Oldsmar saldırısından çıkarılacak **dersler & güvenlik liderlerinin atacağı adımlar**

OTD Bilişim'den Eray Atlas, siber saldırıdan çıkarılması gereken dersleri ama en önemlisi de son birkaç yıldır bu tür sorunları ne şekilde çözmeye çalıştıklarını endüstriyel siber güvenlik ürünlerinden gerçek örneklerle paylaştı.

Birkaç gündür siber güvenlik alanında çalışan gazeteciler ile ICS güvenlik topluluğu, Oldsmar Florida su sistemine yapılan siber saldırıyı tartışıyor ki artık bu bıkkınlık verecek dereceye geldi. Pek çok kişi, bu "haber" konusunu ancak haberlere düştükten sonra konuşmaya başladı. Oysa biz çoğu müşlerimizle bu konuyu uzun zamandır konuşuyorduk. Bu yazıda bu siber saldırıdan çıkardığımız dersleri, ama en önemlisi de son birkaç yıldır bu tür sorunları ne şekilde çözmeye çalıştığımızı endüstriyel siber güvenlik ürünlerimizden gerçek örneklerle göstereceğim.

OLDSMAR SU TESİSİ SALDIRISI

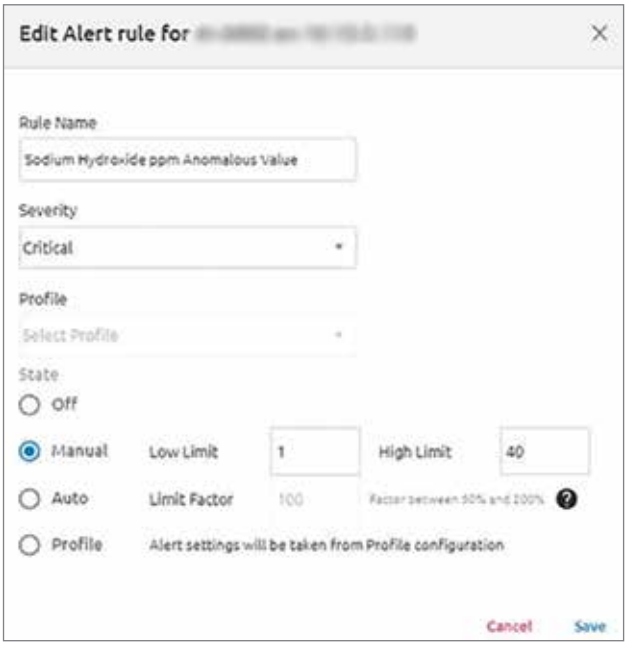
5 Şubat tarihinde bir hacker, Oldsmar, Florida su arıtma sistemine erişim sağladı ve tesisin operasyonel kontrolünü ele geçirdi. Sudaki sodyum hidroksit içeriğini geçici bir süreliğe zehirli düzeylere çıkardı. Oldsmar tesisi, 15,000 sakini bulunan şehrin ana içme suyu kaynağıdır. Neyse ki tesis operatörü, suyu normal düzeye döndürmeyi başardı. Bu olay, eyalet altyapısının küresel ölçekte güvenlik düzeyinin ele alınmasına sebep oldu.

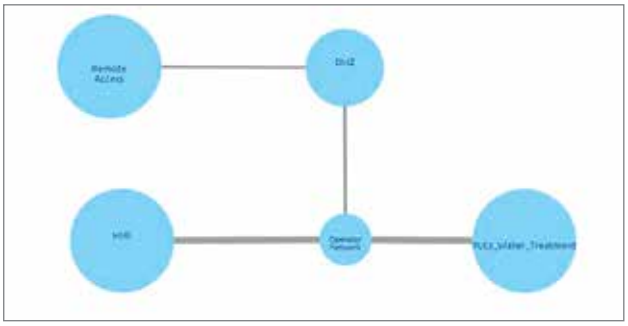
HİKAYE BUNUNLA DA BİTMİYOR

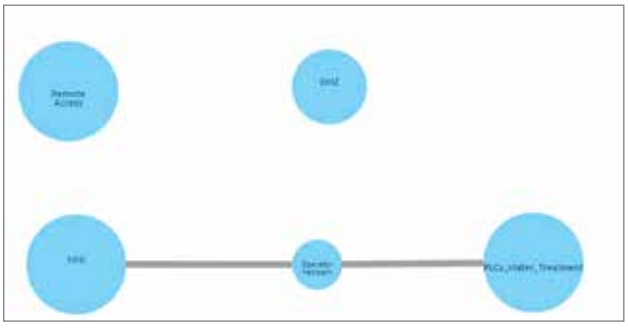
Massachusetts Eyaleti Çevre Koruma Dairesi'nin hafta başlarında yayınladığı bir güvenlik danışmanlığı uyarısına göre, Oldsmar su arıtma tesisinde bu riski önemli derecede artıran başka güvenli olmayan uygulamalara ve davranışlara atıfta bulunuldu. Bu tür diğer tesislerde de olduğu gibi Oldsmar'da personelin tesis içerisindeki durumları izlemesine ve kontrol etmesine olanak sağlayan SCADA (Merkezi denetim ve veri toplama) sistemi kullanılmaktadır. Aynı zamanda personel, SCADA ağı içerisinde sistemi izlemek ve kontrol etmek için kullanılabilecek en yaygın uzaktan erişim programı olan TeamViewer kullanıyordu. Ne yazık ki kritik altyapıda ara sıra meydana geldiği üzere siber güvenlik, tesisin önceliklerinden birisi değildi. Nitekim Oldsmar tesisi, Microsoft'un artık desteklemediği eski bir yazılım olan Windows 7'yli kullanıyorken tüm çalışanlar da TeamViewer için aynı şifreyi paylaşıyordu. Ayrıca tesis, herhangi bir güvenlik duvarı koruması olmadan İnternet'e doğrudan bağlanmıştı.

SU SİSTEMİNİN MEVCUT DURUMU

Yalnız Birleşik Devletler'de yaklaşık 54,000 farklı içme suyu sistemi bulunmaktadır. Bu sistemlerin büyük çoğunluğu 50.000'den az kişiye hizmet vermektedir. Tesislerin izlemesi ve / veya yönetmesi noktasında çoğunlukla uzaktan erişime olan güven yüksektir. Tesislerin pek çoğunda personel bulunmamakta, yeterli fon sağlanmamakta ve BT faaliyetlerini 7/24 izleyecek bir görevli bulunmamaktadır. Son olarak ise pek çok tesis, tehdit aktörleri tarafından gerçekleştirilecek yetkisiz girişleri veya tehlikeli potansiyel değişiklikleri tespit etmek üzere OT (operasyonel teknoloji) ağını güvenlik sistemlerinden ayırmamıştır. Girişim, zararlı sonuçlar doğurmadan evvel tesis operatörü tarafından tespit edilmiş ve çözülmüştür ancak bu tür bir terörist ya da ulus devlet eyleminin gelecekte ne kadar ciddi bir tehdit oluşturabileceğine ilişkin sorular gündeme gelmiştir.



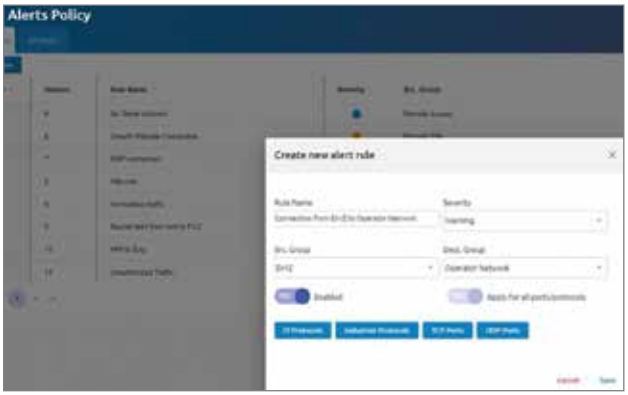




HABERLERDE NEDEN BU TÜR OLAYLARI DAHA ÇOK GÖRMÜYORUZ?

Bu tür OT ağları ile uzaktan etkileşim kurmak her ne kadar kolay olsa da Oldsmar'dakine benzer olayları haberlerde pek fazla görmüyoruz. Bunun bir sebebi de bu tesislerin bir olay olur olmaz hemen dışarıya yansıtmıyor olması olabilir. Ayrıca özellikle kamu sektöründe faaliyet gösteren pek çok şirket, kötü intiba bırakmaktan kaçınmak ve isimlerinin siber saldırı manşetlerinde yer almasını engellemek için bu konuda ellerinden geleni yapmak istiyor. Birçok şirketin, özellikle de kamu şirketlerinin bir siber saldırıdan sonra hisse senedi değerlerinin düştüğünü ve marka güvenilirliğini kaybettiğini gördük.

Fakat bu tür olayları haberlerde bu kadar sık görmemenizin asıl sebebi SCADAfence'in pek çok kritik altyapı tesisine koruma sağlamasıdır. Son yedi yıldır SCADAfence, OT ağlarının güvenliğini sağlamak için su ve atık su tesisleri de dahil olmak üzere birçok kritik altyapı kuruluşuyla çalışmaktadır. Bunu da tam ağ görünürlüğü sunarak yapıyoruz ve uzaktan erişim kaynaklı anormallikler de dahil olmak üzere her türlü anormal hareketi ve kötü niyetli davranışı doğru bir şekilde tespit ediyoruz. Uzaktan erişim güvenliği bir gerelilik olmadan önce (dışarı çıkma yasağı sebebiyle) 2020 için hazırdık ve bunun faydalarını görüyoruz.



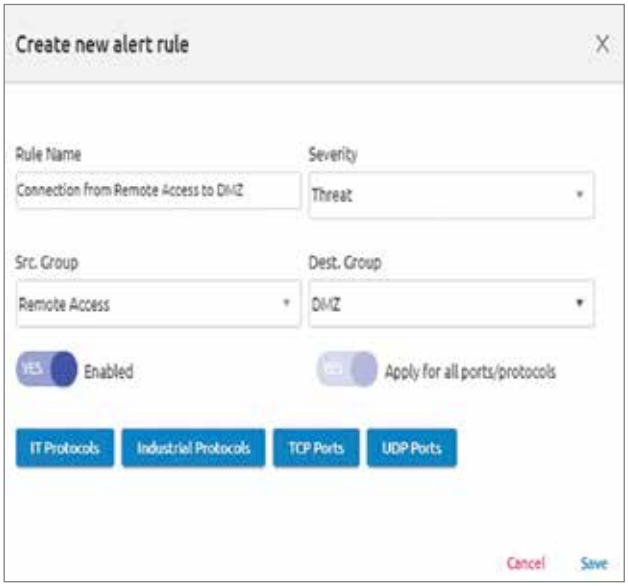
"Son yedi yıldır SCADAfence, OT ağlarının güvenliğini sağlamak için su ve atık su tesisleri de dahil olmak üzere birçok kritik altyapı kuruluşuyla çalışmaktadır. Bunu da tam ağ görünürlüğü sunarak yapıyoruz ve uzaktan erişim kaynaklı anormallikler de dahil olmak üzere her türlü anormal hareketi ve kötü niyetli davranışı doğru bir şekilde tespit ediyoruz"

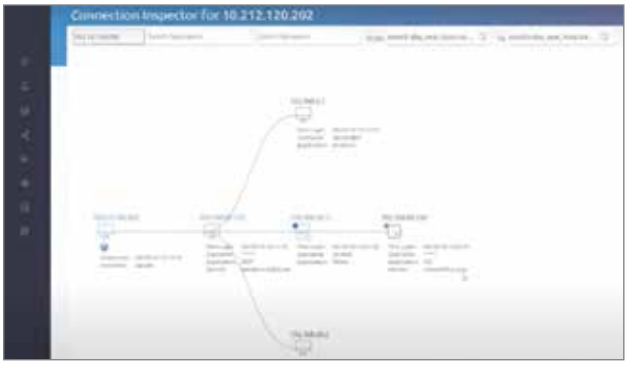
PEKİ, SCADAfence, SU ARITMA TESİSLERİNİ NASIL KORUYOR?

Gelin size müşterilerimiz için bu tür saldırıları nasıl engellediğimizi birkaç örnekle göstereyim (gerçek ekran görüntüleri ile).

1. SCADAfence Platform'un sürekli ağ izleme özelliği ile OT ağlarına yapılan uzaktan erişimleri, özellikle de OT ağlarındaki TeamViewer bağlantılarına ilişkin detaylı uyarıları kolaylıkla tespit edebiliyoruz.

2. Ayrıca, yetkisiz değişiklikleri veya süreç manipülasyonunu önlemek için belirli bir eşiği geçen değer seviyesi değişiklikleri söz konusu olduğunda derhal uyarı gönderiyoruz. Platform aynı zamanda o kadar esneklik sunuyor ki kullanıcılar, aşağıdaki gibi değişkenlere özel güvenlik duvarı kuralları oluşturabiliyor. "Sodyum Hidroksit ppm Anormal Değer" uyarısı. Böylelikle sudaki Sodyum Hidroksit değerinin maksimum değeri (örneğin) 40 ppm'yi (milyonda bir parça) aşması veya 1 ppm'nin altına düşmesi durumunda sistem uyarı veriyor.



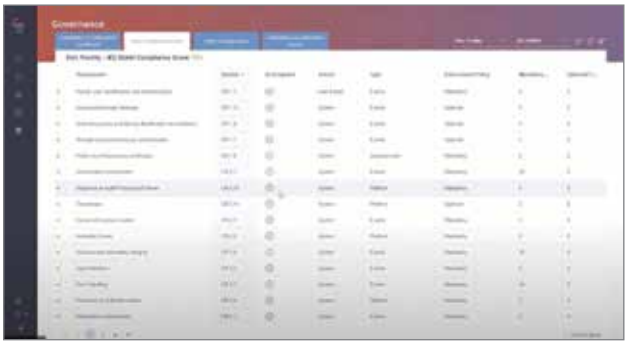


3. Ek olarak SCADAfence Platformu, kötü niyetli etkinlikleri haftalar, hatta aylar öncesinden tespit edebilen görsel teşhir haritaları sunuyor. Buna benzer bir olayda (haberlere çıkmamıştı) normal operasyonları sırasında su arıtma tesisini izliyorduk. Aşağıdaki ekran görüntüsünde de göreceğiniz üzere uzaktan erişim grubu ile DMZ grubu arasında herhangi bir bağlantı bulunmuyordu.

Tesis saldırıya uğradığı sırada güvenlik ekipleri uzaktan erişim grubundan DMZ grubuna ve DMZ grubundan da operatör ağ grubuna yeni bağlantılar yapıldığını derhal tespit etti (bkz: aşağıda) Uyarı gönderilir gönderilmez güvenlik ekipleri değişiklikten haberdar oldu ve uzakten erişim bağlantısı kesilerek saldırıyı gerçekleştirenler derhal durduruldu.

4. Belirli ağ grupları arasında bağlantı olması durumunda uyarı verecek otomatik kurallar oluşturmak gerçekten çok kolaydır. Bu durumda DMZ'den operatör ağına veya uzaktan erişimden DMZ grubuna bir bağantı gerçekleşmesi durumunda gönderilmek üzere bir uyarı oluştururuz.

5. Oldsmar'daki olayda yıllardır üzerinde durduklarımızın önemi bir kez daha göz önüne çıktı. OT ağlarında uzaktan erişim



büyük bir risk sağlar. Demek isteğim şu ki uzaktan erişim tamamen ortadan kalkıyor değil. SCADAfence platformu, uzaktan çalışma gerçekleştirirken kullanıcılar ve faaliyetleri arasında güvenlik personeli ile korelasyon sağlar. OT ağındaki anormal veya yetkisiz eylemlere ilişkin uyarılara ek olarak, kullanıcı adı, kaynak iş istasyonu ve uzaktan erişim faaliyetlerine bütüncül bir görünüm sağlamak için kullanılan bir uygulama olan hop-to-hopda dahil olmak üzere güvenlik ekiplerine tesise ilişkin detaylar sağlar.

> "Uzaktan erişim güvenliği bir gereklilik olmadan önce (dışarı çıkma yasağı sebebiyle) 2020 için hazırdık ve bunun faydalarını görüyoruz."

6. Aslında bu, endüstriyel standartlara uyumla da ilişkilidir. SCADAfence, operatörlerin uyum politikalarını tanımlamalarına ve çoğu ICS standardı, çerçevesi ve düzenlemelerine uyum durumunu kesintisiz olarak izlemelerine olanak tanıyan bir yönetişim portalı sunar.

KORKMAYIN, HAZIRLIKLI OLUN

Pek çok su ve atık su tesisi, OT ağlarına görünürlük sağlamak ve kritik altyapı ağlarını güvende tutmak amacıyla halihazırda kesintisiz ağ izleme ve uzaktan erişim teknolojilerini kullanıyor. Ağ izleme, anormallik tespiti, uzaktan erişim görünürlüğü ve uyumluluğa ilişkin bu bütüncül yaklaşım ile pek çok su ve atık su tesisi gelecek saldırılara karşı risk düzeyini yüzde 95 oranında azaltmıştır. Bunun en iyi yanı ise bu çözümlerin aracı gerektirmemesi, müdahaleci nitelik taşımaması ve bir çalışanın maliyetinin çok altında söz konusu görevleri yerine getirebilmesi. Eğer siz de tesisinizdeki endüstriyel ağlarını güvence altına almak istiyorsanız SCADAfence uzmanlarının deneyimlerine güvenebilir ve süreci size anlatmalarına izin verebilirsiniz. Ürünlere ilişkin daha detaylı bilgi almak ve PoC Talebiniz için "https://onlineteknikdestek.com/Pocrequest?culture=tr" adresini ziyaret edin. Bu hikâye hakkında daha ayrıntılı bilgi ve ürün hakkında detaylı bilgi almak isterseniz, OTD BİLİŞİM satış ekibi ile iletişime geçebilirsiniz.

> "SCADAfence Platform'un sürekli ağ izleme özelliği ile OT ağlarına yapılan uzaktan erişimleri, özellikle de OT ağlarındaki TeamViewer bağlantılarına ilişkin detaylı uyarıları kolaylıkla tespit edebiliyoruz."