Palo Alto Networks ML Destekli Yeni Nesil Güvenlik Duvarı ve Nozomi Networks Guardian

Endüstriyel Kontrol Sisteminin(EKS) ve Nesnelerin İnternetinin(IoT) Güvenliğinin Sağlanması

Entegrasyonun Faydaları

- EKS siber esnekliğini iyileştirin ve Nozomi Networks ile gerçek zamanlı operasyonel görünürlük sağlayın.
- Palo Alto Networks NGFW ile siber tehditlere karşı otomatik eylemlerle olay yanıtını hızlandırın.
- Palo Alto Networks NGFW ile entegrasyon yoluyla Guardian'ın pasif izleme ve tespitini otomatik uygulamaya genişletin.
- Guardian grafiksel ağ haritaları ve tabloları aracılığıyla engellenen düğümleri ve bağlantıları kaldırarak düğüm ve bağlantı engelleme politikalarının yönetimini basitleştirin.

Zorluklar

Şimdiye kadar, EKS ağlarının, cihazlarının ve süreç değişkenlerinin heterojen ortamına kapsamlı, gerçek zamanlı görünürlük sağlamak zordu. Bu bağlamsal içgörü olmadan, endüstriyel operasyonlar, kontrol ağını siber saldırılardan korumak ve üretim kesintilerini önlemek için zorlanır. **Nozomi Networks**'ün yenilikçi teknolojisi, bu zorlukları EKS ve SCADA (denetimsel kontrol ve veri toplama) sistem ağları için müdahaleci olmayan ve güvenli bir şekilde çözer. Palo Alto Networks Yapay Zeka Destekli Yeni Nesil Güvenlik Duvarını (NGFW) **Nozomi Networks Guardian®** ile entegre ederek, ortak müşteriler olay yanıtını hızlandırabilir ve koruyucu önlemleri otomatikleştirebilir.

Nozomi Networks Guardian

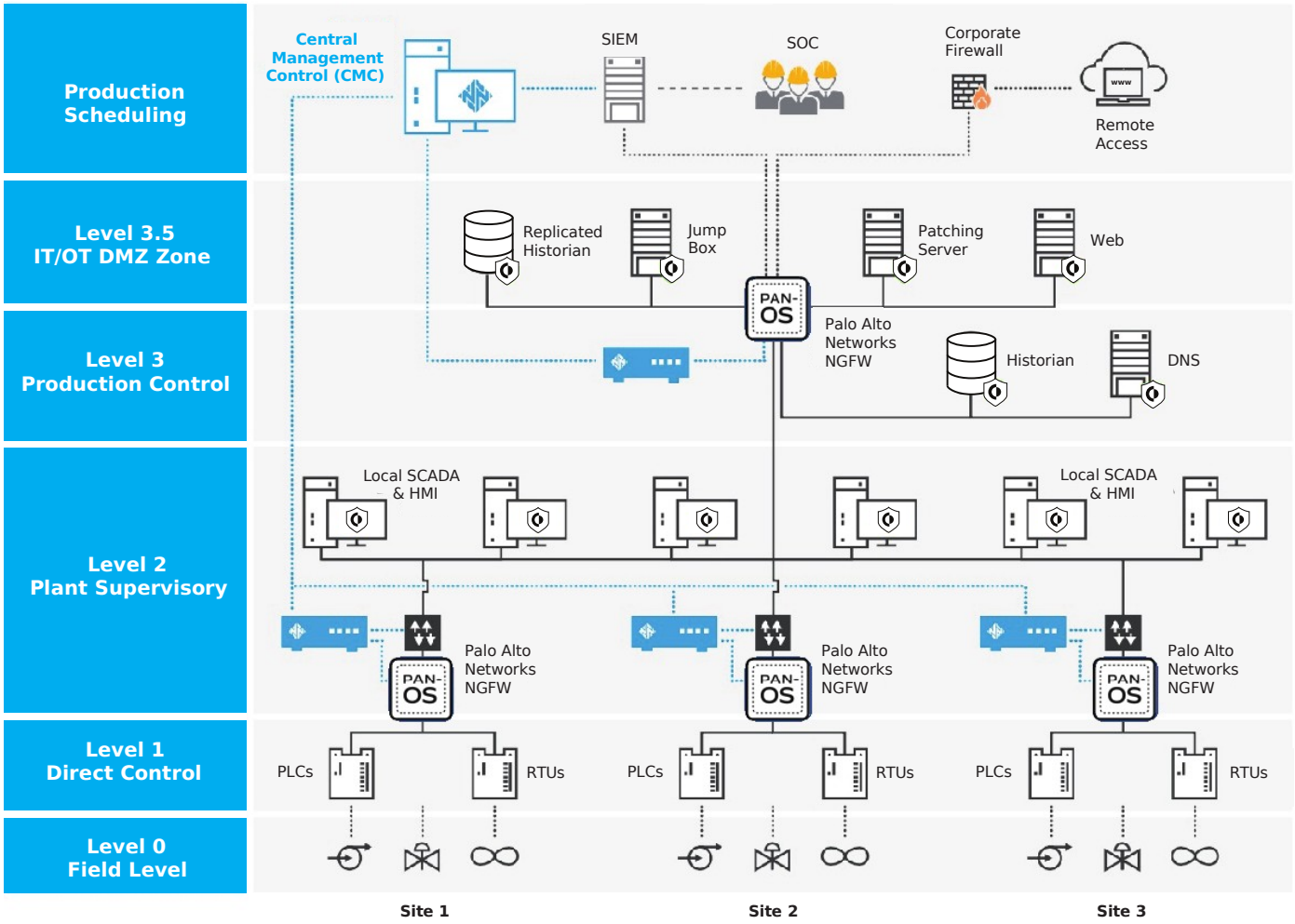
Nozomi Networks, endüstriyel ağlar için kapsamlı varlık görünürlüğü, ağ izleme ve siber güvenlik tespiti sağlayan küresel bir ICS siber güvenlik çözümleri şirketidir. Nozomi Networks çözüm seti, bir güvenlik duvarı ile entegre edildiğinde siber tehditleri görselleştirmek, izlemek, tespit etmek ve bunlara karşı düzeltme eylemi gerçekleştirmek için bir dizi uygulama modülünden oluşur. Siber esnekliği artırmak ve coğrafi olarak ayrılmış birden çok tesis dahil olmak üzere SCADA ağlarında konsolide operasyonel teknoloji (OT) görünürlüğü sağlamak için gerçek zamanlı olarak çalışır. Müdahale etmeden devreye girerek, kontrol ağı gecikmesi, determinizm veya paket dalgalanması üzerinde hiçbir etkisi olmadan ana bilgisayar ağındaki tüm varlıkları otomatik olarak öğrenir. Öğrenme aşaması tamamlandıktan sonra çözüm, siber saldırıları, siber riskleri ve süreç anormalliklerini otomatik olarak izlemek ve tespit etmek için mevcut güvenlik altyapısıyla uyum içinde çalışır.

Palo Alto Networks Yeni Nesil Güvenlik Duvarları

Palo Alto Networks Yeni Nesil Güvenlik Duvarları, dağıtılması ve çalıştırılması kolay, önleme odaklı bir mimari sunar. Palo Alto Networks NGFW'ler, tüm uygulamalar, tehditler ve içerik dahil olmak üzere tüm trafiği denetler ve konum veya cihaz türünden bağımsız olarak bu trafiği kullanıcıya bağlar. Otomasyon, manuel çabayı azaltır, böylece güvenlik ekipleri niz bağlantısız araçları sıkı bir şekilde entegre edilmiş yeniliklerle değiştirebilir, önemli olana odaklanabilir ve her yerde tutarlı koruma uygulayabilir. Kullanıcı, uygulama ve içerik, yani işinizi yürüten unsurlar, kurumsal güvenlik politikanızın bütünleyici bileşenleri haline gelir. Sonuç olarak, güvenliği iş ilkelerinizle uyumlu hale getirebilir ve anlaşılması ve bakımı kolay kurallar yazabilirsiniz.

Palo Alto Networks ve Nozomi Networks

Palo Alto Networks ve Nozomi Networks, kurumsal ve endüstriyel siber güvenlik paydaşlarına BT ve OT operasyonları arasındaki boşluğu sorunsuz bir şekilde kapatan akıllı, proaktif ve ölçeklenebilir bir siber güvenlik çözümü sunmak için teknolojilerini entegre etti. Palo Alto Networks API ve Nozomi Networks açık API ile, her iki çözüm de tehdit algılama ve iyileştirme eylemlerini bir zamanlar mümkün olanın ötesine taşımak için birlikte çalışabilir. Ayrıca, hem Palo Alto Networks hem de Nozomi Networks, kural tabanlı imza kullanarak güçlü tehdit avlama yetenekleri sunar. analiz, müşterilerin politika uygulamasını proaktif olarak genişletmesine olanak tanır. Palo Alto Networks ve Nozomi Networks entegrasyonu ile müşteriler, Guardian'ın hibrit ICS tehdit algılama ve dinamik öğrenme yeteneklerinden elde edilen ek avantajlarla Palo Alto Networks Yeni Nesil Güvenlik Platformunu güvenilir bir şekilde kullanabilirler.



Şekil 1: Örnek Palo Alto Networks/Nozomi Networks dağıtım mimarisi

Kullanım Alanı 1: Elektrik Trafo Merkezi

Kötü amaçlı yazılım, onaylanmış bir protokol kullanarak bir Programlanabilir Mantık Denetleyicisini (PLC) veya Uzak Terminal Birimi'ni (RTU) yeniden programlamak için kullanılır.

Zorluklar

Son derece güvenilir bir alt ağ (Kontrol Ağını yöneten İşlem Ağı) içindeki bir düğüm, örneğin bir PLC'yi yeniden programlamak gibi izin verilen bir komut biçiminde anormal ve belki de kötü niyetli bir eylem gerçekleştirmeye çalışır. Kötü amaçlı yazılım, farklı arka kapılar kullanarak harici bir C2 sunucusuna işaret eder ve bir DNP3 yükü kullanarak bir saldırı başlatır.

Çözüm

Nozomi Networks ve Palo Alto Networks çözümleri arasındaki entegrasyon, kuruluşun, güvenilir olsa da, SCADA varlığına yanıt olarak DNP3 protokolü erişimini "salt okunur" durumla sınırlamak için otomatik eylemde bulunmasını sağlar. İlk olarak, kötü amaçlı yazılım, kural tabanlı analiz kullanılarak hemen tanınır. Kötü amaçlı yazılım yeni bir sürümse ve henüz bir kural dahilinde açıklanmadıysa, Guardian'ın davranışa dayalı anormal etkinlik tanıma özelliği kötü amaçlı yazılımın komutlarını keşfedecektir. Ayrıca saldırıyı işaretlemek, düzeltmek ve engellemek için Palo Alto Networks NGFW ile işbirliği yapacak.

Bu olay yalnızca bir ilke ihlali olsaydı, DNP3 protokolü erişimi sınırlı kalabilir, bu da izleme işlevine izin verir, ancak erişimi kontrol edemez.

Kullanım Alanı 2: Üretim Prosesi/Petrol ve Gaz

Tanınmayan bir cihaz keşfedilir ve iletişim halinde kalmaya devam eder.

Zorluklar

Bu senaryoda, güvenilir bir alt ağa ait bilinmeyen bir bağlantı noktası, kapsamlı Dağıtılmış Kontrol Sistemi (DCS) ağı içindeki kontrolden tamamen izole edilmiştir.

Çözüm

Nozomi Networks ve Palo Alto Networks arasındaki entegrasyon, kuruluşun cihazı hemen keşfetmesini, cihazların ayrıntılarını incelemesini ve NGFW aracılığıyla otomatik iyileştirme eylemleri gerçekleştirmesini sağlar. Bu, IP adresinin engellenmesini ve kötü niyet ve risk düzeyi açısından incelenmesini içerir. Ayrıca, bu senaryo gelecekteki senaryolar için standart bir operasyonel yaklaşıma dahil edilebilir.

Kullanım Alanı 3: Ayrık Üretim/Petrol ve Gaz

Bir İnsan-Makine Arayüzü (HMI)'ne yerleşen kötü amaçlı yazılım bir PLC'yi ayarlamaya çalışır.

Zorluklar

Son derece güvenilir bir alt ağ (Kontrol Ağını yöneten İşlem Ağı) içindeki bir bağlantı noktası, izin verilen bir komut (örneğin, bir PLC'yi yeniden programlama) biçiminde anormal ve belki de kötü niyetli bir eylem gerçekleştirmeye çalışır.

Çözüm

Nozomi Networks ve Palo Alto Networks arasındaki entegrasyon, kuruluşun PLC'lere tam erişim elde etmeden veya üretim zekası elde etmeden önce bu saldırıyı keşfetmesini sağlar. Guardian saldırıyı tanımlar, uyarır ve bir Palo Alto Networks Güvenlik Duvarı kullanarak IP adresini engellemek için NGFW'ye karşı otomatik bir eylem başlatır ve ardından olayın paket yakalamalarını (PCAP'ler) alır.

Nozomi Networks Hakkında

Nozomi Networks, gerçek zamanlı siber güvenlik ve operasyonel görünürlük sağlamak için en kapsamlı platformla Endüstriyel Kontrol Sistemi (EKS) siber güvenliğinde devrim yaratıyor. Dünyanın en büyük endüstriyel kurulumlarında konuşlandırılan müşteriler, gelişmiş siber güvenlikten, iyileştirilmiş operasyonel güvenilirlikten ve gelişmiş BT/OT entegrasyonundan yararlanır.

Palo Alto Networks Hakkında

Küresel siber güvenlik lideri Palo Alto Networks, insanların ve kuruluşların çalışma şeklini değiştiren teknolojiyle bulut merkezli geleceği şekillendiriyor. Misyonumuz, dijital yaşam tarzımızı koruyarak tercih edilen siber güvenlik ortağı olmaktır.

hello@cerrus.io
cerrus.io