- COVID misp topluluğu, 4 vCPU ve 8GB bellek ile binlerce kullanıcıya hizmet verir.
- Eğitim örnekleri, sadece 2GB bellek ve tek bir vCPU üzerinde çalışır (ancak bunun eğitimler / deneyler dışında kullanılması önerilmez).

Veri tabanı:

- MISP'in ana veritabanı MariaDB'ye dayanır.
- Düşük gecikme süresi için SSD kullanılması önerilir.
- Kullanılan depolama türü, gecikmeyi ve kullanılan disk alanını etkileyebilir.

Feed Önbelleği:

- Feedlerden gelen ögeleri önbelleğe almak için RAM kullanılır ve ögeler önbelleğe alınır.
- Varsayılan olarak kullanılabilir feedler etkinleştirilmiş ise, tüm feedlerin 1.2GB'a kadar bellek kullanabileceği unutulmamalıdır.