SCADAfence

Value-Added Distributor
OTD BİLİŞİM
www.onlineteknikdestek.com

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

SCADAfence Platformu

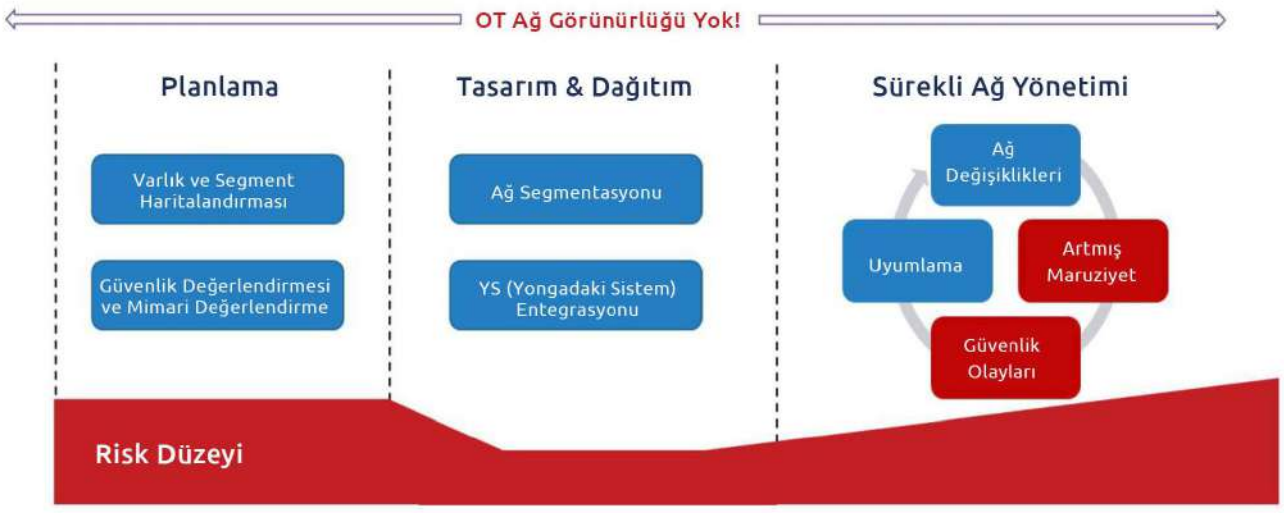
SCADAfence Platformu Ağ Segmentasyonunu Nasıl Verimli ve Etkili Bir Hale Getiriyor

Giriş

Çok da uzak olmayan geçmişte, yaşamsal sistemler dış tehditlerden asıl olarak anlamı diğer ağlar ve İnternet ile etkileşimi engellemek için sistemlerin iletişimlerini kesmek olan "hava aralığı" aracılığıyla korunurdu.
Bugün, 4. sanayi devriminin ortasında, artan bağlanabilirlik düzeylerinin hava aralığının ilgisini tamamen ortadan kaldırarak kurumları güçlendirmesi ve hala rekabet

OT Ağ Segmentasyon Projelerinin Zorlukları

Meşgul iç OT ağlarında segmentasyon işlemi bilinen BT Sınır korumasından farklıdır. Bağlantıların aralığı ve karmaşıklığı çok daha yüksektir ve üretim süreçlerinin önem düzeyi özellikle çok sayıda güvenlik duvarı dağıtıldığında ve mikro segmentasyon hedeflendiğinde kurum sınırından geçen günlük ofis trafiğinden çok daha fazladır. Dolayısıyla, uygun şekilde yapıldığında segmentasyon OT ağ güvenliğini artırırken, bu yatırımı etkili hale getirmek için halen göz önünde bulundurulması gereken büyük zorluklar ve muhtemel zayıflıklar söz konusudur.



Şema# 1: Uygun Görünürlüğe Sahip Olmayan Ağ Segmentasyon İşlemi ve OT İşlemi İlişkisi

Bu problemler çoğunlukla ağ görünürlüğünün yetersiz olmasından, manuel işlemlere bel bağlamaktan ve ağ cihazlarının ağ üzerinde çalışan OT işlemleri ile karşılıklı ilişkisinin eksik olmasından kaynaklanır.

Planlama ve dağıtım aşamasındaki zorluklar:

• **Görünürlük Eksikliği Nedeniyle Yüksek Risk.** Segmentasyon projeleri analiz, planlama ve dağıtım aşamaları nedeniyle genel olarak birkaç ay, hatta daha uzun sürer. Bu süre içerisinde, ağın görünürlüğü kaybolur ve uygun güvenlik sağlanamaz. Günümüzün dinamik ortamında, bu ortaya çıkacak kritik güvenlik olaylarına ilişkin çok uzun bir süre demektir.

• **Etkisiz Dağıtım.** Güvenlik duvarları iç meşgul ağlara dağıtılırken, tehlikeli trafiğin tamamını "göremeyebilirler". Uzaktan bağlantılar veya dolandırıcı cihazlar mevcut olabilir ve güvenlik duvarını aşabilir ve bu durum güvenlik duvarı loglarında görünür olmayabilir. Bazen, lokasyonun kendisi uygun şekilde seçilmez, çünkü farklı bir ağ kesişme noktasının segmentasyonu çok daha etkin bir şekilde yapılabilir. Bu tür durumlarda, güvenlik ekibi gerekli koruma düzeyi yetersizken yanlış bir güvenlik algısına sahip olabilir.

• **İş süreçleri ile karşılıklı ilişki eksikliği.** Güvenlik duvarları gördükleri IP adresi ile cihazın rolü arasında karşılıklı bir ilişki kurmaz. Birçok IP'si ve uygulama trafik türü bulunan dahili ağlarda, bu durum trafik örüntülerini anlamada, kritik endüstriyel işlemleri yanlışlıkla engellemede ve bu işlemlere müdahale etmede - veya diğer bir yandan - endüstriyel ağı riske atarak güvenlik duvarında birçok gereksiz port açarak sayısız manuel (ve uzun süreli) iş yüküne sebep olabilir.
Bu da segmentasyon teknolojilerindeki yatırımı etkisiz hale getirir ve en nihayetinde yüksek risk düzeyi teşkil eder.

Sürekli yönetim aşamasındaki zorluklar:

• **Zamanla bozulma.** Ağ segmentasyonu ağ değişiklikleri, politika ihlalleri ve insan hatası nedeniyle zamanla "çözülür". Ağa yeni sistemler eklenir ve mevcut yapılandırmalar ve politikalar güvelik politikasında "boşluklar" yaratarak dinamik olarak evrilir.
Bu da segmentasyon projesi ile düşürülen risk düzeyinin hemen güvenlik duvarı kullanımı sona erdikten sonraki birinci günden başlayarak tekrar yükseldiği anlamına gelir.
Fark edilmemeye devam ederse, bu bozulma ciddi güvenlik olaylarına ilişkin yüksek bir risk teşkil eder.

• **Sınırı aşan saldırı vektörleri** Ağ altyapısında sınır güvenliğini aşmak için genellikle kasten değişiklikler yapılır. BT ve OT veya dış sağlayıcılar için arka kapılar oluşturulur, bu da ardında riskli açıklar bırakır. Kontrolsüz bir şekilde İnternetten/İnternete yeni bağlantılar kurulabilir. Ağı tehdit eden saldırı vektörlerine örnek olarak dahili kullanıcılar, USB cihazları, kablosuz erişim, e-posta üzerinden kötü amaçlı bulaşma verilebilir.
Dolayısıyla, ağ güvenliğini sağlamak için OT ağlarının güvenlik duvarı dışında başka araçlar ile izlenmesi gerekir.

• **Uygulama ve Yönetim Sistemleri.** Ağ uygulama düzeyinde genellikle "düz" olarak görüntülenir. Domain kontrolörleri veya İmalat Yürütme Sistemleri (İYS) gibi sistemler kurum içerisindeki alt ağların tümüne erişim sağlar ve segmentasyon ile korunmaz.

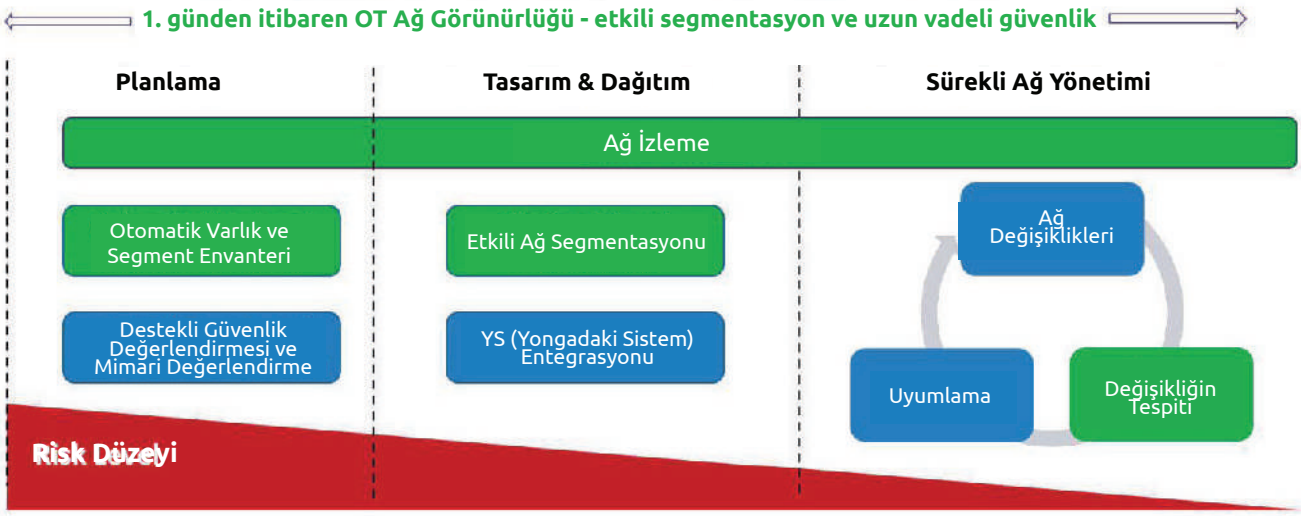
NEW YORK,462 W Broadway New York, NY 10012, ABD +1-646-475-2173
MÜNİH, Schellingstr. 109a80798 Münih Almanya +49-322-2109-7564

TOKYO, Clip Nihonbashi, 3-3- 3 Nihonbashi Honcho
Chuo - ku, Tokyo 103-0023, Japonya +81- 3-4588-5432

İrtibat: info@scadafence.com © 2019
www.scadafence.com

Sürekli İzleme ve Otomatik Varlık Keşfi Ağ Segmentasyon Zorluklarını Nasıl Ele Alır

SCADAfence Platformu sürekli ağ izleme ve otomatik varlık keşfi sağlar. Yukarıda belirtilen zorlukların çözülmesine yardımcı olan ve güvenlik mimarisini tamamlayan ekstra bir siber savunma katmanı sunar.



Şema #2: Sürekli izleme ve varlık keşfi ile etkili ağ segmentasyonu

Planlama ve dağıtım aşamalarındaki zorlukların ele alınması:

• Segmentler arasındaki trafik örüntülerinin analizi. SCADAfence Platformu tüm ağ segmentlerini haritalandıran bir "Segmentler Haritası" ve mantık grupları arasındaki ve farklı ağ kısımları arasındaki bağlantıları gösteren ve anormal veya riskli trafik ile ilgili uyarılar veren bir "Maruziyet Haritası" sunar. Ek otomatik trafik analizi görüntülemeleri kullanıcıya içgörü ve uygulama davranış ve gereklilikleri sağlar ve güvenlik duvarını aşan eksik trafiği engeller.

Bu da ilgili trafiğin tamamının tespit edilmesini ve segmentasyon işleminin etkili bir şekilde yapılmasını sağlar.

• Otomatik Risk Değerlendirme Raporu. İzleme çözümü değerli iletişim örüntülerini belirlemek ve güvenlik sorunlarını tespit etmek için kullanılan bir risk analiz aracı olarak görev yapar. Maruziyetleri ve güvenlik açıklarını ortaya çıkarır, potansiyel saldırı vektörlerinin haritalandırılmasını sağlar ve manuel araştırma ile değil, gerçek verilere dayanarak güvenlik gereksinimlerinin tespit edilmesine yardımcı olur. Son olarak, ağ yöneticisine bulgulara ve düzeltici tavsiyelere dair detaylı bir rapor sunulur. Bu rapor, segmentasyon işleminin kritik ağ risklerini ele almasını ve önemli güvenlik sorunlarının görmezden gelinmemesini sağlar.

NEW YORK,462 W Broadway New York, NY 10012, ABD +1-646-475-2173
MÜNİH, Schellingstr. 109a80798 Münih Almanya +49-322-2109-7564

TOKYO, Clip Nihonbashi, 3-3- 3 Nihonbashi Honcho
Chuo-ku, Tokyo 103-0023, Japonya +81-3-4588-5432

İrtibat: info@scadafence.com © 2019
www.scadafence.com

•1. günden itibaren riskin azaltılması - ağın izlenmesi, görünürlük sağlanması ve herhangi bir anormal aktivite veya politika sapmalarına ilişkin uyarılar alınması ile anında risk azaltımı alınır ve güvenlik olaylarına ilişkin ağı açık bırakarak tüm güvenlik mekanizmaları devrede olana kadar aylarca ertelenmez.
Sürekli yönetim aşamasında ağın temiz ve güvende tutulması:

• **Değişikliklerin tespiti ve güvenlik olaylarının önlenmesi.** Ağlar dinamiktir: varlıklar eklenir, güvenlik duvarı kuralları güvensiz işlemlere izin vermek için değiştirilebilir, uzaktan bağlantılar konfigüre edilir ve hepsi segmentasyon aracı tarafından tespit edilmez. İzleme çözümü ağ bağlanabilirliğine dair net bir resim sunar ve her türlü değişikliğe ve politika ihlallerine ilişkin uyarılar verir.
Bu sayede, bir sonraki güvenlik olayı ortaya çıktıktan sonra değil, çıkmadan önce uyumlama yapılmış olur. İzleme siber saldırı ve kötü amaçlı yazılım bulaşmaları riskini düşürür ve potansiyel olayları halletmek için gerekli zamanı azaltır.

• **Güvenlik duvarını aşan arka kapıların ve saldırı sağlayıcıların ortadan kaldırılması.** SCADAfence Platformu, segmentasyon kapıları ile görülmese dahi yeni oluşturulan bağlantıları ve varlıkları hızlı bir şekilde keşfeder. Bu da kötü amaçlı aktörler tarafından ele geçirilmeden önce güvenlik kapılarının ve diğer arka kapıların geçilmesini önler.

• **Segmentasyonu Yapılmamış Sistemlerin Güvenliğinin Sağlanması.** Daha önce bahsedilen segmentasyonu yapılmamış yönetim uygulamaları, güvenlik duvarları ile korunmayan sistemler oldukları için anormal aktivitelere karşı sürekli olarak izlenmektedir.

Sağlanan faydaların özeti:

• Yatırımın faydasını en üst seviyeye çıkaran etkili segmentasyon
• Bütüncül bir çözüm sağlayarak ek ve güvenlik duvarı ile ilgili olmayan saldırı vektörlerini kapsar
• OT işlemleri ile sıkı ilişki ve minimum müdahale
• Görünürlük alma ve kör noktaları tutmak yerine 1. Günden itibaren Risk Düzeyini düşürür
• Dağıtım aşamasından sonra dinamik bozulma etkisini kontrol eder ve kritik olaylara ilişkin riski düşürür
• Güvenlik duvarı ile segmentasyonu yapılmamış olan uygulamaların trafiğini izler

NEW YORK,462 W Broadway New York, NY 10012, ABD +1-646-475-2173
MÜNİH, Schellingstr. 109a80798 Münih Almanya +49-322-2109-7564

TOKYO, Clip Nihonbashi, 3-3- 3 Nihonbashi Honcho
Chuo - ku, Tokyo 103-0023, Japonya +81- 3-4588-5432

İrtibat: info@scadafence.com © 2019
www.scadafence.com

SCADAfence Platformunu Ağ Segmentasyon Projesinde kullanma adımları

Bahsedildiği üzere, SCADAfence Platformu segmentasyon projesinin planlanması için kullanılır, bu sayede hem proje süresi hem de dolayısıyla maliyeti azalır ve daha sıkı bir segmentasyon çözümü sunulur.

Segmentasyon projesinin bir parçası olarak aşağıdaki adımları izleyin:

• Ağ trafiğinin analiz edilmesini sağlamak için sistemi ağa bağlayın - varlık envanteri ve ağ bağlanabilirliği haritaları otomatik olarak oluşturulacaktır.
• Hangi Alt Ağların mevcutta kullanımda olduğunu görmek için Alt Ağ Topoloji Haritasını kullanın. Alt ağların tümünü gördüğünüzden emin olun.
• Maruziyet haritasını kullanın ve uygulamalar, OT işlemleri ve siteler arasındaki trafiği anlamak adına gruplar arasındaki bağlantı düzeyini araştırın.
• OT işlemi ile ağ trafiği ilişkilendirmek ve iletişimin mahiyetini hızlı bir şekilde anlayabilmek için otomatik varlık envanterini (otomatik olarak tespit edilen cihaz rolleri de dahil) kullanın.
• Gerçek ağ trafiğine dayanarak bir güvenlik risk değerlendirmesi yapmak için Tehdit Değerlendirme görüntüsünü, Maruziyet Haritasını ve Güvenlik Raporlarını kullanın.
• Giden bağlantıları tespit etmek için Maruziyet Haritasını ve İnternet bağlanabilirliği ile ilgili dahili uyarıları kullanın. Aşağıdaki hususları inceleyin: A. bu bağlantıların yetkili bağlantılar olup olmadığını. B. Çevre/güvenlik duvarı kesişme noktalarını aşan bağlantıların tespit edilmesi.
• Alt ağlar arasındaki bağlanabilirliği tespit etmek için Ağ Maruziyet Haritalarını kullanın. Bunlar arasında iletişim gerektirmeyen alt ağlar farklı segmentlere ayrılmalıdır.
• Son olarak, her bir alt ağ için hangi alt ağlar ile iletişim kurulması gerektiğine karar verin. Bağlanabilirliği mümkün olduğunca sınırlandırmaya çalışın ve bağlanabilirliğe izin vermeniz durumunda izin verilen durumu sınırlandırın.
• İşlem sonucunu segmentasyon kılavuzu olarak kullanın.
• Dağıtım aşamasından sonra, segmentasyonun başarılı olduğundan ve koruma düzeyinin iyileştirildiğinden emin olmak için aynı yöntemi kullanın.
• Dağıtım aşamasından sonra, güvenlik durumundaki herhangi bir bozulmayı tespit etmek ve güvenlik olaylarının önüne geçmek adına sistemin anormal trafik, yeni cihaz ve yeni bağlantı uyarılarını kullanmaya devam edin.

NEW YORK,462 W Broadway New York, NY 10012, ABD +1-646-475-2173
MÜNİH, Schellingstr. 109a80798 Münih Almanya +49-322-2109-7564

TOKYO, Clip Nihonbashi, 3-3- 3 Nihonbashi Honcho
Chuo - ku, Tokyo 103-0023, Japonya +81- 3-4588-5432

İrtibat: info@scadafence.com
www.scadafence.com