TREND MİCRO APEX ONE ON-PREMISE INSTALLATION

Fiziksel yada sanal suncumuzun kurulumunu gerçekleştiriyoruz.

Sunucularımızı kurarken trend micro documents a gidip kurulacak ürünün sistem gereksinimlerine bakarak kurulması gerekmektedir.

Trend micro download center a gidip Apex One full installation package indirelim.

Apex Central da aynı sunucuya kurulacaksa onu da download center üzerinden indirelim. Product Patch’leri de indirerek son sürüme yükseltebilirsiniz. Ben demo ortamı kuracağım için indirmiyorum.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Sunucumuz kurulduktan sonra,

UAC,DEP,WindowsFW,IE Enchanced kapatılması gerekiyor.

Static IP’mizi verelim.

Remote Desktop açalım.

Server Manager üzerinden Add Features diyerek aşağıdaki görüntüdeki featuresler açılması gerekiyor.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Şimdi Apex One Setup dosyamızı çalıştırarak kuruluma geçelim.

Run As Admin ile çalıştır dedim ve extract etmeye başladı. Tamamlandığında wizard karşılayacak bizleri.

Graphical user interface

Description automatically generated

Graphical user interface, application, Word

Description automatically generated

Next diyip devam ediyoruz.

Graphical user interface, text, application, email

Description automatically generated

Lisansı kabul edip devam ediyoruz.

Graphical user interface, text, application, email

Description automatically generated

Bu noktada eğer scan the target endpoint seçeneği seçilirse kurulum yapmadan önce tüm makineyi tarayacak ve o şekilde kuruluma geçecektir. Do not scan derseniz taramadan kurulum yapacaktır. Kurulum aşaması do not scan derseniz daha hızlı olacaktır. Zaten temiz bir makineye kurulum yapılacağı için ilk etapta taramasını istemeyebilirsiniz.

Graphical user interface, application

Description automatically generated

Burada sunucumuz direk internete çıkabiliyorsa bu aşamada değişiklik yapmadan devam edebiliriz.

Graphical user interface, text, application

Description automatically generated

Apex One lisansımızı girip devam ediyoruz.

Graphical user interface, application

Description automatically generated

Kurulumun yapılacağı path karşımıza geliyor. Değişiklik yapmadan geçebilirsiniz.

Graphical user interface, text, application

Description automatically generated

Burada FQDN de yazılabilir makine ip’si de yazılabilir. Bazen DNS’ten isim çözme konusunda sorunlar yaşamamak için ben ip tercih ediyorum.

Graphical user interface, application

Description automatically generated

Trend Micro burada ajanlarla konuşmak için bir sertifika üretiyor. Sertifika geçerliliğini ben 10 yıl olarak yaptım siz isterseniz 3 olarak da bırakabilirsiniz. Portlar da geldiği gibi bırakabilirsiniz.

Graphical user interface, text, application, email

Description automatically generated

Bu aşamada on premise EDR modülünü etkinleştirmek isteyip istemediğimizi soruyor. Varsa lisansınızda kullanabilirsiniz.

Graphical user interface, text, application, email

Description automatically generated

Var olan SQL server’ınız kullanabilirsiniz. Ya da install/create a new seçeneğinde bırakarak trend micro kendi üzerinde bir sql express kuracaktır. Sa password verip database ismi girip geçebilirsiniz.

Graphical user interface, text, application, email

Description automatically generated

Bu aşama bilgilendirme aşamasıdır next diyip devam edelim.

Antivirüs Database’leri belirli saatlerde güncelleme alır. Örneğin her gün saat 12:00 de yeni gelen tehditlerin güncellemesi database’lere işlenir.

Scan methodlarından Conventional Scan seçerseniz bu güncelleme gelip database güncellenene kadar yeni gelen tehditlerden bilginiz olmaz.

Smart Scan methodunu kullanırsanız anlık bulunmuş tehditleri smart scan server gidip Trend Micro Global database’sine sorarak yeni gelen tehditi database’ine yazar ve o tehditten korunmanınızı sağlar.

Graphical user interface, text, application, email

Description automatically generated

Burada apex one ajanlarının smart scan yapabilmesi için gerekli olan smart protection server kuracağını belirtiyor. Eğer aynı makinede olmasını istemiyorsanız başka bir sunucuya kuracaksanız no diyebilirsiniz.

Graphical user interface, text, application, email

Description automatically generated

Kurulum bittikten sonra ajanı da yüklemiş oluyorsunuz eğer seçerseniz. Kurulum sonrasında da kurabilirsiniz. Next diyip devam edelim.

Graphical user interface, text, application, email

Description automatically generated

Smart Feedback yapılsın mı diye soruyor. Eğer isterseniz seçip devam edebilirsiniz.

Graphical user interface, text, application

Description automatically generated

Makinemize kurulacak ajanın konuşacağı port’u 21112 olarak varsayılanda bırakabilirsiniz.

Graphical user interface, text, application, email

Description automatically generated

Varsayılan politika Windows FW de geçerli olsun mu diyor. Bu şekilde bırakıp geçebilirsiniz.

Graphical user interface, text, application, email

Description automatically generated

Next diyip devam edelim.

Graphical user interface, text, application

Description automatically generated

Bu aşamada Spyware’lere değerlendirme yapmak istiyormuyuz diye soruyor. Bazen spyware’ler iyi amaçlada kullanıldığı için ilk kurulumda yes,enable assessment seçeneğini seçip 1-2-3-4 hafta bloklama sadece izle diyebilirsiniz.

Graphical user interface, text, application, email

Description automatically generated

Next diyip devam edelim.

Graphical user interface, text, application, email

Description automatically generated

Ajanlarla konuşurken kullandığı ssl sertifikası için bir parola oluşturabilir. Daha sonra sunucunuzu değiştirmek migrate etmek isterseniz ssl sertifikanızı export-import ederek ajanların aynı sertifika ile çalışmasını sağlayabilirsiniz.Generate a new seçeneğini seçip burada parolamızı yazalım.

Graphical user interface, application

Description automatically generated

Bu aşamada web konsol kullanıcı şifre bölümü karşımıza geliyor. Varsayılan kullanıcı root olarak geliyor. Root kullanıcısına bir passwd oluşturmanız gerekiyor. Aşağıdaki bölümde de ajanların makineden kaldırılmak istendiğinde girilmesi gereken şifreyi belirleyip next diyelim.

Graphical user interface, application

Description automatically generated

Next diyip devam edelim.

Graphical user interface, text, application, email

Description automatically generated

İnstall diyerek kurulumu başlatalım. Ortalama 20-30 dk sürecektir. Tarama işlemi yapılsın dediyseniz bu süre uzayabilir.