CERRUS

Fortinet ve Nozomi Networks ile Tam Kapsamlı BT/OT Siber Güvenlik

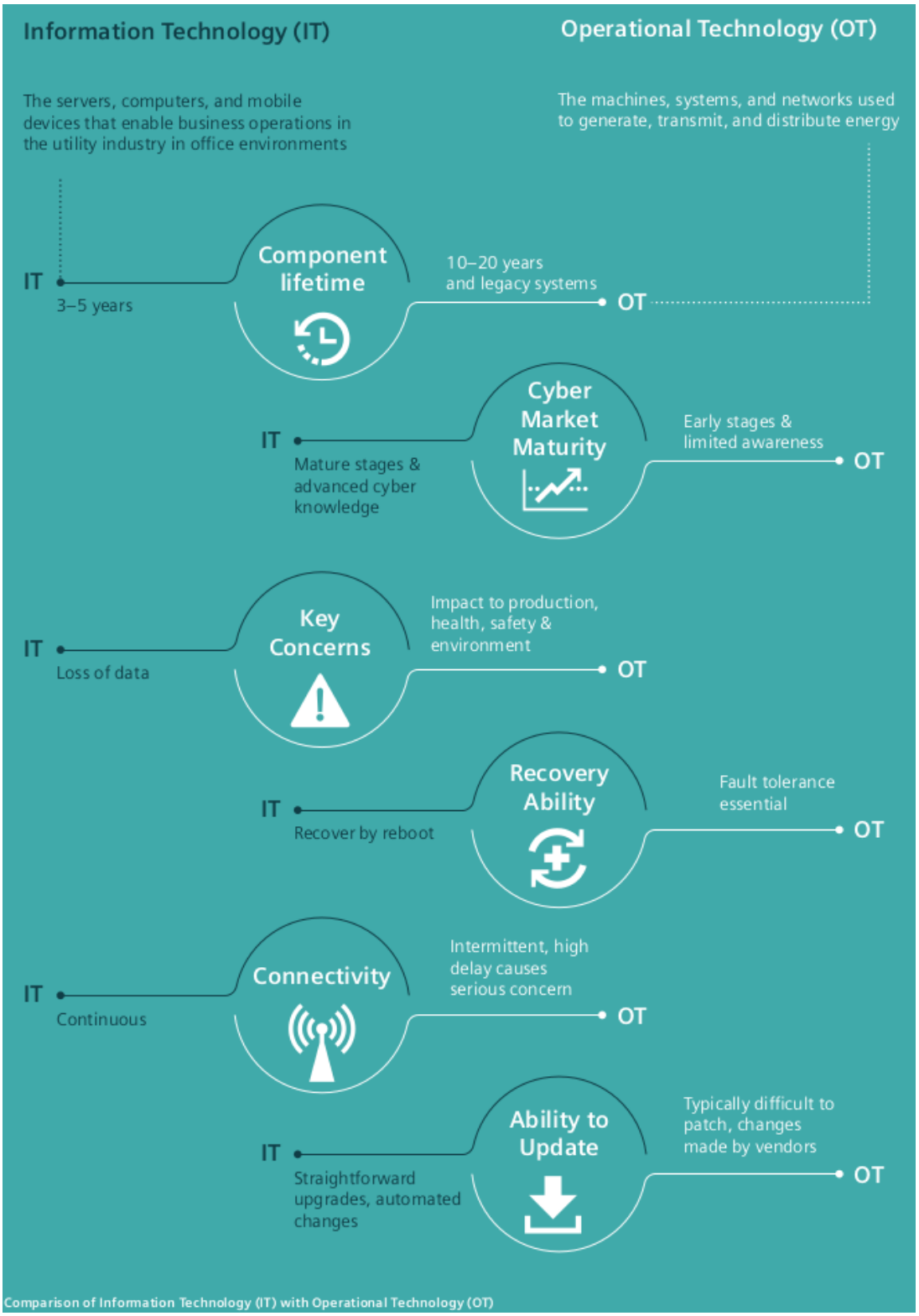
Endüstriyel Kontrol Ağları için Gerçek Zamanlı Siber Güvenlik ve Görünürlük ile Geniş, Entegre ve Otomatikleştirilmiş Güvenlik

Kritik altyapıların omurgasını oluşturan endüstriyel kontrol sistemleri (EKS), enerji, elektrik, su, üretim, imalat ve hatta askeri tesisler dahil olmak üzere tüm endüstrilerde kullanılmaktadır. Son on yılda, EKS çok daha otonom ve gelişmiş hale geldi, ancak aynı zamanda geleneksel Bilişim Teknolojileri (BT) ve kurumsal ağlara her zamankinden daha fazla bağlı hale geldi. Ağ Bağlantılarındaki bu artış, kurumların daha yüksek bir verimlilik düzeyine ulaşmasına yardımcı olurken, EKS ağlarını ve cihazlarını yeni siber kaynaklı ve operasyonel güvenlik açıklarına maruz bıraktı.

Ortak İnternet protokollerinden yararlanmanın avantajları, HMI'lar ve SCADA'lar gibi Windows tabanlı terminalleri kullanmanın kolaylığı ve maliyet tasarrufu ile birleştiğinde, Operasyonel Teknoloji (OT) ağlarını geleneksel BT sistemleri ve ilgili güvenlik riskleri ile karşı karşıya kaldı. Bu dönüşümle ilgili iki temel sorun vardır. Birincisi, kritik altyapı ile ilgili EKS ağları, Windows tabanlı terminalleri savunmasız bırakarak, planlanmamış bakım veya temel güncelleme yamaları için bile beklenmedik kesintileri – yani planlanmamış kapalı kalma sürelerini – karşılayamaz. İkinci sorun, EKS'nin yalnızca TCP / IP içinde kapsüllenmiş olan bu seri protokollerinin, temel kimlik doğrulama veya şifreleme gibi içlerinde yerleşik hiçbir güvenlik özelliğine sahip olmaması ve yine temel bir güvenlik açığıdır.

Tipik Endüstriyel Ağlar ve Bileşenler Savunmasızdır

- **Alana özgü teknolojiler:** Birçok teknoloji, endüstriyel kontrol sistemleri teknolojisi ve iletişimleri konusunda özel bilgi gerektirir. Kurumsal BT güvenlik teknolojileri, OT'nin farkında değildir.
- **Haberleşme:** Özel saldırılara eğilimli özel protokollerle iletişim kurabilirler
- **Operasyonel Teknoloji eksiklikleri:** PLC'ler ve RTU'lar, valfler, pompalar, motorlar vb. gibi fiziksel bileşenleri kontrol etmek için yapılmış düşük CPU'lu bilgisayarlardır. Bu nedenle kaynakların tükenmesinden muzdariptirler.
    - Kimlik doğrulama eksikliği
    - Şifreleme eksikliği
    - Arka kapılar (Backdoor)
    - Arabellek taşması (Buffer Overflow)
    - Fiziksel kontrol bileşenlerine özel saldırılar



Bilişim Teknolojileri ve Operasyonel Teknolojiler arasındaki Farklar

Yeni Gerçek – Malware/Ransomware Saldırıları

EKS güvenlik olaylarının sıklığı, can kaybı, büyük kesintiler, milyarlarca gelir kaybı ve büyük ölçekli altyapı hasarı gibi felaket yaratan sonuçlarla artmıştır ve bu eğilimin artması muhtemeldir. Industroyer – Crash Override, WannaCry, BlackEnergy ve Stuxnet, EKS'yi önemli sonuçlarla olumsuz etkileyen kötü amaçlı yazılım örnekleridir. Günümüzde de neredeyse her gün yeni bir zararlı yazılım saldırısıyla karşılaşılmaktadır.

	Organization	Attack Type	Incident and Impact	Cost
Energy	**Ukrenergo** (Ukrainian power company)	OT-Specific Malware: Industroyer/CrashOverride	Disrupted operations resulting in a blackout in the capital city of Kiev.[9][10]	**225K** customers without power
Food & Beverage	**Mondelez**	Ransomware: NotPetya Targeted twice in a year	Lost sales, compromised electronic data plus software and equipment damage.[11]	**$150-$188M**
Manufacturing	**Reckitt Benckiser**	Ransomware: NotPetya	Lost sales, disruptions to manufacturing & ordering systems, shipping terminals, IT networks and other vital infrastructure, in multiple markets.[12]	**$117M**
Pharma	**Merck**	Ransomware: NotPetya	Production shutdown, including inability to fulfill vaccine orders, lost sales and technology remediation.[13]	**$670M**
Shipping and Logistics	**Fedex**	Ransomware: NotPetya	IT operations disruption, impacted deliveries and sales, loss of revenue, and drop in earnings for one quarter.[14]	**$300M**

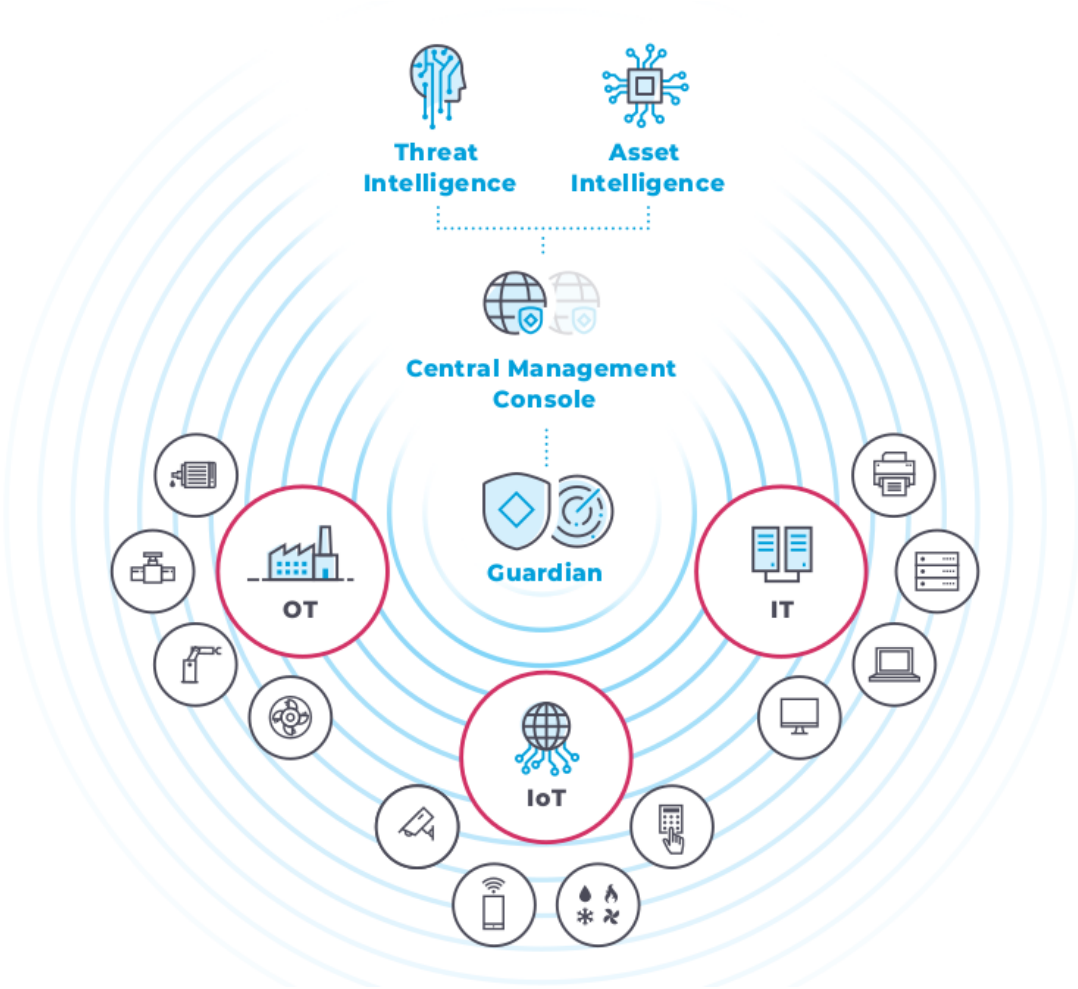
Ransomware kaynaklı birkaç saldırı ve maliyetleri

Yeni Normal – Uzaktan Erişim ve Bağlanabilirlik

Dijital teknolojilerin yaygın olarak benimsenmesi şirketlerin verimliliğinin ve sürdürülebilirliğinin artmasına ve maliyetlerin düşmesine yardımcı oldu. Yine de, **artan bağlanabilirlik**, şirketlerin **kritik altyapıları için siber saldırı**ya maruz kalma ihtimalini her geçen gün yükseltiyor.

Geleneksel OT güvenlik modeli, dış dünyaya fiziksel bir bariyer oluşturan yalıtılmış bir çevre tabanlıdır. Bu yaklaşım, **USB** cihazlarından, **kablosuz erişim** noktalarından ve artan **uzaktan erişim** ve bağlantı ihtiyacından dolayı kusursuz veya sürdürülebilir uzun vadeli değildir. Uygulanması gereken **güvenlik yamaları** arasında, yalıtılmış sistemler yeni saldırılara karşı savunmasız kalır ve yalıtılmış bir ortam, saldırıların yayılmasını engellemeyebilir.

Nozomi Networks ve **Fortinet** Ortak çözümü ile Uzaktan erişimleri kontrol altına alabilir, Endüstriyel Protokol seviyesinde NGFW özellikleri ile izinsiz girişleri ve işlemleri engelleyebilirsiniz.



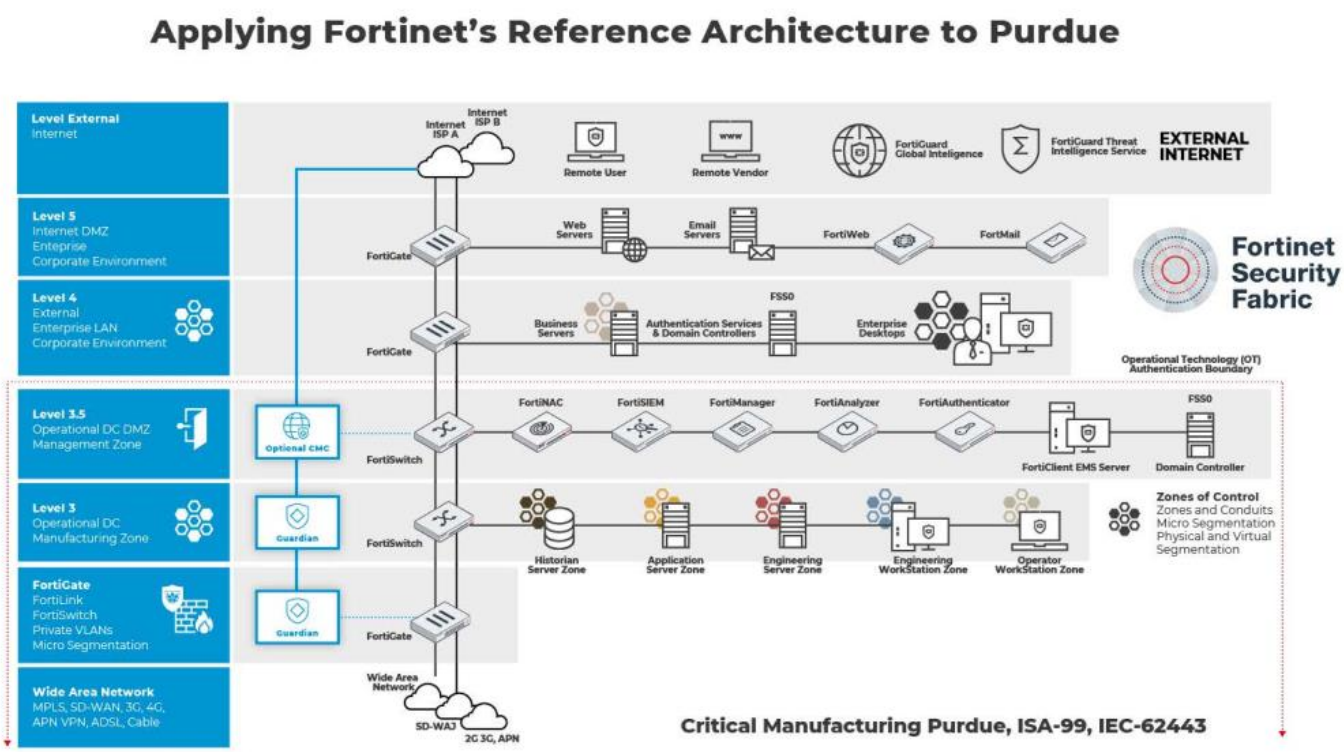
Nozomi Networks Çözüm Kapsamı

Nozomi Networks Guardian ile ağınızın siber güvenlik **zaafiyet ve risk derecelendirmesi**ni ve **gerçek zamanlı** takip edilmesini sağlayabilir, güvenlik ve ya **operasyonel anomalile**rin oluşması durumunda **gerçek zamanlı alarmlar** üretebilir, istenildiği takdirde **SIEM, NAC, FW** vb. gibi diğer siber güvenlik ürünleriyle zahmetsiz bir şekilde **entegre olarak gerekli aksiyonların alınması**nı sağlayabilirsiniz. **Threat Intelligence** hizmeti ile güncel saldırılar otomatik olarak YARA, STIX kuralları ile **Nozomi Networks Labs** tarafından güncellenir ve bu sayede saldırılarla karşılaşma olasılığınızı düşürebilirsiniz. Otomatik ve ya kişiselleştirilmiş kural ve alarmlarla OT ağınızın korunmasını ve Yapay Zeka temelli anomali tespiti ile proses üzerinde oluşabilecek operasyonel ve siber tehditleri önceden tespit edebilirsiniz.

Fortinet-Nozomi Networks Ortak Çözümü

Ortak çözüm, **Nozomi Networks Guardian** ile **Fortinet**'in OT / EKS / SCADA Sistemleri için kapsamlı güvenlik ürününü birleştiriyor. Guardian'ın yerleşik **yapay zeka (AI)** ile müdahaleci olmayan EKS protokol izleme yetenekleri, EKS ağındaki **anormallikleri gerçek zamanlı olarak tespit etmek** için endüstriyel cihazların **davranışının profilini** çıkarır. OT ve BT ağları arasında yanıt vermek ve güvenli bir ağ geçidi sağlamak için **Fortinet Security Fabric**'in bir parçası olarak Fortinet **FortiGate, FortiNAC, FortiDeceptor** ve **FortiSIEM** ile yakın işbirliği içinde çalışır.

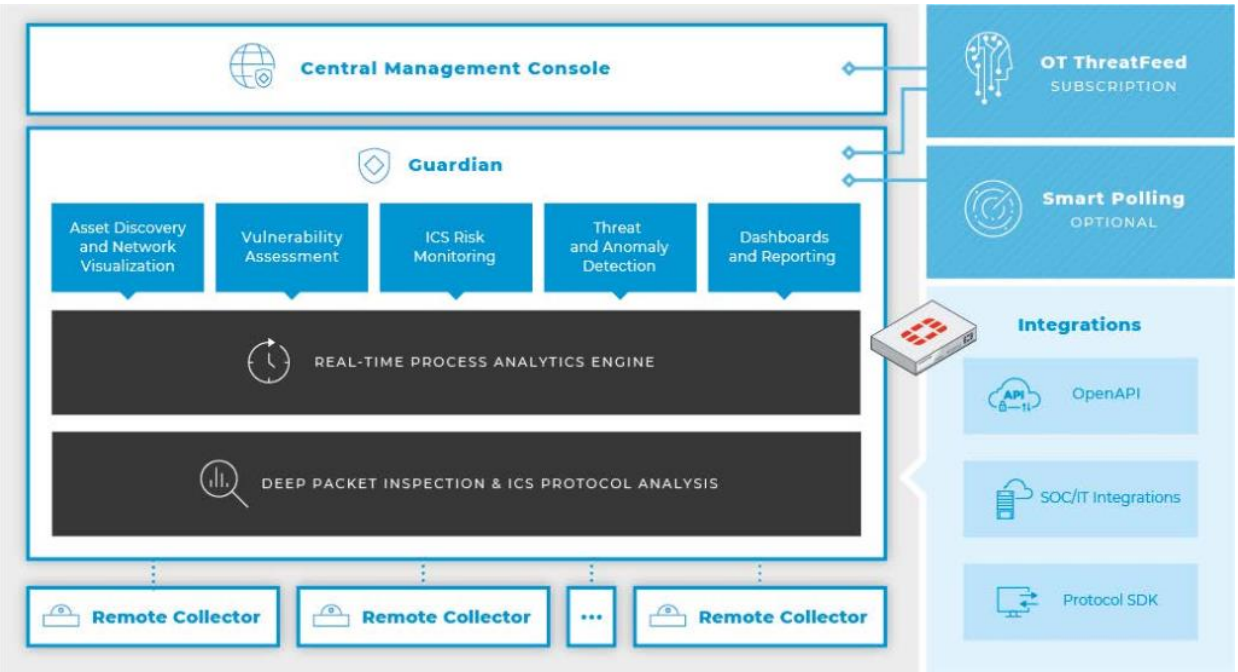
Guardian, tüm ağın, uç noktaların ve ağdaki her cihazın davranışının dahili bir temsilini oluşturmak için **ağ trafiğini pasif olarak izler**. Bir anormallik veya şüpheli davranış tespit edildiğinde, bir alarm oluşturulur ve güvenlik operatörlerine ve ağ yöneticilerine gönderilir. Aynı zamanda **Guardian, şüpheli trafiği engellemek için FortiGate'te doğru politikayı otomatik olarak girebilir**. Çözümü bir EKS ağında daha derinlemesine ölçeklendirmek için katmanlı bir mimari yaklaşım devreye girer.



Fortinet Security Fabric ve Nozomi Networks

Standart IP ağının benimsenmesiyle, tipik EKS ağı normal ağ kurallarını takip eder, bu da nispeten düz ve açık olduğu anlamına gelir. Bu segmentasyon eksikliği, bir tehdit sisteme girdiğinde, istediği zaman hareket edebileceği ve potansiyel olarak neden olabileceği hasar miktarını artırabileceği anlamına gelir. BT ağları, kötü amaçlı yazılımın ağın yalnızca bir bölümünde bulunabilmesi için dahili ağlarını bölümlere ayırmak için güvenlik duvarlarını kullanarak bu sorunu giderir.

Bu aynı koruma, **FortiGate-Guardian** çiftlerini aşağıda gösterildiği gibi EKS ağına daha derin yerleştirerek, çözümü tüm EKS ağına ölçeklendirerek ve daha büyük bir koruma granülerliği sağlayarak uygulanabilir.



Kurumsal bir ağ ile bir kez birbirine bağlandığında, EKS, normal BT güvenlik ihlalleri ile aynı potansiyel siber tehditlere ve hasara maruz kalır. Bunlar genellikle güvenlik riskleri, hatta can kaybı potansiyeli ile birlikte gelir. Örneğin, Almanya'daki Federal Bilgi Güvenliği Bürosu'na göre, 2014 yılında bir çelik fabrikasına yönelik hedefli saldırı, sosyal mühendislik ile birleştirilmiş sphearphishing kimlik avı e-postaları kullanılarak önce çelik fabrikasının BT ağına erişim sağladı ve bu da bilgisayar korsanlarını OT ağına yönlendirdi. Etki, bir yüksek fırının kontrolsüz bir şekilde kapatılmasıydı ve önemli güvenlik risklerinin yanı sıra büyük hasara ve arıza süresine neden oldu. Planlanmamış kesintiler, ekipman onarımında en az yüz binlerce hasar içerir ve tipik olarak yüz milyonlarca gelir kaybına yükselir.

Ortak Çözümün Bileşenleri

Nozomi Networks Çözümü

Nozomi Networks Çözümü, Guardian cihazı ve Merkezi Yönetim Konsolundan (CMC) oluşur. Guardian, endüstriyel kontrol ağları için **gerçek zamanlı siber güvenlik ve operasyonel görünürlük** sağlayan fiziksel veya sanal, pasif bir cihazdır. CMC, yüzlerce tesisten verileri toplayarak, yüksek kullanılabilirliğe sahip, merkezi ve uzaktan siber güvenlik yönetimi sağlar. Birlikte, görünürlüğü ve yapay zekayı OT ağlarına derinlemesine genişleten kapsamlı OT görünürlüğü, siber esneklik ve güvenilirlik sağlarlar. Yüksek entegrasyon yetenekleri ile Güvenlik Operasyon Merkezi (SoC), SIEM, ITSM, Firewall vb. Çözümlerle entegre olarak gerekli aksiyonların alınması için anlık uyarılar ve tetiklemeler oluşturur.

Fortinet FortiGate Kurumsal Güvenlik Duvarı

Fortinet Kurumsal Güvenlik Duvarı Çözümü, endüstrinin en gelişmiş güvenlik tehditlerine ve hedefli saldırılara karşı en iyi koruması için tek bir platform, tek bir ağ güvenliği işletim sistemi ve merkezi görünüm ile birleşik politika yönetimi ile uçtan uca ağ güvenliği sunar. Yenilikçi güvenlik işlemcisi (SPU) teknolojisi, SSL / TLS şifreli trafikte kötü amaçlı yazılımların gizlenmesine karşı korumaya yardımcı olmak için endüstrinin en hızlı SSL denetleme motoruyla birlikte yüksek performanslı uygulama katmanı güvenlik hizmetleri (NGFW, SSL denetimi ve tehdit koruması) sunar.

Fortinet Industrial License ile NGFW özelliklerinin üzerine onlarca Endüstriyel protokolü destekleyerek Operasyonel haberleşmeleri en granüler seviyede kontrol altına alabilir.
Platform ayrıca sıfırıncı gün saldırıları da dahil olmak üzere gelişmiş tehditlere karşı yeni nesil koruma için görünürlük ve kontrol sağlamak için Fortinet **FortiGuard** Güvenlik Abonelik Hizmetlerinin küresel tehdit istihbaratından yararlanır.

Tam Varlık Görünürlüğü ve Erişim Kontrolü için Fortinet FortiNAC

Nozomi Networks, siber riski yönetmek ve endüstriyel operasyonlar için esnekliği artırmak için gerçek zamanlı görünürlük için en iyi çözümü sunan **endüstriyel siber güvenliğin lideridir**. Tek bir çözümle müşteriler, gelişmiş siber güvenlik, gelişmiş operasyonel güvenilirlik ve kolay BT / OT entegrasyonu elde eder. Yapay zeka kullanımında yenilikler yaratan şirket, dünya çapındaki en büyük endüstriyel tesislerin kritik **endüstriyel kontrol ağlarını Görmelerine ve Güvenli Hale Getirmelerine** yardımcı oluyor. Bugün Nozomi Networks, kritik altyapı, enerji, imalat, madencilik, ulaşım ve kamu hizmetleri gibi sektörlerde çeyrek milyondan fazla cihazı destekliyor ve operasyonel ağlara (OT) yönelik artan siber risklerin üstesinden gelmeyi mümkün kılıyor.

FortiDeceptor ile Operasyonel Teknoloji Siber Güvenlik Güvencesi

Kuruluşların %90'ında bir OT sistemine izinsiz giriş yapıldı ve bu da birçok kişinin OT'de güvenliği benimsemesine neden oldu. OT güvenliğiyle ilişkili kesinti ve karmaşıklık, benimsemenin önündeki zorluklardır.

FortiDeceptor, saldırganları OT/IT varlıklarından uzaklaştıran ve hedef ağa gerçek zarar vermelerini önleyen, müdahaleci olmayan bir güvenlik çözümüdür. Purdue Modeli ile uyumlu olan **FortiDeceptor**, SCADA/ICS, Windows ve Linux sistemlerinin kapsamlı tuzak simülasyonu yoluyla hem OT hem de BT ağlarındaki güvenlik bölgelerine yönelik tehditleri tespit eder. Security Fabric, erken tehdit yanıtını otomatikleştirmek ve tehdit avını desteklemek için **FortiDeceptor**'ın Fortinet ve üçüncü taraf güvenlik çözümleriyle entegrasyonunu sağlar.

BT ve OT'de Çapraz Korelasyon için FortiSIEM

EKS ağlarından gelen verileri sürekli olarak izleyen bu entegrasyon, müşterilerin OT riski hakkında gerçek zamanlı istihbarat elde etmesine ve bunu BT ağlarından diğer tehdit bilgileriyle ilişkilendirmesine olanak tanır.

Bu entegrasyon, **FortiSIEM**'in BT ve OT verilerini, güvenlik operasyon merkezlerine ve olay müdahale ekiplerine uyarılara eksiksiz, kapsamlı ve küresel erişim sağlayan tam görünürlük için birleştirmesine olanak tanır.

Nozomi Networks çözümü, **makine öğrenimi ve tehdit istihbaratı**nın bir kombinasyonunu kullanarak riske dayalı uyarılara öncelik verir. Fortinet'in Güvenlik Olay Yönetimi (SIEM) çözümü, bu verileri BT ağlarından toplanan verilerle birleştirerek müşterilere tek, ölçeklenebilir bir çözümde görünürlük ve otomatik yanıt ve düzeltme (ARR) sağlar. Ağ ve güvenlik operasyonlarını yönetmenin karmaşıklığını azaltarak ve ihlal tespitini iyileştirerek, FortiSIEM ile entegrasyonun müşteriler için değerli olacağına inanıyoruz.

Fortinet Security Fabric

Fortinet Security Fabric, daha fazla iş yükü ve veri eklendikçe güvenliğin dinamik olarak genişlemesine ve uyarlanmasına olanak tanır. Güvenlik; verileri, kullanıcıları ve uygulamaları ağ boyunca IoT, cihazlar ve bulut ortamları arasında hareket ederken sorunsuz bir şekilde takip eder ve korur. FortiGate, diğer **Fortinet Security** ürünleri ve **Fabric-Ready Partner** çözümleriyle sıkı bir şekilde entegre olarak görünürlük ve kontrol yoluyla güvenliği genişleten **Security Fabric**'in temelidir.

Fortinet ve Nozomi Networks OT ile BT Arasındaki Boşluğu Kapatıyor

BT ve OT ortamlarının hızlanan yakınsamasıyla, **FortiSIEM**, **FortiNAC**, **FortiDeceptor, FortiGate** ve **Nozomi Networks** entegrasyonu ile sağlanan birleşik zeka, ağ kör noktalarını ortadan kaldırır ve FortiNAC'ın Otomatik Tehdit Müdahale Yeteneklerini geleneksel BT ortamlarının ötesinde OT Ortamlarına genişletir. Nozomi Networks çözümü ve Fortinet'in endüstriyel güvenlik ürünleri arasındaki yenilikçi entegrasyon, OT ağlarına bugün **mevcut olan en kapsamlı siber güvenlik çözümü**nü sağlıyor.

Nozomi Networks Hakkında

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.

Cerrus Hakkında

Dijital Dönüşüm artık tüm işletme ve tesislerin gerekliliği ve birinci önceliğidir. **Sürekli artan işlemci gücü, yüksek hacimli, yüksek hızlı sensör verileri ve kesintisiz iletişim Dijital Dönüşümün merkezinde yer alır.**

İşletmenizin bu dönüşümden en etkili şekilde yararlanabilmesi için **Cerrus olarak biz**, **atacağınız her adımda** size öngörü sunan bir yardımcı ve **değer zinciri** sağlayan 7/24 sizinle birlikte geliştirmeler yapan partneriniz oluyoruz.

Veri Toplama, **Depolama**, **Geliştirme**, **Yapay Zeka** ve **Siber Güvenlik** dahil olmak üzere modern **IIoT (Endüstriyel IoT)** teknolojilerinin işletmenize en uygun kombinasyonu ve modelini oluşturarak; ticari karlılığı artırmak amacıyla mevcut ekipman, makine parkı, reçete ve üretim hatları üzerinden veri toplaması ve depolaması yapılarak, üretim süreçlerini kesintiye uğratmadan ideal sonuçlara yönelik analizleri oluşturuyoruz.

İş ihtiyaçlarınız, üretim dizayn ve ortamınız size özel olduğundan sunulan IIoT çözümleri, iyileştirme olanakları da size özel olacaktır.

Tüm üretim tesislerinde ana masraf kaynakları olan hammadde, tedarik, proses, zaman, personel, lojistikgibi kaçınılmaz başlıklar için ayrı ayrı ya da birlikte geliştirilmiş tesis modelleri yaratmak için mevcuttaki akışı takip ederek dinliyor, verileri tüm ilgili uç noktalardan markadan bağımsız olarak topluyor ve size özelalgoritmaları oluşturarak operasyonlarınızın rasyonel verilerle optimum maliyetle ilerlemenize ön ayak oluyoruz.

Tüm bunları 30 yıllık saha ve yönetim tecrübemiz ile lokal olarak ülkemizde **Global Bilgi, Yerel Uzmanlık** ve **Yerel Destek** ile yapıyoruz.