NOZOMI NETWORKS CERRUS

EBOOK

OT Siber Güvenlik Çözümleri Satın Alma Rehberi

Gartner, operasyonel teknolojiyi (OT), fiziksel cihazların, süreçlerin ve olayların doğrudan izlenmesi ve/veya kontrolü yoluyla bir değişikliği algılayan veya buna neden olan donanım veya yazılım olarak tanımlar.

OT sistemleri, kritik altyapımıza ve sudan enerjiye ve ulaşıma kadar günlük yaşamımız için gerekli olan operasyonlara güç sağlar. Bu hayati sistemlerin kesintiye uğraması veya tahrip olması, ciddi mali zararlara neden olabilir ve hatta halk sağlığını ve güvenliğini tehlikeye atabilir.

Saldırılar giderek daha karmaşık hale geliyor ve genellikle fiziksel hasara yol açmanın yanı sıra operasyonları da aksatıyor. OT'ye özgü güvenlik araçlarına duyulan ihtiyaç acildir. Endüstriyel kuruluşlar güvenlik savunmalarını güçlendirmeye çalışırken, piyasada endüstriyel siber güvenlik çözümlerinin çoğaldığını keşfedecekler.

Bu Rehberde Bulacaklarınız:

OT/IoT ortamlarındaki eğilimler ve bunun güvenlik risklerini nasıl etkilediği

Endüstriyel kuruluşların güvenlik seviyelerini güçlendirme çabalarında karşılaştıkları IoT/OT zorlukları

Bir endüstriyel güvenlik çözümünde nelere dikkat edilmesi gerektiğine dair ipuçları

Global Pazar Yönelimleri

IT/OT yakınsaması devam ediyor

Geleneksel olarak güvenlik, OT sistemleri için bir sorun değildi çünkü bunlar genellikle BT sistemlerinden "hava boşluklu"ydu ve ayrı, silolu bir ortamda çalışıyorlardı.
Nesnelerin İnterneti (IoT) cihazlarının artışı sistemleri uzaktan kontrol etmeyi ve izlemeyi kolaylaştırdı. Bu, OT sistemlerini daha erişilebilir ve verimli hale getirirken, bir zamanlar kuruluşun geri kalanından ayrı olan bir ortama yeni bir dizi güvenlik açığı getirdi.

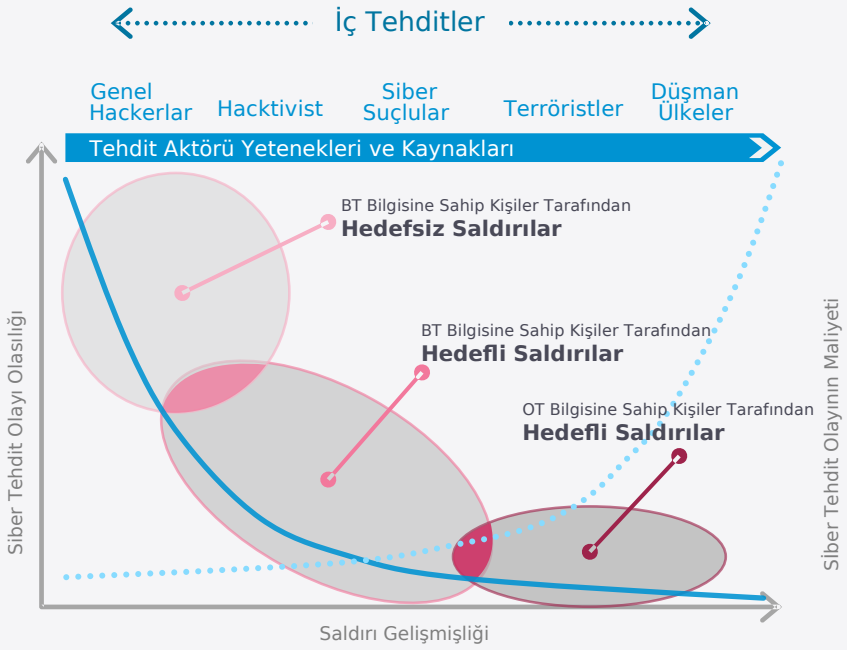
OT siber güvenlik yetenek eksikliği

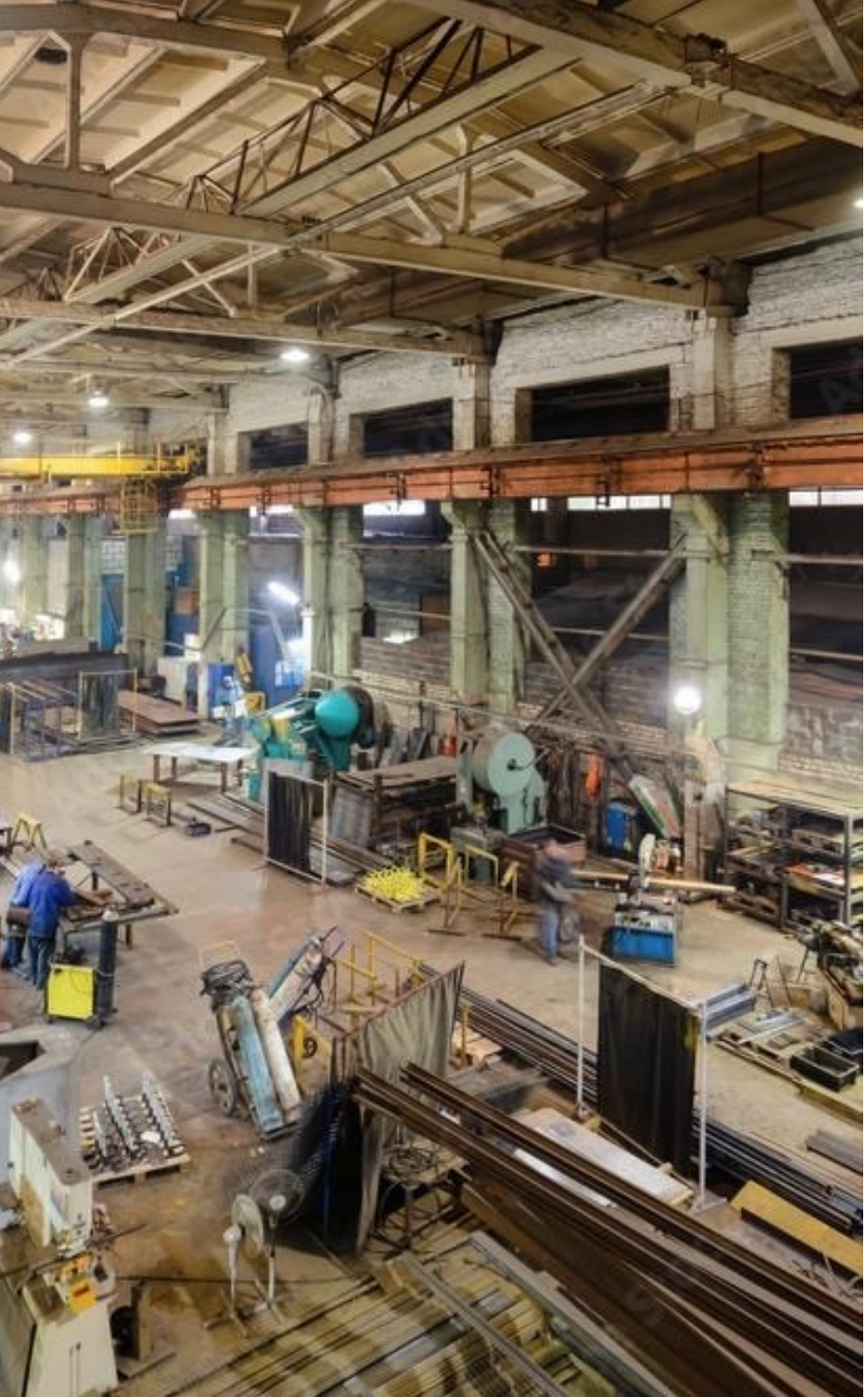
Karmaşık OT ortamı, siber güvenlik uzmanlarının siber güvenlik bilgisine sahip olmalarını ve aynı zamanda OT sektörüne nüfuz eden arkaik ve eski sistem ve süreçlerin zorluklarıyla nasıl başa çıkacaklarını anlamalarını gerektirir.
OT ortamlarına yönelik saldırıların artması ve yaygınlaşmasıyla, mevcut yetenek açığı genişliyor ve kuruluşları tehdit ve saldırılara karşı mücadelelerinde daha tehlikeli bir konuma getiriyor.

Siber saldırılar artıyor

OT kuruluşlarının %93'ü son 12 ayda bir ihlal yaşadı. Tehditlere ayak uydurmak, güvenlik uzmanları için büyük bir zorluktur.
Bilgisayar korsanları, IP hırsızlıkları, fidye talepleri, operasyonları kesintiye uğratmak ve OT ekipmanına zarar vermek için OT sistemlerine sızıyor.

Endüstriyel Siber Tehditlerin Gelişmişliği Farklılık Göstermektedir





OT Ortamlarını Güvenli Hale Getirmenin Zorlukları

Eski sistemler saldırılara karşı savunmasızdır

OT sistemleri, bakım için çok az kesinti süresiyle on yıllarca 7/24 çalışacak şekilde tasarlanmıştır. Bu nedenle, çoğu durumda, bu ortamlarda çalıştırılan ve riskli bir güvenlik ortamı oluşturan eski aygıt yazılımı veya yazılımlar görürsünüz.

Karmaşık üçüncü taraf ekosistemi

Veri ihlallerinin yarısından fazlası, aktarım sırasında veya ticari yazılımlardaki güvenlik açıkları nedeniyle verilerin kaybolması veya çalınmasıyla üçüncü taraf bir satıcıyı ilgilendiriyor. Günümüzün OT kuruluşları, kendi yazılımları ve iletişim protokolleri ile güvenlik açıklarını güncellemeyi veya düzeltmeyi zorlaştıran çok sayıda üçüncü taraf OT/IoT çözümünden yararlanıyor.

Arıza süresi risklidir

Birçok şirket, yükseltmeleri ve yamaları güvenlik ve kullanılabilirlik açısından yüksek risk olarak görüyor. OT sistemleri, yoğun şekilde entegre bir ekosistemde çalışır ve küçük bir kesinti, tüm ekosistem üzerinde domino etkisi yaratabilir. Bir OT ağının yönetiminde yapılan hatalar, insan hayatını riske atabilir, üretimi veya hizmetleri sürüncemede bırakabilir ve işletmeyi ciddi finansal risk altına sokabilir.

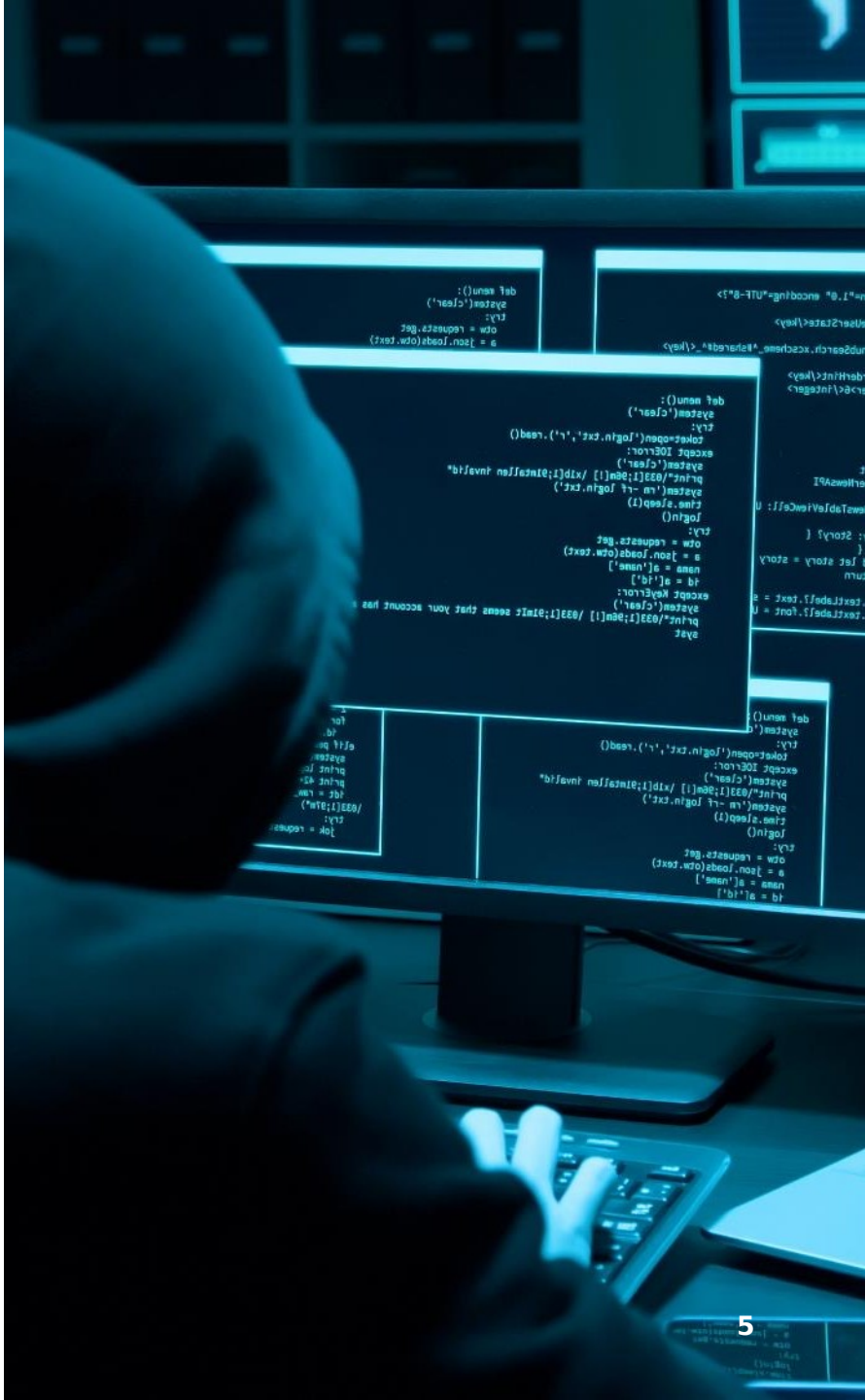
Bir OT Çözümünde Dikkate Alınması Gereken Temel Kriterler

OT güvenliği artık bir seçenek değil

OT/IT sistemlerinin birbirine yakınsaması ve nesnelerin internetine (IoT) artan bağımlılıkla birlikte, "hava boşluklu" OT sistemlerinin geleneksel güvenlik önlemi, OT ortamlarını güvenli tutmak için artık yeterli değil. BT ortamında başlayan siber saldırılar artık güvenli olmayan bir OT sistemine kolayca geçerek hayati operasyonlarda aksamalara ve kamu, sağlık ve güvenlik açısından gereksiz risklere neden olabilir.

Bir dizi yüksek profilli fidye yazılımı olayı, endüstriyel tesislerin karmaşık ve hedefli saldırılarla başa çıkmak için ne kadar hazırlıksız olduğu konusunda dikkat ve farkındalık yarattı.

Ulus devletler bilgisayar korsanlarından sosyal aktivist gruplara, örgütün zayıflıklarından yararlanmak ve bunlardan para kazanmak için fırsatlar aramaya devam ediyor, özellikle kritik altyapıyı hedeflemek için özel kötü amaçlı yazılım kodları oluşturuyorlar.



Bir OT Çözümünde Dikkate Alınması Gereken Temel Kriterler

BT çözümleri OT ortamlarında çalışmaz

BT ortamları için tasarlanan çözümler, çeşitli nedenlerle OT ve endüstriyel ortamların taleplerini karşılayamaz.

OT sistemleri, gizliliğe göre kullanılabilirliğe değer verir. Fiziksel alanda, kullanılabilirlik güvenlik anlamına gelir ve kanalizasyon sistemi gibi hayati bir operasyonla uğraşırken arıza süresi savunulabilir bir seçenek değildir.

Eski sistemler, OT ortamında bir gerçekliktir. Endüstriyel ağlar, çeşitli sayıda varlık ve birden fazla bağlantılı mimari içerir ve bunların tümü yama ve yükseltmeyi zorlaştırır.

OT sistemleri, genellikle ekipman üreticisi tarafından belirlenen çeşitli endüstriyel protokolleri destekler. Endüstriyel protokoller genellikle BT dünyasında bilinmez ve doğası gereği güvensizdir.

Bu temel farklılıklar, BT güvenlik araçlarının uygulanmasını zorlaştıran OT ve BT ortamlarının DNA'sına işlenmiştir.

Bir OT Çözümünde Dikkate Alınması Gereken Temel Kriterler

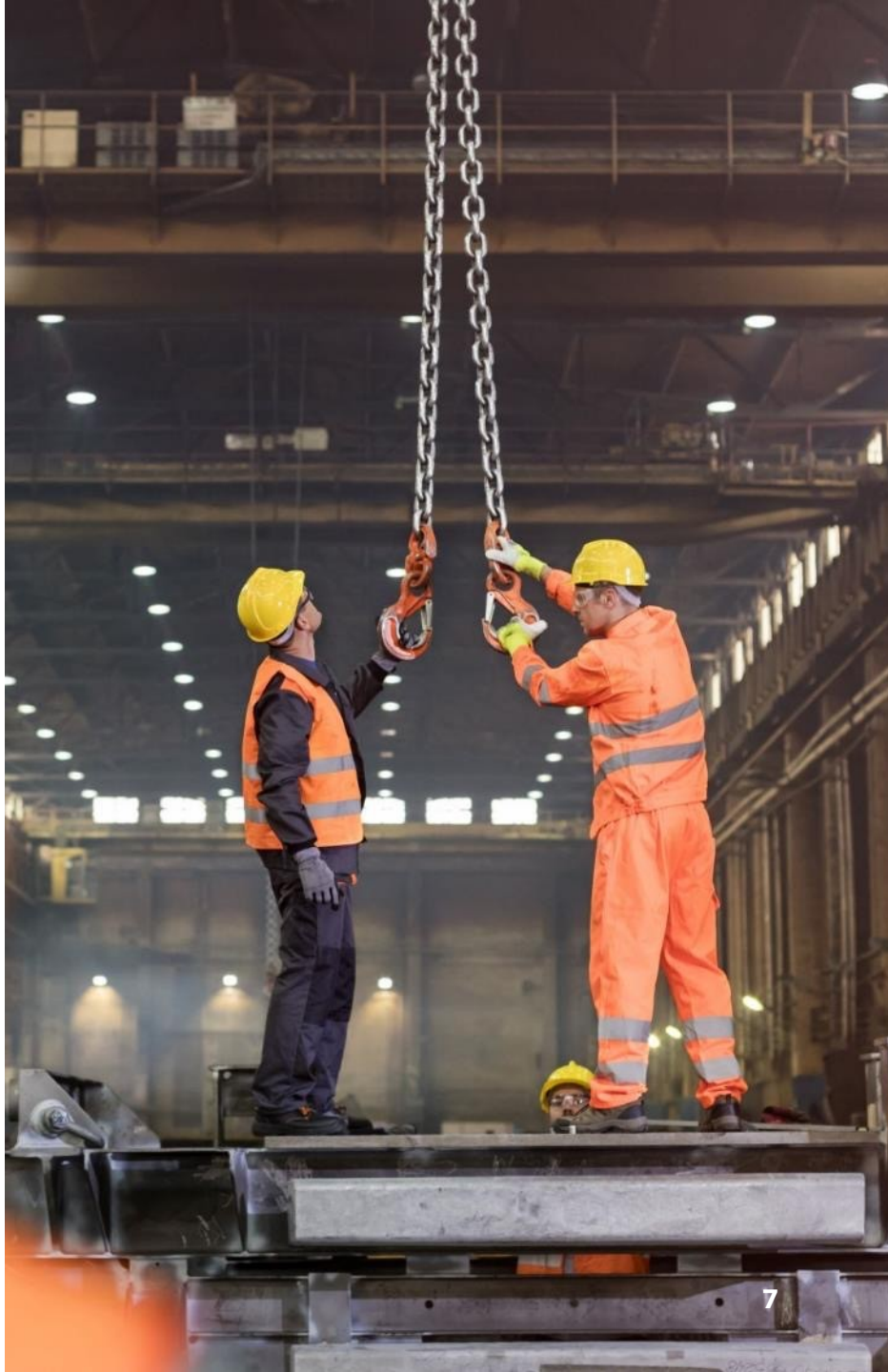
Kuruluşlar, OT güvenlik çözümlerini değerlendirirken varlık görünürlüğü, tehdit ve anormallik algılama özellikleri içeren bir çözümü düşünmelidir. Dikkate alınması gereken diğer bir konu da, sorunları hızlı bir şekilde düzeltebilmeniz ve uygun bir yanıtı koordine edebilmeniz için çözümün toplanan verilerle neler yapabileceğidir.

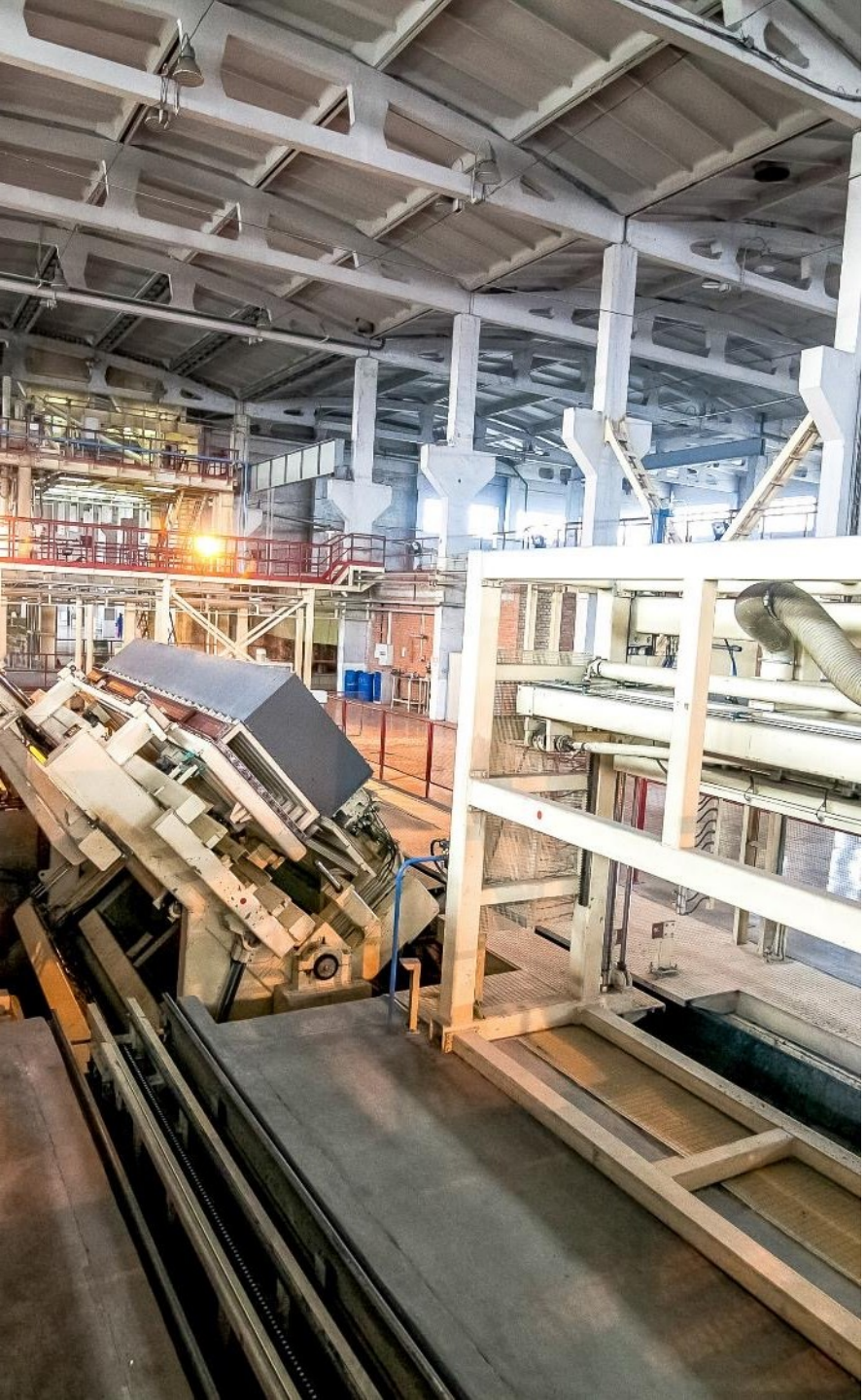
Varlık görünürlüğü

Bir OT güvenlik çözümünü değerlendirmek için birincil kriter, veri toplama kaynakları dahil olmak üzere hangi verileri toplayabildiği ve analizin doğruluğunun belirlenmesidir. Çözüm, operasyonel ağlar üzerindeki etkiyi en aza indirmenin yanı sıra her varlık için gereken görünürlüğü optimize etmek için verilerin nasıl toplanacağı konusunda esnek olmalıdır.

Çözüm, ağda olup bitenlerin yanı sıra size her cihaz hakkında birleşik bir bakış açısı sağlayan uç nokta sensörleri ile birleşik, ağ tabanlı izleme ve trafik görünürlüğü sunuyor mu? Bazı çözümler, birini veya diğerini sunar veya birine diğerine göre güçlü bir vurgu yapar.

Geçmişte, OT/ICS güvenlik çözümleri pasif izleme çözümleri olarak tasarlanmıştır. Endüstriyel gereksinimler geliştikçe, birleşik bir pasif ve aktif yaklaşıma ihtiyaç vardır.





Bir OT Çözümünde Dikkate Alınması Gereken Temel Kriterler

Tehdit ve Anormallik Tespiti

OT ortamlarına yönelik siber saldırıların artmasıyla birlikte, tehdit ve anormallik tespitine sahip olmak, tüm OT güvenlik çözümlerinde temel bir özellik haline geldi.

Bir güvenlik çözümü, yalnızca tespit edebildiği tehditler kadar iyidir. Platform, hem bilinen hem de sıfır gün tehditleri için tehdit tespitinde ne kadar gelişmiş? En son sıfır gün tehditleri ve fidye yazılımı trendlerinden en son imzaları ve uzlaşma göstergelerini içeriyor mu?

Çözüm, normal cihaz davranışını ve çeşitli ağ protokollerinin ayrıntılarının nasıl analiz edileceğini anlayabilir mi? Bu, doğru anormallik ve tehdit tespiti için temel bir gerekliliktir.

Bazı çözümler, temel neden koşullarını hızlı bir şekilde teşhis etmenize ve daha hızlı düzeltme için eyleme geçirilebilir zeka sağlamanıza olanak tanıyarak, beklenmedik süreç değişikliklerini ve yerleşik temel modellerden sapmaları derinlemesine incelemek için basit ağ anormalliği tespitinin ötesine geçer.

Bir OT Çözümünde Dikkate Alınması Gereken Temel Kriterler

İçgörüler, Eyleme Geçirilebilir İstihbarat

Çözüm, toplanan muazzam miktarda veri ve oluşturulan uyarılarla ne yapabilir?

- Daha derin bilgi sağlayabiliyor mu veya kök neden analizini otomatikleştirmeye yardımcı oluyor mu veya çok sayıda uyarı ve sorunu ilişkilendirip filtreliyor mu?
- Bu sistem sadece uyarıları mı kaydedip herhangi bir anormalliği vurguluyor yoksa varlık parametreleri ve güvenlik açıkları hakkındaki verileri mi yönetiyor?
- Sistem, güvenlik ekibi için herhangi bir olay müdahale aşamasını basitleştirebilecek veya otomatikleştirebilecek daha derin bir analiz düzeyi sunabiliyor mu?
- Sistem, risk azaltma çabalarına öncelik verebilir ve en yüksek öncelikli uyarılara odaklanabilir mi?
- Platform, bir ihlalin veya süreç anomalisinin görünür semptomlarına karşı uyarı vermenin yanı sıra temel neden analizine yardımcı olabilir mi?

Sonuç

Sonuç olarak, OT güvenliği günümüzün kurumsal güvenliğinin hayati bir bileşenidir. Kuruluşunuzun tüm ihtiyaçlarını karşılayan bir çözüm seçmek, operasyonel sürekliliğin sağlanmasına, kritik OT sistemlerinize yönelik saldırıların önlenmesine ve gizli verilerin korunmasına yardımcı olabilir.

NOZOMI NETWORKS

CERRUS

OT/IoT sistemlerinizi korumaya nasıl yardımcı olabileceğimiz hakkında daha fazla bilgi edinmek için;

cerrus.io
hello@cerrus.io