SCADAfence

Value-Added Distributor
OTD BİLİŞİM
www.onlineteknikdestek.com

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

Tanıtım Belgesi

Güç Dağıtım Ağlarının Güvenliğinin Sağlanması

Giriş

Toplum olarak elektriğe bağlı yaşıyoruz. Evlerimizde ışığı açmaktan, multi milyon dolarlık bir üretim ekipmanı kullanmaya ve milyar dolarlık kritik altyapı sistemleri işletmeye kadar elektrik çalışma ve yaşama biçimimizi birbirine bağlayan temel bir unsurdur. Elektrik gücü dağıtım ağlarının bozulması önemli sağlık, ekonomik ve çevresel hasarlara sebep olabilir.

Son yıllarda, dünya çapında yaygınlaşan siber saldırılar büyük nüfuslu alanlara sağlanan güç kaynağının bozulmasına sebebiyet vermiş, bu da büyük hasarlara neden olmuştur.

Bu siber saldırılara ilişkin örnekler arasında şunlar yer almaktadır; switchleri, kesicileri ve alt istasyon iletişim protokolleri hedef alan ve Ukrayna'nın güç şebekesinde ortaya çıkan hatanın ana sorumlusu olan Industroyer. Endüstriyel kontrol sistemleri üzerinden genel anlamda başarılı olan bilgi toplama girişimi ile yüzlerce kurumu etkileyen kötü amaçlı yazılım Dragonfly. Hastanelerin, bankaların ve üniversitelerin faaliyetlerini etkileyen bir fidye yazılımı solucanı WannaCry. Nükleer tesislerin kontrolünü ele geçiren ve İran'ın Natanz uranyum zenginleştirme tesisindeki çok sayıda santrifüjü tahrip eden bir bilgisayar solucanı Stuxnet. Endüstriyel kontrol sistemlerindeki SCADA uygulamalarına karşı hizmeti engelleme saldırıları başlatmak üzere tasarlanan BlackEnergy ve enerji, yağ ve gaz kontrol sistemlerinde kullanılan ekipmanlara saldırıda bulunan kötü amaçlı bir yazılım Trisis.

Ulusal Güvenlik Ajansı (NSA), teknik olarak açıkça "ABD güç şebekelerini, su sistemlerini ve diğer önemli altyapı şebekelerini işleten kontrol sistemlerini ele geçirme" kabiliyetine sahip kurumlarca ICS'ye izinsiz girişler rapor etmiştir. 1
Ancak, güç dağıtım kurumlarının sürekli olarak OT ağları ve diğer ağlarının bağlanabilirliğini artırmaları gerekir. Daha kesin ve etkili bakım ve daha hızlı olay müdahalesi için merkezi kontrol odaları ve uzak alt istasyonlar (daha önce yüksek oranda segmentasyonu yapılmış) arasında daha fazla bağlantı kurulmasını gerektirir. Güç dağıtım ağlarının şu anda organizasyonel sistemlerle daha fazla bağlantısı vardır ve uzaktan erişim bağlantısı daha önce hiç olmadığı kadar fazladır.

Bu kötü amaçlı yazılım veya fidye yazılımı bulaşması olup olmadığı veya saldırıların iyi organize olmuş hacker grupları veya ulusal tehdit aktörleri tarafından dikkatli bir şekilde hedeflenip hedeflenmediği önemli olmaksızın bu artan bağlanabilirlik, sonuç olarak güç dağıtım ağlarının güvenlik olaylarına karşı daha hassas olmasına neden olmaktadır.

ABD Enerji Bakanlığı'na göre, "Saldırı tespit sistemlerinin (IDS) ve BT ve OT ağları izleme çözümlerinin yokluğu, yazılımların siber saldırılara ilişkin adli verileri alamayacağı anlamına gelmektedir. Tüm yazılımlarda minimum siber güvenlik prosedürü olarak saldırı tespit ve izleme araçlar bulunmalıdır."

https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf (Page 6)

https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf (Page 33)

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

Güç Dağıtım Ağlarına İlişkin Güvenlik Problemleri

Böylesi büyük, önemli ve dağılmış ağları korurken, ele alınması gereken birçok özel problem ve gereklilik bulunmaktadır.

1. Uzak Varlıklı Büyük Dağılmış Ağlar

Güç dağıtım ağları dağılmış ve genellikle uzaktan mürettebatsız bölgelerde kullanılan büyük ağlardır. Bu, segmentasyon yetersizliği, yanlış yapılandırmalar, yetersiz yönetim ve iletişim problemleri ile kategorize olan risklere meyilli oldukları için tehdit aktörleri için potansiyel ilgi çekici giriş noktaları olabilecek birçok hareketli bölüme sahip oldukları anlamına gelir. Ayrıca, çevre güvenliği tüm ağ giriş noktalarını kontrol edemez ve geçilmesi halinde saldırganlar çok sayıda varlığa erişebilir ve uzun süre tespit edilmeden kalabilir.

2. Kötü Amaçlı Yazılım ve Fidye Yazılımı

Sayıları giderek artan kötü amaçlı yazılım ve fidye yazılımı olayları dünya genelindeki kurumları hedef almaktadır. Genellikle BT'de ortaya çıkar ve OT ağlarına yayılır, büyük maddi ve operasyonel hasarlara sebep olurken, aynı zamanda OT ağlarını ve OT destekleme işlemlerini felç eder. Ayrıca, bazı endüstriyel ve elektriği hedef alan saldırılar (örn. Aralık 2016'da Ukrayna'nın elektrik şebekesini vuran Industroyer yazılımı) enerji üretim ve dağıtım süreçlerini zayıflatmak için tehdit aktörleri tarafından özel olarak tasarlanmaktadır.

3. Güvensiz İletişim Protokolleri (ICS)

ICS ağları genelinde kullanılan iletişim protokolleri ayrıca dikkat edilmesi gereken bir husustur. Güç sisteminin tamamında kullanılan Modbus ve DNP3 gibi yaygın ve uzun süredir kullanılan ICS protokollerinde güvenlik önlemleri çok azdır veya hiç yoktur. Doğrulama işlevleri yetersiz olan bu mesajlar engellenebilir, gizlenebilir veya değiştirilebilir, dolayısıyla operasyon ortamında tehlikeli bir olaya sebep olabilir.

4. Zayıf Cihazlar

Programlanabilir mantık denetleyiciler (PLC) gibi birçok otomasyon elemanı mikro işlemciler aracılığıyla çalışır ve fonksiyona özel yazılım programları içerir. Aynı zamanda ağ yolları üzerinde yönetim ve iletişim işlevlerine de sahiptir. Bu tür cihazlar kontrol sistemine erişebilme aracı olarak siber saldırıların ana hedefidir.

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

5. Uzaktan Erişim Bağlantıları

Coğrafi olarak yaygın olan varlıkları yönetmek, uygunluğu sağlamak ve maliyetleri azaltmak için, güç dağıtım kurumları (diğer birçok kurum gibi) uzaktan erişilebilen ekipmanlara ve mobil cihazlara giderek daha çok ihtiyaç duymaktadır. Ancak, uzak araçlar ve cihazlar ile önemli sistemlere güvensiz erişim veya bağlantıdan kaynaklanan güvenlik açıkları ciddi güvenlik olaylarına ve ağ problemlerine sebebiyet verebilir.

6. Üçüncü Taraf Hizmetler

Bazı ICS ekipmanı sağlayıcıları sağlayıcı bakım politikaları nedeniyle cihazlara veya yazılımlara erişmek için kasti veya kasıtsız "arka kapılar" oluşturulması veya parola değiştirme veya onaylanmamış güvenlik paketleri yükleme gibi fabrika ayarları ile yeniden yapılandırılmışsa ekipman garantilerini geçersiz hale getirme gibi istemsiz olarak siber güvenlik problemleri yaratabilmektedir.

7. Akıllı Şebekeler

Akıllı şebekeye geçiş, kullanılan yazılımların operasyonlarına on binlerce yeni cihaz ekleyeceği anlamına gelecektir ve bu cihazlar arasında yeni sensörler, kontrolörler, röleler, sayaçlar ve diğer benzer cihazlar yer almaktadır. Bu cihazların birçoğu BT ağına, İnternete ve halka maruz kalacaktır, bu maruziyet de yeni iletişim protokollerinin geliştirilmesine sebep olacaktır.

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

Güç Dağıtım Ağlarına yönelik Bir Güvenlik Çözümünün Değerlendirilmesi

Güç dağıtım ağlarına yönelik bir güvenlik çözümünü değerlendirildiğinde, çözüm aşağıdaki kriterleri karşılamalıdır:

1. Özel Güç Dağıtım Ağı Mimarisine Uygundur:

Uzak bölgeler ile ana veri merkezleri arasındaki iletişimler zaman zaman sınırlanabilir ve stabil olmayabilir. Seçtiğiniz çözüm güvenli bir şekilde çalışmak için büyük bant genişliği gerektirmezken yerel veri analizi ve depolamasını desteklemelidir.

2. Doğrudan Eylem Maddeleri ile Net Bildirimler Sağlar

Ekipman bölgede uzak bir yerde bulunabileceğinden ve mürettebatsız çalışabileceğinden, uzak lokasyonlarda gereksiz ziyaretlere ihtiyaç duyulmaması açısından güvenlik çözümünün merkezi kontrol odalarına net ve doğrudan bildirimler göndermesi önemlidir.

3. Düşük Maliyetlidir

Çok sayıda önemli uzak bölge için çok sayıda sensör kullanımı satın alma ve bakım açısından pahalı bir yük teşkil eder. Güç dağıtım ağlarının yalnızca ilk satın alma işlemi için değil, aynı zamanda uzun vadeli bakım çalışmaları için de uygun maliyetli bir güvenlik çözümüne ihtiyacı vardır.

4. Yönetmelikleri ve Uygunluk Gerekliliklerine Dikkat Eder

Bu güvenlik çözümünün NERC-CIP ve diğer yönetmelikler gibi güç dağıtım ağlarına ilişkin yönetmeliklere uygun olması ve uygunluğu sağlaması gerekir.

5. Gelecekteki Değişikliklerden Etkilenmeyen Bir Güvenlik Sağlar

Güvenlik çözümü aynı zamanda gelecekte sistemler ekleyerek veya akıllı şebeke teknolojilerine geçilerek getirilen çok sayıda cihaz, teknoloji ve protokole yönelik ölçülebiliyor olmalıdır.

6. Pahalı Mimari Değişiklikler Gerektirmez

Son olarak, güvenlik çözümünün üretim süreçlerini engellememesi ve alt istasyonda veya merkezi ağ mimarilerinde mimari değişiklikler gerektirmemesi önemlidir. Aynı zamanda, güvenlik çözümü mevcut izleme ve güvenlik yönetim araçları ile entegre olmalıdır.

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 Platformu ile Güç Dağıtım Ağlarının Güvenliğinin Sağlanması

SCADAfence Platformu, güç dağıtım ağlarındaki ağ varlıklarının tam görünürlüğünü ve günlük işlevlerinin sorunsuz bir şekilde yapılmasını sağlar. Anormal ve yetkisiz davranışların gerçek zamanlı olarak tespit edilmesini sağlar. SCADAfence Platformu aynı zamanda güvenlik duvarı ve antivirüs yazılımları gibi diğer güvenlik araçlarının "kapsamadığı" güvenlik senaryolarını da kapsar. Dış ve iç saldırı düzenleyicileri ele alır. Güvenlik mekanizmaları, kötü amaçlı yazılım ve fidye yazılımı aktivitesi, yanlış yapılandırma ve her türlü hackleme girişimi gibi durumlarda uyarılar verir (hedeflenmiş olup olmadığı önemli olmaksızın).

Kurulum süreci operasyonel ağı aksaklığa uğratmaz ve sistem algoritmaları kullanıcıdan herhangi bir zahmetli girdi alınmadan otomatik olarak yapılandırılır.

Güç Dağıtım Ağlarının Güvenlik Problemlerinin Ele Alınması

Sistemin kötüye kullanılmasını veya bir siber saldırı hedefi haline gelmesini önlemek için güç dağıtım ağlarının sürekli olarak izlenmesi gerekir. Ayrıca, iç hizmet bozulmaları, ekipman hataları ve aktivasyon bekleyen etkisiz kötü amaçlı yazılımlar gibi uygunluk ile ilgili sorunlar da önemlidir ve düzenli olarak izlenmelidir.

SCADAfence Platformu ağ trafiğini analiz eder ve aşağıdaki saldırı senaryolarını ele alır:
• Yanlış yapılandırılmış çevre cihazlar veya 'güvenlik duvarı etrafındaki' rotalar ile dış ağ erişimi.
• Bilinmeyen kötü amaçlı yazılımlar ve fidye yazılımları kolaylıkla güvenlik duvarını ve anti virüs çözümlerini aşabilir.
• Bilinen kötü amaçlı yazılım ve fidye yazılımı ayrıca AV sınırlandırmaları veya uç noktalara ajan kurulumu nedeniyle enfekte cihazlar veya USB cihazları aracılığıyla ağa içeriden bulaşabilir.
• Yetkisiz uzaktan erişim veya yetkisiz erişim eskalasyona imtiyaz tanır.
• İçerideki OT ağ tavizini ima edebilecek şüpheli trafik.
• Önemli OT ekipmanlarına doğrudan erişim ve genellikle endüstriyel protokol düzeyinde saldırıları içeren üretim süreci manipülasyonu.
• Yetkili istasyonlardan, giriş kapılarından, yetkisiz kablolu ve kablosuz yönlendiricilerden gelen BT-OT yayılımı.
• İnsan hatası/yanlış yapılandırma veya servis veya donanım hatalarına sebep olan operasyonel sorunlar.

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

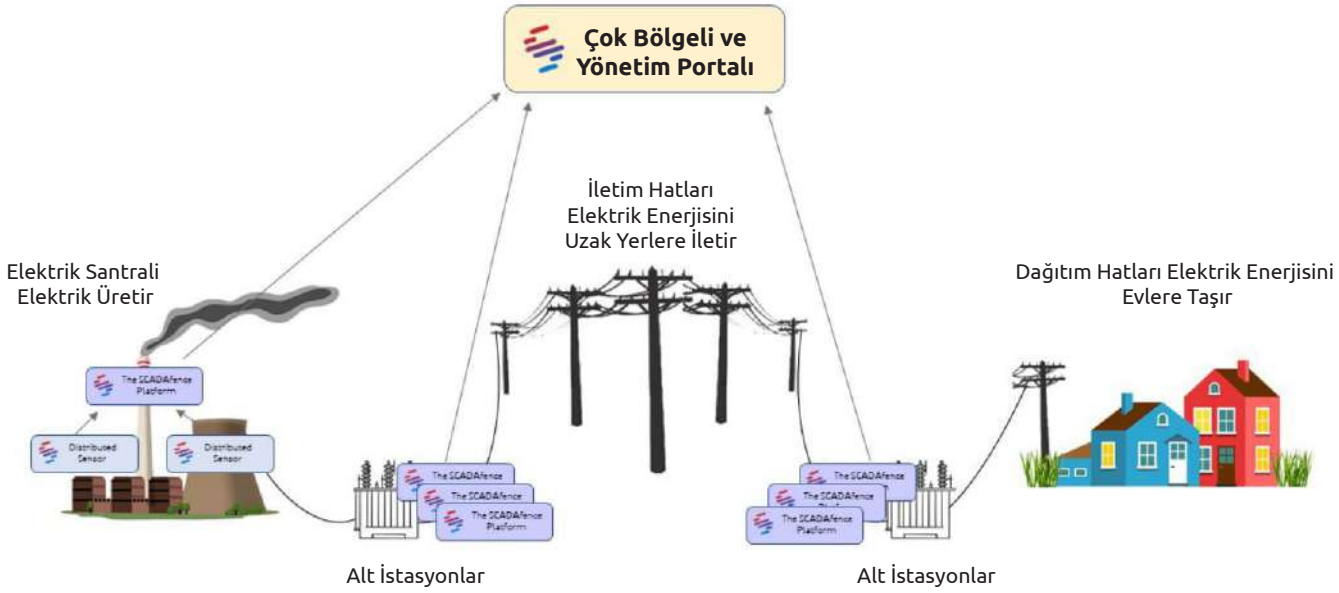
TOKYO, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Tokyo 103-0023, Japonya +81-3-4588-5432

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

İrtibat: info@scadafence.com

Ölçeklenebilir Mimari

SCADAfence Platformu bir veya birden fazla hiyerarşik modelden oluşan çoklu mimari modelleri destekler ve küçük veya çok büyük sayıdaki alanı ve izleme noktasını yönetmeye uygundur. Bu uzak sensörler yerel trafik analizini gerçekleştirir.



Şema #1: SCADAfence Platformunun Çok Katmanlı Mimarisi

Düşük Maliyetli Dağıtım

SCADAfence Endüstriyel DPI Sensörleri performans düşüklüğüne sebep olmadan on binlerce cihaz için hizmet vererek yüzlerde dağılmış durumu ölçebilir.

SCADAfence Platformu aynı zamanda özel bir "NetFlow Analyzer" özelliği ile birlikte tasarlanmıştır. Bu özelliği kurumların her bir segmentte pahalı sensörleri kullanmayı bırakmasını sağlar, dolayısıyla kullanıcıların uzak segmentleri "aracısız" ve uygun maliyetle izleyebilmesine olanak tanır. Bu işlem, NetFlow verilerini SCADAfence sensörüne göndermek için ağ altyapısı desteği yapılandırılarak gerçekleştirilir. SCADAfence Platformunun yüksek performanslı işlevlerinin kombinasyonu, NetFlow Analyzer ile birleştiğinde büyük dağılmış ağların güvenliğini sağlamanın yanında daha küçük ve uzak ağ segmentlerini de kapsamanın elverişli ve uygun maliyetli bir yolunu sunar.

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

Kesintisiz, Mevcut Mimariye Entegre Olma

SCADAfence Platformunun varsayılan modu kesintisiz bir çözüm olarak çalışmaktadır, dolayısıyla üretim sürecine herhangi bir etkisi yoktur. Üretimde aksaklığa sebep olmaz veya uzun bakım süreleri gerektirmez. Daha ayrıntılı varlık verisinin toplanması için aktif mod mevcuttur.

Ayrıca, SCADAfence Platformu SIEM veya Olay Yönetim sistemleri gibi merkezi güvenlik yönetim sistemleri ile entegre olacak şekilde tasarlanmıştır ve güvenliğin ve OT ağının dayanıklılık mimarisinin ayrılmaz bir parçasıdır.

Derin Paket Analizi

SCADAfence sensörü her bir bölgede RTU, IED, akıllı sayaç ve aktüatör gibi varlıkları keşfedecek ve izleyecektir. Sensör bölge varlıklarını otomatik olarak keşfedecek, DNP3, IEC-104, MMS ve GOOSE gibi endüstriyel trafik de dahil olmak üzere ağ trafiğinin DPİ işlemini yapacak ve siber güvenlik ve operasyonel olaylara ilişkin uyarılar verecektir.
SCADAfence Platformu aynı zamanda yerel varlıkları kurcalama girişimlerine dair uyarılar verecek, kritik altyapı bileşenlerini kapatacak ve ağ cihazlarına yönelik yetkisiz OT komutları başlatacaktır.

Doğru Tespit ve Minimum Yalancı Pozitiflik

SCADAfence'in Mikro Granüler Taban Çizgisi varlık ve trafik özelliklerine göre granülerdir. Bu özel taban çizgisi, taban çizgisinin yapılandırılmasına veya değişiklik yapılması halinde yeniden yapılandırılmasına gerek duyulmaksızın en doğru tespit mekanizması sunacak şekilde tasarlanmıştır.

SCADAfence'in Mikrogranüler Taban Çizgisi aşağıdaki gibidir:

Yalancı Pozitiflik Uyarılarını Azaltır - Granüler ve adaptif taban çizgisi sistemin kullanılabilir ve güvenilir olmasını sağlayarak yalancı pozitiflik uyarılarının sayısını azaltır. Ağ ne kadar büyük olursa, olayların sayısı da katlanarak artar, dolayısıyla sorunu kritik bir sorun haline getirir.

Uyumlama ve Kullanıcı Yapılandırması Gerektirmez - SCADAfence Platformu ağ içerisinde hızlıca ve kolaylıkla dağılabilir. Uzun süreli analizler ve uzman uyumlaması yapılmasına gerek yoktur.

Yeniden Yapılandırma ve Başlatma Gerektirmez - Taban çizgisi adaptif olduğundan ve düzenli bir şekilde ayarlandığından, sistemi uzun süre kullanılamaz hale getiren ve ağ maruziyetini ve riskleri artıran çalışmalara, uzun süreli durdurma/yeniden başlatma işlemlerine ve yeniden öğrenme adımlarına ihtiyaç duyulmaz.

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

Yönetim ve Uygunluk

SCADAfence Yönetim Portalı güvenlik yönetiminin başka bir yenilikçi katmanını oluşturur. Portal, BT ve denetim departmanlarının kurumun şirket politikalarına ve NERC-CIP ve NIST çerçevesi, iç politikalar ve en iyi uygulamalar gibi OT ile ilgili standartlara ve yönetmeliklere bağlılığını merkezi olarak tanımlamasını ve izlemesini sağlar.

Bilgi Teknolojilerinden Sorumlu Kişilerin (CISO) ağlardan alınan güncel verilere dayanarak organizasyonel uygunluklarını otomatik olarak raporlama ve ölçmenin yanı sıra, siber güvenlik stratejilerini planlamalarını sağlar.

SCADAfence Yönetim Portalı 3. taraf araçlara bağlanabilir ve merkezi bir organizasyonel uygunluk yönetim portalı olabilir.

SCADAfence'in NERC-CIP uygunluk çözümü hakkında daha fazla bilgi almak için buraya tıklayın.

Uzaktan Erişimli Kullanıcıların Güvenliğinin Sağlanması

SCADAfence Platformu uzaktan ağa erişen kullanıcılar arasında karşılıklı ilişki kurarak ekstra özel bir güvenlik katmanı ekler ve bu kullanıcıların OT ağındaki aktivitelerini takip eder. Anormal ve yetkisiz eylemleri tespit eder ve bunlara ilişkin uyarılar verir ve kullanıcı adı, esas çalışma istasyonu ve uygulama ile ilişki kurulmasını sağlar.

OT'de uzaktan erişim güvenliğinin nasıl sağlanacağı ile ilgili kısa bir demo videosu izlemek için buraya tıklayın.

Gelecekteki Değişikliklerden Etkilenmeyen Güvenlik

IoT cihazlarını ve protokollerini destekleyen ve büyük IoT filolarının yönetilmesi için en gelişmiş özelliklere sahip patent bekleyen bir teknolojiye sahip olan SCADAfence Platformu, gelecekteki büyümeyi ve Akıllı Şebeke teknolojilerinin kullanımını kolaylaştırmak için en iyi şekilde tasarlanmıştır.

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

SCADAfence

Value-Added Distributor
OTD BİLİŞİM
www.onlineteknikdestek.com

ICT
OTD
PREFER EXPERIENCE ONLINE
Since 2011