SCADAfence

Value-Added Distributor
OTD BİLİŞİM
www.onlineteknikdestek.com

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

Teknik Tanıtım Belgesi

SCADAfence ile Ağ Segmentasyonunun Basitleştirilmesi

OT Ağ Segmentasyon Zorlukları

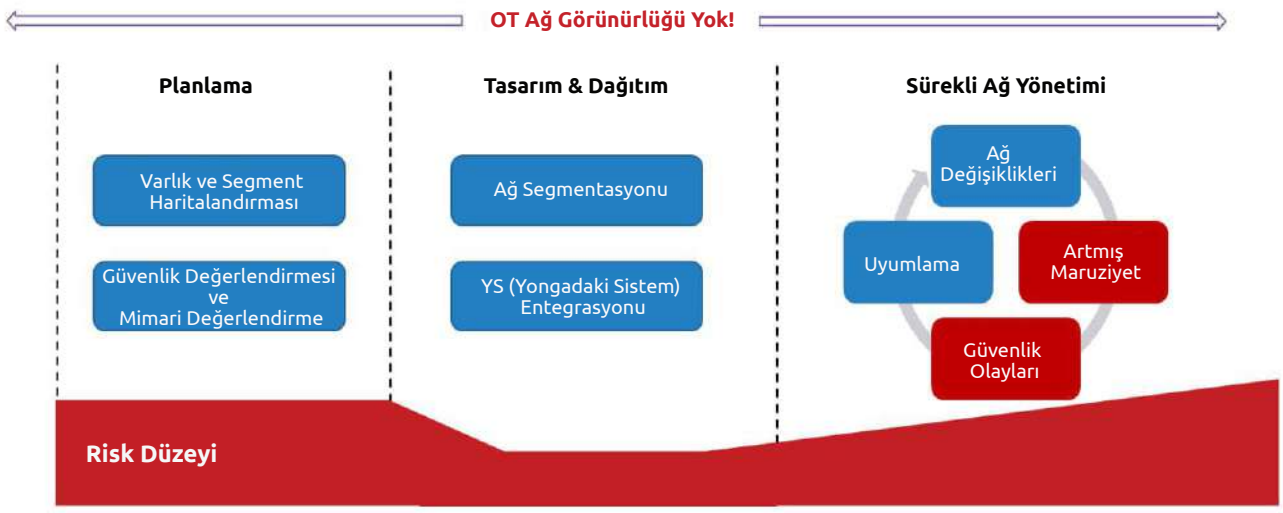
Çok da uzak olmayan geçmişte, yaşamsal sistemler dış tehditlerden asıl olarak anlamı diğer ağlar ve İnternet ile etkileşimi engellemek için sistemlerin iletişimlerini kesmek olan "hava aralığı" aracılığıyla korunurdu.

Bugün, 4. sanayi devriminin ortasında, artan bağlanabilirlik düzeylerinin hava aralığının ilgisini tamamen ortadan kaldırarak kurumları güçlendirmesi ve hala rekabet eder halde tutması gerekmektedir.

Artan bağlanabilirliğe yönelik bu trend, OT ağlarını savunmasız hale getirerek bir dizi yeni saldırı vektörlerine maruz bırakmaktadır. Bu riskleri hafifletmek adına, kurumlar ağ segmentasyonunu uygulamak için güvenlik duvarı teknolojilerini kullanmaktadırlar.

Meşgul iç OT ağlarında segmentasyon işlemi bilinen BT Sınır koruma yöntemlerinden farklıdır. Bağlantıların aralığı ve karmaşıklığı çok daha yüksektir ve üretim süreçlerinin önem düzeyi kurum sınırından geçen günlük ofis trafiğinden çok daha fazladır. Bu durum özellikle çok sayıda güvenlik duvarı dağıtıldığında ve mikro segmentasyon hedeflendiğinde ortaya çıkar.

Uygun şekilde yapıldığında segmentasyon OT ağlarının 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 Segmentasyonu 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.

NEW YORK, 462 W Broadway New York, NY 10012, ABD +1-646-475-2173

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

MÜNİH, Schellingstr. 109a80798 Münih Almanya +49-322-2109-7564

İrtibat: info@scadafence.com

Dağıtım Sürecindeki Zorluklar

Görünürlük Eksikliği Nedeniyle Yüksek Risk. Segmentasyon projeleri genel olarak birkaç ay, hatta daha uzun sürer. Bu projeler genel olarak analiz, planlama ve dağıtım aşamalarını kapsar. Bu süre içerisinde, OT ağının görünürlüğü kaybolur ve uygun güvenlik sağlanamaz. Günümüzün dinamik ortamında bu, ağın maruz kalacağı ve ortaya çıkacak kritik güvenlik olaylarına ilişkin çok uzun bir süre demektir.

Etkisiz Dağıtım. Güvenlik duvarları iç meşgul ağlara dağıtılırken, güvenlik duvarları tehlikeli trafiğin tamamını "göremeyebilirler". Uzaktan bağlantılar veya dolandırıcı cihazlar mevcut olabilir ve güvenlik duvarında görünmeden güvenlik duvarını aşabilir. Bazen, dağıtım lokasyonu uygun şekilde seçilmez, çünkü farklı bir ağ kesişme noktası çok daha etkin olabilir. Bu senaryolar güvenlik ekibinin gerekli koruma düzeyi yetersizken yanlış bir güvenlik algısına sahip olmasına neden olur.

İş süreçleri ile karşılıklı ilişki eksikliği. Güvenlik duvarları gördükleri IP adresi ile cihazın OT sürecindeki rolleri arasında karşılıklı bir ilişki kurmaz. Birçok IP'si ve uygulama trafik türü bulunan dahili ağlarda, bu durum trafik örüntülerini anlamada sayısız manuel (ve uzun süreli) iş yüküne sebep olabilir. Bu karşılıklı ilişki eksikliği önemli süreçlerin yanlışlıkla engellenmesine sebep olabilir veya diğer bir yandan gereksiz portlar açabilir ve ağa aşırı maruziyet yaratabilir.

Bu da segmentasyon teknolojilerindeki yatırımı etkisiz hale getirir ve en nihayetinde yüksek risk düzeyi teşkil eder.

Sağlanan Faydaların Özeti

• Yatırımın faydasını (YF) en üst seviyeye çıkarak etkili segmentasyon.

• Bütüncül bir çözüm sağlayarak ek ve güvenlik duvarı ile ilgili olmayan saldırı vektörlerini kapsar.

OT işlemleri & sıkı ilişki ve minimum müdahale.

1. günden itibaren tam görünürlük ve risk azaltımı ve uzun süreler boyunca kör nokta oluşturmama özelliği.

• 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

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

MÜNİH, Schellingstr. 109a80798 Münih Almanya +49-322-2109-7564

İrtibat: info@scadafence.com

Dağıtım Sürecindeki Zorluklar

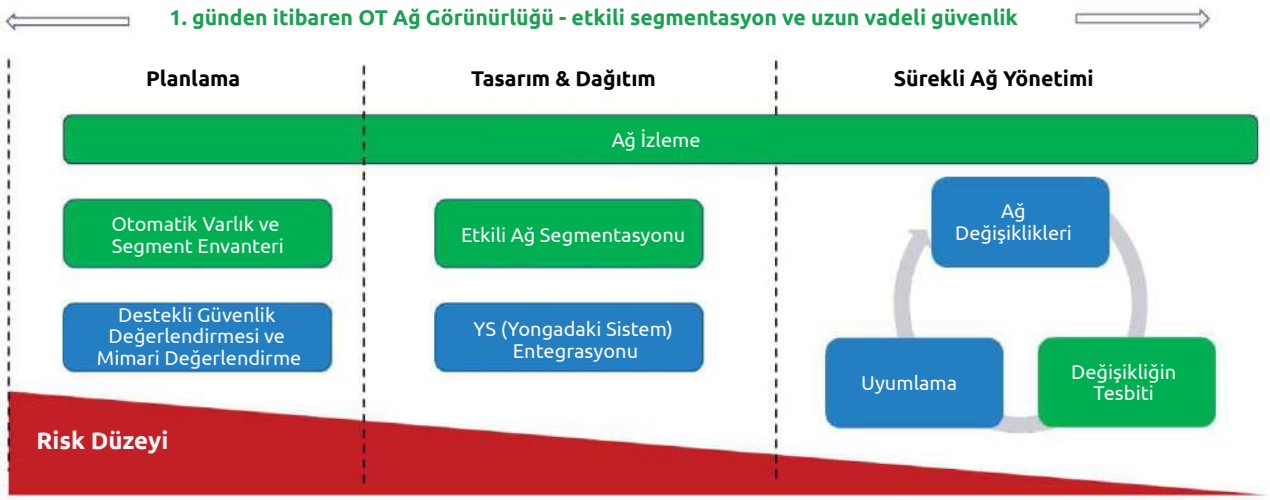
• **Zamanla Bozulma.** Ağ segmentasyonu ağ değişiklikleri, politika ihlalleri ve insan hatası nedeniyle zamanla "bozulur". Ağa yeni sistemler eklenir ve mevcut yapılandırmalar ve politikalar güvelik politikasında "boşluklar" yaratarak dinamik olarak evrilir.
Bu da segmentasyon projesi ile düşürülen risk 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 sağlayıcıların personel üyeleri için arka kapılar oluşturulur, bu da ardında yeni saldırılara kapı açar. Kontrolsüz ve yetkisiz 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 bulaşmalar verilebilir.
OT ağlarının güvenliğini sağlamak için OT ağlarının güvenlik duvarı dışında başka araçlar ile izlenmesi gerekir.

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

Sürekli İzleme & 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: Etkili Segmentasyon ve Uzun Vadeli Güvenlik

NEW YORK, 462 W Broadway New York, NY 10012, ABD +1-646-475-2173

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

MÜNİH, Schellingstr. 109a80798 Münih Almanya +49-322-2109-7564

İrtibat: info@scadafence.com

Segmentasyon Projesi Sırasında Zorlukların Ele Alınması

• **Segmentler Arasındaki Trafiğin Sanallaştırılması.** SCADAfence Platformu tüm ağ segmentlerini haritalandıran bir "Segmentler Haritası" ve mantık grupları arasındaki ve farklı ağ kısımları arasındaki trafik örüntülerini gösteren bir "Maruziyet Haritası" sunar. Ek otomatik trafik analizi görüntülemeleri kullanıcıya içgörü ve uygulama davranış ve gereklilikleri sağlar. Bu sayede, trafikteki sınırı / ağı aşma girişimleri anında tespit edilir.

Bu aynı zamanda ilgili ağ trafiğinin tamamının tespit edilmesini ve segmentasyon işleminin etkili bir şekilde yapılmasını sağlar.

• **Otomatik Varlık Envanteri ve OT Prosesi ile Karşılıklı İlişkisi.** SCADAfence Platformu ulusal endüstriyel protokolleri kullanarak rolleri ve uygulama aktiviteleri de dahil olmak üzere ağ içerisindeki tüm varlıkları keşfeder ve haritalandırır. Bu da birçok ağı, iletişim yönü ve önemli endüstriyel uygulamaya sahip olan dahili OT ağlarındaki segmentasyon kurallarının daha doğru ve etkili olmasını sağlar.

• **Otomatik Risk Değerlendirme Raporu.** SCADAfence Platformu önemli 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.

•**Birinci Günden İtibaren Riskin Azaltılması -** Ağı izleyen, tam görünürlük sağlayan ve herhangi bir anormal aktivite veya politika sapmasına ilişkin uyarılar veren SCADAfence Platformu anında risk azaltımı sağlar. Ayrıca, risk azaltımı tüm güvenlik mekanizmaları uygun olana kadar aylarca ertelenmez, bu sayede ağ güvenlik olaylarına maruz kalmamış olur.

Dağıtımdan Sonra 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. Bunların tümü segmentasyon teknolojileri tarafından basitçe tespit edilemeyebilir. SCADAfence Platformu ağın güvenliği ve sağlığına dair net bir resim sunar ve her türlü değişikliğe ve politika ihlallerine ilişkin uyarı bildirimleri gönderir.

Bir sonraki güvenlik olayı ortaya çıktıktan sonra değil, çıkmadan önce uyumlama yapılmış olur. İzleme ayrıca siber saldırı ve kötü amaçlı yazılım bulaşmaları riskini düşürür ve potansiyel olayları halletmek için gereken 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.

NEW YORK, 462 W Broadway New York, NY 10012, ABD +1-646-475-2173

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

MÜNİH, Schellingstr. 109a80798 Münih Almanya +49-322-2109-7564

İrtibat: info@scadafence.com

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

SCADAfence Platformu Bir Ağ Segmentasyon Projesinde Nasıl Kullanılır?

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

Başarılı bir segmentasyon için aşağıdaki adımları uygulayın:

• 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 trafiğini ilişkilendirmek ve iletişimin mahiyetini hızlı bir şekilde anlayabilmek için tasarlanan otomatik varlık envanterini (otomatik olarak tespit edilen cihaz rolleri de dahil) kullanın.

• 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 durumları doğrulamanız gerekmektedir:
A. Bu bağlantıların yetkili bağlantılar olup olmadığı.
B. Bağlantıların sınırı/güvenlik duvarı kesişme noktalarını aşıp aşmadığı.
Alt ağlar arasındaki bağlanabilirliği tespit etmek için ağ haritasını kullanın. Bunlar arasında iletişim gerektirmeyen alt ağlar segmentasyon projesinin bir parçası olarak ayrılmalıdır.

• Her bir alt ağ için hangi alt ağlar ile iletişim kurulması gerektiğine karar verin. Bağlanabilirliği mümkün olduğunca sınırlandırmaya çalışın ve bağlanabilirliğe izin verilmesi durumunda izin verilen durumu sınırlandırın.

• İşlem sonucunu segmentasyon kılavuzu olarak kullanın.

• Segmentasyon projesinden sonra, segmentasyonun başarılı olduğundan ve koruma düzeyinin zaman içerisinde korunduğundan emin olmak için aynı yöntemi kullanın.

• Segmentasyon projesinden sonra, güvenlik durumundaki herhangi bir bozulmayı tespit etmek ve güvenlik olaylarının önüne geçmek adına sistemin anormal trafik, yeni cihaz ve yeni bağlantı uyarılarını kullanın.

NEW YORK, 462 W Broadway New York,
NY 10012, ABD +1-646-475-2173

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

MÜNİH, Schellingstr. 109a80798
Münih Almanya +49-322-2109-7564

İrtibat: info@scadafence.com

SCADAfence Hakkında

SCADAfence OT & IoT siber güvenliği alanında global bir teknoloji lideridir. SCADAfence sınıfının en iyisi ağ izleme, varlık keşfi, yönetim, uzaktan erişim ve IoT cihaz güvenliği sağlayarak büyük ölçekli ağlar sunan geniş kapsamlı endüstriyel siber güvenlik ürünleri sunar. 2020 yılında Gartner "Cool Vendor" ödülüne layık görülen SCADAfence, Avrupa'daki en büyük üretim tesisi de dahil olmak üzere dünyanın en karmaşık OT ağlarının bazılarına güvenlik ve görünürlük hizmeti sunar. SCADAfence kritik altyapı, üretim ve bina yönetimi sektörlerinde faaliyet gösteren kurumların güvenli, güvenilir ve verimli bir şekilde çalışmalarını sağlar. Daha fazla bilgi almak için www.scadafence.com adresini ziyaret edebilirsiniz.

NEW YORK, 462 W Broadway New York,
NY 10012, ABD +1-646-475-2173

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

MÜNİH, Schellingstr. 109a80798
Münih Almanya +49-322-2109-7564

İrtibat: info@scadafence.com