asma
know your assets

Ağ Görünürlülüğünüzü Sağlayarak Güvenlik Seviyenizi Yükseltin

ASMA Hakkında

Ağ varlıklarınızın farkına varmak ve varlıklarınızı yönetmek için geliştirilmiş olan web tabanlı siber güvenlik yazılımıdır. Varlıkların IP adresini, işletim sistemini ve aktif servislerini otomatik olarak keşfeder ve sahibi, sorumlusu, marka, modeli vb. bilgilerini tutmanızı sağlar.

Saldırganların ilk hedefi bilinmeyen, bilinmediği için güncellenmeyen ve zafiyet barındıran sistemlerdir.

Organizasyonlar, ağlarında yer alan yetkili ve yetkisiz varlıklardan haberdar değillerdir

Sistemlerdeki yetkisiz değişiklikler tespit edilememektedir.

Varlık envanteri uygulamaları güvenlik odaklı olmadığından ağa yeni dahil olan yetkisiz varlıkları tespit edememektedir.

Ağdaki varlıkların aktif ve pasif yöntemler ile tespit edilmesi, sahibinin, sorumlusunun ve önem derecesinin belirlenmesi gerekir.

Sahibi, sorumlusu olmayan varlıkların tespit edilmesi önemlidir.

Otomatik ve güncel bir envanter tutulması ağ görünürlüğünü arttıracaktır.

Ağ görünürlüğünün sağlanması ile anomali tespiti yapılabilecektir.

Nasıl Çalışır?

ASMA temel olarak iki bileşenden oluşur; bu bileşenler **merkezi yönetim bileşeni** ve **sensör bileşenidir.**

Sensör bileşeni, varlık ve servis keşfi yapılmak istenen ağ segmentine kurulan hafifleştirilmiş ve sıkılaştırılmış linux tabanlı bir sanal sunucudur. Sensör ilgili ağ segmentinde sürekli olarak pasif dinleme ve aktif keşif yaparak varlıkları ve varlıklar üzerindeki servisleri keşfeder.

Merkezi yönetim bileşeni ise sensörlerden aldığı verileri işlemek, varlık envanterini yönetmek, alarm ve uyarıları izlemek ve rapor oluşturmak için kullanılan bileşendir. Merkezi yönetim bileşeni ağın istenilen herhangi bir segmentine kurulabilen linux tabanlı sıkılaştırılmış bir sanal sunucudur.

Aktif Tarama Nedir?

Aktif keşif, IP adresine sahip varlıkların üzerindeki TCP servislerini tespit etmek için kullanılan bir yöntemdir. Aktif keşif ile OSI 4. katmandaki TCP servislerinin keşfedilmesi amaçlanır. Aktif keşif sırasında sensör, ilgili varlık üzer- inde koşan servis ile etkileşime girdiğinden, varlık üzerinde kurulu olan FW vb. koruma yöntemlerinden etkilenir.

Keşif sırasında en çok kullanılan 1000 TCP portuna tarama gerçekleştirilir. Sensör, varlığın bulunduğu ağ segmentine konumlandırıldığından, tarama ilgili ağ segmenti dışına çıkmaz.

Pasif Dinleme Nedir?

Pasif dinleme, IP adresine sahip varlıkları keşfetmek için kullanılan ve OSI 2. katmanda çalıştırılan bir keşif yöntemidir. Pasif dinleme sırasında sensör, konumlandırıldığı ağ segmentindeki IP varlıkları tarafından üretilen ARP/RARP paketlerini dinleyerek varlık keşfini sağlar. Pasif dinleme sırasında sensör IP varlıkları ile herhangi bir etkileşime girmemektedir.

Aktif - Pasif Varlık Keşfi

Ağ segmentlerine konumlandırılan sensörleri aracılığıyla BT varlıklarını gerçek zamanlı olarak tespit eder.

IP Adresi Değişikliği Tespiti

Varlıklarınızdaki IP adres değişikliklerini tespit eder.

Yeni Varlık Tespiti

Ağ envanterinizde olmayan bir varlık belirdiğinde, bu durumu anında tespit eder.

MAC Adres Değişikliği Tespiti

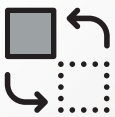
Varlıklarınızdaki MAC adres değişikliklerini tespit eder.

Yeni Servis Tespiti

Varlıklarınızda bir servis oluşması durumunu tespit eder.

Varlık Temelli Korelasyonel Anomali Tespiti

Ön tanımlı korelasyon kuralları ile varlıklarınızdaki güvenlik anomalilerini tespit eder.



Servis Değişikliği Tespiti

Ağınızda yer alan varlıklardaki servis değişikliklerini tespit eder.

Kullanıcı Dostu Arayüz ile Kolay Varlık Envanteri Yönetimi

Kullanıcı dostu arayüzü ile kurulduğu anda varlık envanterini toplamaya ve yönetmeye olanak sağlar.