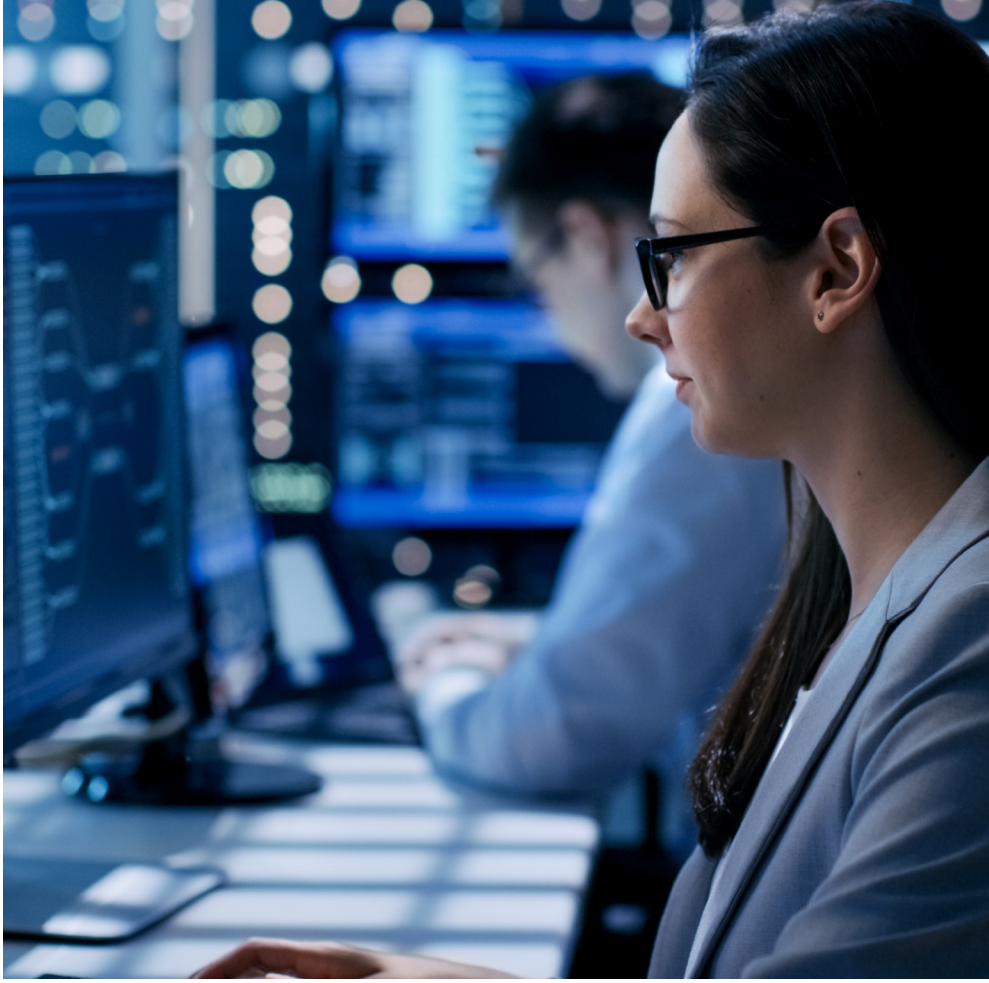
NOZOMI NETWORKS

CERRUS



BT Uzmanları için OT/IoT Güvenliği Kılavuzu

Dijital risk, CEO'dan son kullanıcıya kadar herkesin işidir. Yine de birçok kuruluşta, onu yönetmek ve en aza indirmekle görevli olan BT departmanıdır.

Gartner, 2023 yılına kadar kuruluşların %75'inin risk yönetimi programlarını yeni siber-fiziksel sistemleri ve birleşik BT, OT, IoT ve fiziksel güvenlik ihtiyaçlarını ele alacak şekilde genişleteceğini tahmin ediyor. Bugün %15'in altında.

Her şeyin bir IP adresine sahip olduğu ve dijital risk yüzeyinin katlanarak genişlediği bir dünyada, BT profesyonelinin işi daha zor ve acil hale geldi.

Günümüzde BT ekibi, yalnızca çalışanlar tarafından kullanılan çok sayıda kişisel bilgi işlem cihazının güvenliğini sağlamaktan sorumlu değildir. Endüstriyel Kontrol Sistemleri (EKS), Operasyonel Teknoloji (OT) sistemleri, siber-fiziksel sistemler ve BT, OT ve IoT cihazlarının bir kombinasyonu gibi kritik görev altyapısını yönetmekten ve korumaktan giderek daha fazla sorumlu hale geliyor.

Bu kılavuz ile:

BT ve OT ağları arasındaki **temel farkları** anlayın

Görev açısından kritik operasyonel ortamların ortaya çıkardığı benzersiz **güvenlik zorluklarını yönetin**

Risklerin bir adım önünde olmak için **birleşik görünürlük ve sistem**ler kullanın

Anormallikleri ve tehditleri tespit etmek için teknolojiden yararlanın ve otomasyon sistemlerini savunmak için **hızlı önlem alın**

BT ve OT Ağlarını Etkin Bir Şekilde Yönetmek

Daha Fazla Cihaz + Otomatik/Kritik Görev Sistemleri =

Katlanarak Artan Yüksek Risk

OT sorumluluğunun geniş kapsamı, BT uzmanları için yeni zorluklar yaratır. Bunlardan bazıları şunlardır:

- Geleneksel BT güvenlik araçlarının ve taktiklerinin OT, IoT cihazları ve ağlarını bozarak yeni yaklaşımlara ihtiyaç duyması riski,
- Güvenlik ve çevresel risklerin yanı sıra üretim ve hizmet çalışma süresine odaklanma.
- OT ağları için artan riskler, çünkü:
  - Birçok EKS cihazı, aksama ve arıza süresi riskleriyle ilgili endişeler nedeniyle değerlendirilemez, yükseltilemez veya yamalanamaz.
  - Çoğu OT ağı düzdür, standart ağ iyileştirme taktiklerini karmaşıklaştırır ve kötü amaçlı yazılımın kolayca yayılmasına izin verir.
  - Kurumsal BT ortamlarında olduğu gibi, EKS ağlarında uyumluluk gereksinimlerinin karşılanması SOP (standart işletim prosedürü) değildir.

BT ve OT Ağları: Temel Farklılıklar

Çoğu BT uzmanı, uzman sorun çözücülerdir. Kurumsal BT sorunlarını giderirken, genellikle bunu aktif olarak yaparlar - ping atarak, tarayarak, araştırarak (örneğin nmap çalıştırarak, vb.) ve tabii ki Googling. Artık kendilerini OT ağlarından sorumlu bulan BT uzmanları için zorluk, bu taktiklerin çoğunun artık çalışmamasıdır. BT ekibinin sorun gidermeye çalıştığı ağı bile çökertebilirler.

Aslında, tek bir ICMP paketi bir PLC'yi kolayca devre dışı bırakabilir. Ve PLC'nin sağladığı hizmete bağlı olarak kritik bir altyapı felaketi haline gelebilir. En nazik ping'ler bile bir EKS ağında bir Ping of Death'e dönüşebilir. Ve bu ağlar genellikle düz olduğundan ve yönlendirici ACL'leri veya güvenlik duvarları gibi filtreleme tıkanıklık noktaları içermediğinden, olası sorunlar hızla kontrolden çıkabilir.

Elbette, bir EKS sorunu üzerinde bir Google araması yapmak ağınızı çökertmeyecektir. Ancak kabul edelim - muhtemelen 10 veya daha eski dişliler için pek çok yararlı sonuç bulamayacaksınız.

Ama bekleyin... Peki ya IoT?

IoT cihazlarını yönetmek, hızla BT ekibinin sorumluluk kapsamının bir parçası haline geliyor. Görev açısından kritik olarak kabul edilsinler veya edilmesinler, kablosuz sensörler, yazıcılar, CCTV kameralar, akıllı TV'ler, kart okuyucular ve diğer cihazlar gibi yönetilmeyen IP özellikli varlıklar, risk yüzey alanınızı genişletir.

Bugün değilse, çok yakında bu cihazları da BT kontrolüne nasıl alacağınızı bilmeniz gerekecek.

Hem BT hem de OT ağlarını yönetmek, her zamankinden daha dikkatli ve yaratıcı bir şekilde çalışmanız gerektiği anlamına gelir.

Profesyonel İpucu

IP adresi olan her şey için güvenliği takip etmeyi nasıl birleştireceğinizi öğrenerek kendinizi şimdiden hazırlayın.

Benzersiz OT ve BT Ortamlarının İş Etkisi

Aşağıdaki tablo, temel OT ve BT çevre ve algı farklılıklarını ve bunların kuruluşlar üzerindeki etkisini özetlemektedir. Aynı zamanda, eşitsizliğin nasıl etkin bir şekilde yönetileceğine dair tavsiyeler de sunar.

OT Ortamı	IT Ortamı	Birleşik OT ve BT Perspektiflerinin Sonuçları	BT Profesyonelleri İçin Öneriler
Güvenlik bilincine sahip kültür; istikrar ve güvenilirlik temel endişelerdir (örneğin, "çalışıyorsa, dokunma")	Riskin farkında, güvenlik bilincine sahip kültür; veri koruma ve uyumluluk temel endişelerdir (örneğin, "sömürüye açıksa, şimdi düzeltin")	Arıza süresine neden olmadıkça siber riskler konusunda aciliyet eksikliği; EKS varlıkları için potansiyel riskler konusunda farkındalık eksikliği	• OT'ye özel ağ oluşturma ve siber güvenlik konusunda eğitim almak da dahil olmak üzere OT ve BT ortamları arasındaki farklar hakkında bilgi edinin. • Zorluklarını anlamak için OT meslektaşları ile zaman geçirin • OT ekibinizi olası siber risk tehdit senaryoları ve bunların çalışma süresini ve güvenliği nasıl etkileyebileceği konusunda eğitin • OT ve BT ağlarınız için hangi uyumluluk gereksinimlerinin ve güvenlik standartlarının geçerli olduğunu öğrenin
Çok sayıda tanımlanamayan varlık, eski sistemler ve Yönetilmeyen cihazlar	Çoğu varlık bilinir ve riski azaltmak için yeterince yönetilir	OT varlık yönetimi BT sorumluluğuna geçerken risk yüzeyi genişler	• Tüm OT ve BT varlıklarını belirleyin, riskleri değerlendirin ve savunma ve azaltmaları uygulayın
Birçok izole düz (segmente edilmemiş) ağ,	Yüksek düzeyde bölümlere ayrılmış, çok bağlantılı ağlar	Bağlantı eksikliği bazı riskleri azaltabilir ancak güvenlik görünürlüğü eksikliğine katkıda bulunur ve tehdit sınırlama seçeneklerini sınırlar	• OT ağları için güvenli olan ve olaya hızlı yanıt vermeyi kolaylaştıran gerçek zamanlı tehdit algılama teknolojisini uygulayın
Farklı Üretim protokolleri ve güvensiz iletişim karışımı	Standart TCP/IP protokolleri; ACL'ler ve şifreleme aktarımdaki verileri korumak	Belirsiz protokoller ve güvenli olmayan iletişimler saldırganlar tarafından kullanılabilir	• OT ve BT protokolleri için kapsamlı destek ve BT/OT ortamlarıyla derin entegrasyon ile teknolojiye yatırım yapın • Anormallikleri tespit etmek ve ağlar arasında geçiş yapan tehditleri ele almak için OT ve BT ağlarında bir ağ trafiği baseline'ı oluşturun
Önce güvenliğe, sonra iş sürekliliğine odaklanan kesinti ve olağanüstü durum kurtarma planları	İyi kurulmuş, belgelenmiş iş sürekliliği ve felaket veri koruma ve hizmet esnekliğine öncelik veren kurtarma planları	Artan veri kaybı riski artı test edilmemiş ve güvenilmez kurtarma özellikleri	• Birleştirilmiş veri koruması sağlayabilecek ve tüm varlıklar için olağanüstü durum kurtarma çabalarını destekleyebilecek teknolojiye yatırım yapın

BT ve Endüstriyel Otomasyon Yakınlaşmasının Etkisi

Entegrasyon, BT (ve BT güvenliği) teknolojileri için kritik bir başarı faktörü haline geldi. Açık API'lerin her yerde bulunan desteği sayesinde, önde gelen birçok uygulama kendi veri kümelerini diğerlerine besleyerek sorunsuz ve otomatikleştirilmiş iş akışları sağlayabilir. Bu entegre iş akışları, BT uzmanlarının hiç olmadığı kadar hızlı ve verimli çalışmasına olanak tanır.

BT ve OT işlevleri arasındaki siloları yıkmak, özellikle veri analizinden içgörü elde etme söz konusu olduğunda, muazzam faydalar sağlar. Aslında, BT ve OT yakınsamasını yönlendiren birden çok faktör olsa da, veriye dayalı piyasa değeri iştahı belki de en büyük itici güçtür.

Daha fazla veri ihtiyacı, aşağıdaki bazı temel soruları açığa çıkarır:

Ağımızda hangi varlıklar var?

- Özellikleri ve çalışma durumu nedir?
- Nasıl yapılandırılırlar?
- Varsa güvenlik açıkları nelerdir?

Gerçek zamanlı risklerimiz nelerdir?

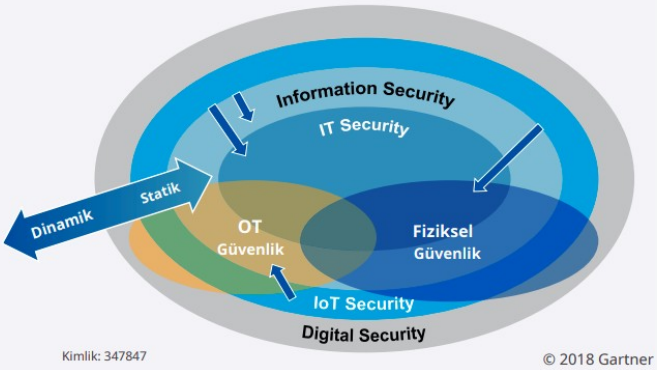
- Kötü amaçlı yazılım salgını, insan hatası veya diğer faktörlerle ilgili aksama süresi riskleri - zamanında temel nedene ulaşamazsanız, üretim veya güvenlik etkilenebilir.
- Veri ihlali riskleri – karmaşık saldırılar işlemleri kesintiye uğratmak, veri çalmak veya her ikisini birden yapmak isteyebilir. Yollarındaki tüm
- tehditleri durdurmak için hızlı yanıt gereklidir.

Bu riskler hakkında neler yapabiliriz?

- Kesintiye neden olmadan yeni araçları ve taktikleri iş akışımıza nasıl dahil ederiz?
- Dağıtılmış ortamlarımızda güvenliği nasıl ölçeklendiririz?
- OT ağlarımızdan ana BT ağlarımıza (veya tam tersi) bir saldırı sızdığında hangi prosedürleri izliyoruz?

BT/OT Yakınsama

Riski azaltmak için güvenlik ve risk yönetimi liderleri, tek bir dijital güvenlik ve risk yönetimi işlevi oluşturarak BT ve OT silolarını ortadan kaldırmalıdır. Bu işlev BT'ye rapor vermeli ancak tüm BT ve OT güvenliğinden sorumlu olmalıdır.



Gartner, Ocak 2018 "IIoT Güvenlik Liderleri WannaCry Gibi Siber Saldırılar Hakkında Neden Endişelenmeli?"

BT ve Endüstriyel Otomasyon Yakınlaşmasının Etkisi

Riskle ilgili bu soruları yanıtlamak için aşağıda özetlenen İnsan, Süreç ve Teknoloji faktörlerini dikkate almak yardımcı olur.

	Kısıtlamalar	Sonuçlar	Öneriler
 **Çalışanlar**	BT ve OT ekipleri arasındaki deneyim öncelik ve beceriye dayalı farklılıkların yanı sıra kültürel farklılıklar. Ortak girişimler için ortak bir kayıt sisteminin olmaması.	Paylaşılan bir kayıt sistemi, metrikler ve SOP'ler üzerinde fikir birliği olmadan, ekipler arasında üretken koordinasyon ve iletişim zor olmaya devam ediyor.	Aşağıdakileri yaparak, BT ve OT ağlarınız genelinde fikir birliği sağlayan ve güvenlik izlemeyi birleştiren eğitim ve araçlarla insanlara olanak sağlayın: • BT ve OT'nin tek bir yönetici lidere rapor vermesi. • BT ve OT ekipleri arasında çapraz eğitim. • Operasyonel ve güvenlik risklerini tespit etmek için tek bir platform kullanmak.
 **Süreç**	Manuel, emek yoğun ve bağlantısız siber iş akışları yüzünden olaylar birbirini beslemez.	OT varlık yönetimi BT sorumluluğuna geçerken risk yüzeyi genişler	• Doğru bir ağ haritası sağlayan otomatikleştirilmiş bir OT ve IoT varlık envanter aracını kullanarak yeni süreçleri kolaylaştırın. Böyle bir araç, tüm ortamlara yönelik riskleri yönetmek için iş akışlarının düzenlenmesine yardımcı olacaktır.
 **Teknoloji**	Silo ortamları ve protokol Eşitsizliği BT ve OT ortamları (TCP/IP) arasında 100'lerce OT protokolüne karşı). Geleneksel araçlar, OT dünyasına ilişkin görünürlükten veya anlayıştan yoksundur.	Çoğu OT ağı, tam olarak tanımlanmamış birkaç cihaz içerir. Birçoğu, güncelliğini yitirmiş ve güvenlik açığı bulunan yazılımlar ve donanım yazılımı (genellikle yükseltilemeyen) kullanır. Ayrıca, uygun güvenlik kontrolleri olmadan, OT ağlarından gelen bulaşmalar omurga BT altyapısına sızabilir.	• Küresel ölçekte EKS cihazlarını izlediği ve güvenliğini sağladığı kanıtlanmış bir teknoloji çözümüne güvenin. Böyle bir çözüm, tehditleri ve anormallikleri gerçek zamanlı olarak tespit etmeli ve hızlı kapsama ve azaltma için BT sistemleri ve iş akışlarıyla entegre olmalıdır.

En önemli 6
OT/IoT Güvenlik İlkesi

OT ağlarının benzersiz doğasını ve karşı karşıya oldukları tehditleri göz önünde bulundurarak, aşağıdaki temel güvenlik yönergelerini uygulamanızı öneririz:

1. Zarar Vermeyin

Kamu güvenliği, OT risk yönetiminin ilk ilkelerinden biridir. Bu nedenle, çoğu durumda, bu ortamlarda çalıştırılan güncel Olmayan donanım veya yazılımlar bulacaksınız. Birçok şirket, güncellemeleri ve yamaları güvenlik ve kullanılabilirlik açısından yüksek risk olarak görür. Her şeyi güncellemeden ve daha sonra soru sormadan önce iyileştirme stratejileri üzerinde fikir birliği sağlayın. Sabırlı olun ve bazı istisnaların yapılmaya değer olduğunu unutmayın ve günün sonunda her şey bir risk hesaplaması haline gelir.

2. Risklerin Yüksek Olduğunu Kabul Edin

Bir OT ağını yönetirken yapılan hatalar insan hayatını riske atabilir. Ayrıca, işletmeyi ciddi finansal riske sokarak üretimi veya hizmetleri durdurabilirler.

Bir intranet sitesinin birkaç dakikalığına kapalı kalması veya Birkaç e-postanın kuyrukta kalması, kritik bir OT varlığının kesintiye uğramasının neden olabileceği olası hasara kıyasla çocuk oyuncağıdır. Bu tür cihazlar ve ağlar ve çeşitli kullanım durumlarının içerdiği riskler hakkındaki bilginizi genişletmeye çalışın. Başka bir deyişle, tek beden herkese uymaz.

3. Neyin Normal Neyin Anormal Olduğunu Bilin

İmza tabanlı güvenlik araçlarının çoğunun altında yatan varsayım, aranması gereken bilinen bir dizi kötü şeyin ('bilinen kötüler') olduğudur. Diğer her şeyin zararsız veya yetkili olduğu varsayılır. Ne yazık ki, bu yaklaşım, henüz imza dosyalarına eklenmemiş, ortaya çıkan kötü amaçlı etkinlikleri ve göstergeleri ('bilinmeyen kötüler') tanımamakta ve risk altındaki kuruluşları ortaya çıkarmaktadır. Stuxnet ve WannaCry, bu tehdit algılama yaklaşımından kaçan ve dünya çapında milyarlarca dolarlık hasara neden olan saldırılardan sadece iki tanesidir.

Temel nedenin operasyonel hata veya siber saldırı olup olmadığına bakılmaksızın, normların dışındaki herhangi bir etkinlik için uyarılar tetiklendiğinden, trafik baseline'ı yakalamak daha hızlı, daha geniş ve daha doğru anormallik algılaması sağlar.

4. Görünürlüğü Birleştirin ve Siloları Yok Edin

Siber saldırganlar genellikle bir ağ üzerinde yanal hareketler yaptıklarından, güvenlik izleme için yalnızca birleşik bir yaklaşım uygulamak mantıklıdır. Genel merkez ofisleri, depolar, veri merkezleri, endüstriyel siteler ve saha ofisleri genelinde görünürlüğü birleştirmek, saldırganların yararlanabileceği kör noktaları ortadan kaldırır ve BT uzmanlarının uyumlu bir savunma programı sürdürmesini sağlar.

5. Mevcut Ürünler ve Süreçlerle Entegrasyon

Muhtemelen, temel BT varlıklarınızı yönetmek için çeşitli BT ve güvenlik teknolojilerine zaten yatırım yaptınız. Mevcut teknolojilerinizi ve prosedürlerinizi bozmak yerine, kuruluşunuzun sistemlerine ve iş akışlarına kolayca entegre olan araçları arayın.

Örneğin, aracı kurulumu veya hantal API'ler gibi teknik gereksinimlerin karşılanması, teslim tarihlerini uzatabilir ve proje zaman çizelgelerini tehlikeye atabilir. Ek olarak, yönetimi karmaşık olan veya mevcut iş akışlarınıza kolayca entegre edilemeyen araçlar genellikle değerlerinden daha fazla sorun yaratır.

6. İşletme Genelinde Bilgiyi Paylaşın

OT ve IoT ağlarınızda benzeri görülmemiş bir görünürlük elde etmek, iş kolu silolarını aşan içgörüleri ortaya çıkaracaktır. İyileştirilmiş esneklik ve güvenlik kesinlikle başlangıçtır, ancak derinlemesine analitik, operasyonların nasıl optimizeedileceğine Ve iş değerinin nasıl artırılacağına da ışık tutabilir. Bu görünürlük düzeyiyle BT uzmanları, yöneticilere ve OT ekiplerine risk yönetiminin ötesine geçen ve olumlu iş sonuçlarına yol açan içgörüler sunabilir. Sonunda herkes kazanır.

BT/IoT Güvenliğini Sağlamak için Sonraki Adımlar

BT, OT ve IoT'nin kuruluşlar arasında hızla yakınsadığı bir sonrak büyük soru şudur: kuruluşunuzun bu eğilimden yararlanmasına yardımcı olacak kısa vadeli ve uzun vadeli güvenlik stratejileri nelerdir?

Yardımcı olabilecek teknoloji çözümleri açısından, tüm güvenlik sağlayıcıları, ortaya atabilecekleri modaya uygun iddialara rağmen, göreve hazır değil.

BT, OT, IoT veya IIoT (Endüstriyel Nesnelerin İnterneti) ile ilgili endişeleriniz olsun olmasın, şunları yapabilmeniz gerektiğini unutmayın:

Topla

varlık ayrıntıları ve ağ trafiği kalıpları

Aksiyon Al

iş operasyonlarını en üst düzeye çıkarmak için hız, hassasiyet ve içgörü ile...

Tespit Et

operasyonel arızalar, tehditler ve diğer anormallikler

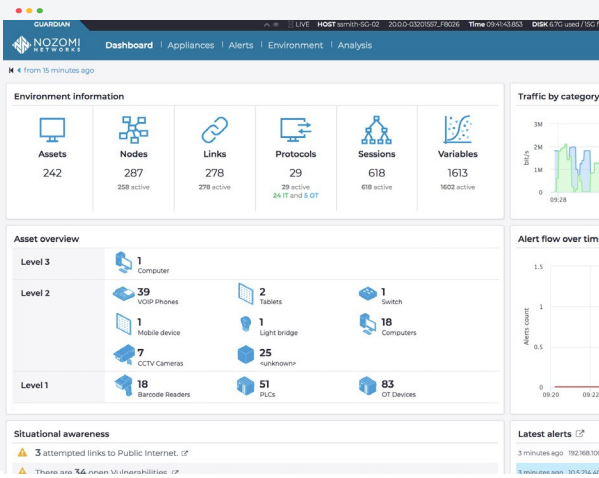
Geleneksel olmayan BT donanımını (EKS, OT, IoT, IIoT, vb.) izlemek için geleneksel bir BT güvenlik aracına yatırım yapmadan önce Satıcınıza aşağıdaki soruları sorun:

- TCP/IP konuşmayan ve/veya güvenilir ağlara bağlanamayan ağları nasıl yönetiyorsunuz?
- Üretim saatlerinde PLC'lerinizden birini devre dışı bırakma riskini nasıl ele alıyorsunuz?
- ICMP'ye yanıt vermeyen (ve aslında bir ping paketi nedeniyle yanıt vermeyebilen) OT varlıklarını nasıl keşfedersiniz?
- Ne tür TCP/IP olmayan protokolleri işleyebilirsiniz? Protokol desteğini genişletmek için nasıl bir süreç izliyorsunuz?
- Tehdit istihbaratı tedarikçiniz OT ve EKS tehditlerinde uzman mı? Hangi veri kaynaklarını kullanıyorlar?
- Hangi varlık keşfi ve envanter teknolojisini kullanıyorsunuz ve bir aracıya mı yoksa başka müdahaleci taktiklere mi bağlı?
- Hangi araçlarla entegre ediyorsunuz? Entegrasyonlarınız çift yönlü mü?
- Temel aktiviteye dayalı kestirimci analiz sunabiliyor musunuz?
- OT/IoT ağları tarafından oluşturulan çok sayıda anormallik uyarısını nasıl ele alıyorsunuz?

Kurumsal Çapta Siber Güvenliği Geliştirmek

Artan siber tehditler haberlere hakim olsa da, iyimser olmak için neden var. Nozomi Networks çözümü gibi yeni teknolojilerin dağıtımı kolay ve güvenlidir, OT/IoT siber güvenliğini önemli ölçüde iyileştirir ve BT altyapısıyla sorunsuz bir şekilde bütünleşir.

OT/IoT siber güvenliğini ve görünürlüğünü iş başında görmek ve Nozomi Networks ile çalışmanın ne kadar kolay olduğunu deneyimlemek için ekibinizin bizimle iletişime geçmesini sağlayın:
hello@cerrus.io / cerrus.io



Dünyanın En Büyük Organizasyonlarını Koruyoruz

En Büyük 20'den 9'u
Petrol & Gaz

En Büyük 10'dan 7'si
İlaç

En Büyük 10'dan 5'i
Maden

En Büyük 10'dan 5'i
Kritik Altyapı

Kimya

Üretim

Otomotiv

Havalimanları

Su

Bina Otomasyonu

Gıda ve Perakende

Lojistik

Akıllı Şehirler

Ulaşım

Referans Dökümanlar

1. **"How to Develop a Security Vision and Strategy for Cyber-Physical Systems,"** Gartner, 4 April 2019.
2. **SANS Online Cyber Security Training Courses**
   S4x20 OnRamp Online EKS Security Training Courses
3. **"How the Nozomi Networks v Supports the NIST Cybersecurity Framework"**
   "How the Nozomi Networks Solution Supports the NIS Directive and Regulations"

Nozomi Networks

OT ve IoT Güvenlik and Görünürlük için Lider Çözüm

Nozomi Networks, endüstriyel siber güvenlik ve operasyonel kontrol için yeniliklere öncülük ederek dijital dönüşümün hızını artırıyor. Sektöre liderlik ederek, artan siber riskleri operasyonel ağlara yönlendirmeyi mümkün kılıyoruz.
Nozomi Networks, tek bir çözümde, dünyanın dört bir yanındaki binlerce en büyük kritik altyapı, enerji, üretim, madencilik, ulaşım ve diğer endüstriyel sitelere OT görünürlüğü, tehdit algılama ve içgörü sağlar.

LG-IT-PRO-GUIDE-8.5x11-004

hello@cerrus.io

CERRUS

nozominetworks.com
cerrus.io