Radiflow

VAKA ÇALIŞMASI

ABD'de Bulunan Bölgesel Bir Elektrik Hizmeti Sağlayıcısının Güvenliğini nasıl sağlıyoruz?

Orjinal yazıyı “Securing a Large US Power Transmission Co-Op” ismi ile ingilizce olarak da okuyabilirsiniz

Kritik altyapı denildiğinde ilk akla gelen, tek bir siber saldırı ile tüm sivil yaşam alanlarını sekteye uğratabilecek potansiyele sahip olan elektrik şebekeleridir. Enerji iletim kooperatifleri, tıpkı benzeri diğer büyük konsolide kurumlar gibi, siyasi saiklerle hareket eden ve ulus devlet destekli ya da tamamen finansal kazançlar sağlamak üzere fidye yazılımları kullanan siber suçlular tarafından gün geçtikçe daha fazla tehdit edilmektedir. Geleneksel olarak ABD'nin kırsal ve şehir dışında bulunan bölgelerindeki hanelere ve küçük işletmelere hizmet sağlayan bu iletim kooperatifleri, çok daha büyük saldırı yüzeylerine sahip olmaları nedeniyle saldırılar açısından ek bir karmaşıklık ve duyarlılık katmanı yaratmaktadır. ABD'de iki eyalette bulunan 120'den fazla trafo merkezinden oluşan bir ağ aracılığıyla dağıtım kooperatiflerine enerji sağlayan büyük bir iletim kooperatifinin OT güvenlik faaliyetlerini geliştirme ve siber durumunu standartlara uygun hale getirme kararı almasının ardındaki temel motivasyon bu olmuştur.

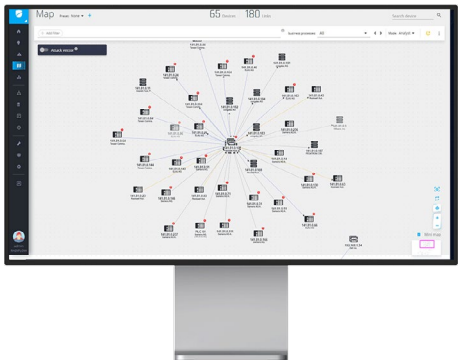
Zorluklar ve Hedefler

Projenin başlatılmasının ardından Kooperatifin aldığı ilk kararlardan biri, ağlarında kapsamlı bir siber risk değerlendirmesi yapmak, farklı operasyonel birimleri etkileyen tehdit aktörlerini ve risk seviyesini belirlemek ve en etkili risk azaltma önlemlerine öncelik vermek üzere, bütçeyi ve özel ihtiyaçları da hesaba katarak üçüncü taraf bir tedarikçi ile çalışmak olmuştur.

Risk değerlendirmesi yapma kararı, NIST-CSF'nin kılavuz ilkelerinde ve IEC62443 standardında belirtildiği gibi, en iyi yerleşik siber güvenlik uygulamalarıyla da uyumlu olmuştur. Her ne kadar tesislerinin çoğu zorunlu NERC-CIP uyumu açısından BES (Toplu Elektrik Sistemleri) seviyesinin altında kalsa da, kooperatif aynı zamanda sistem genelinde NERC-CIP düzenlemelerine uyum sağlamak istemiştir. Kooperatif, siber güvenlik risk değerlendirmesi ve ilişkili danışmanlık hizmetlerini sağlamak üzere, hem IT hem de OT/ICS ağları için çeşitli danışmanlık ve yönetim hizmetleri sağlayan bir MSP olan InfoSight, Inc.'yi tercih etmiştir. InfoSight satıcıdan bağımsız bir danışman olarak faaliyet gösterdiğinden InfoSight, kooperatife, önerilen tüm çözümlerin veya teknolojilerin yalnızca müşterilerinin yararına olacağına dair güvence vermiştir.

Önerilen Çözüm

Siber güvenliğe ilişkin titizlikle yürütülen değerlendirmenin ardından InfoSight müşterinin genel olarak IT açısından yeterli bir siber duruş sergilediği sonucuna varmıştır. Bazı güvenlik açıklarının kapanması için öneri ve yönergeler sunulmuştur.



Radiflow iSID'in ağ haritaları, tüm özellikleri ve bağlantıları ile birlikte tüm aygıtlarda detaylı bilgiler sağlar

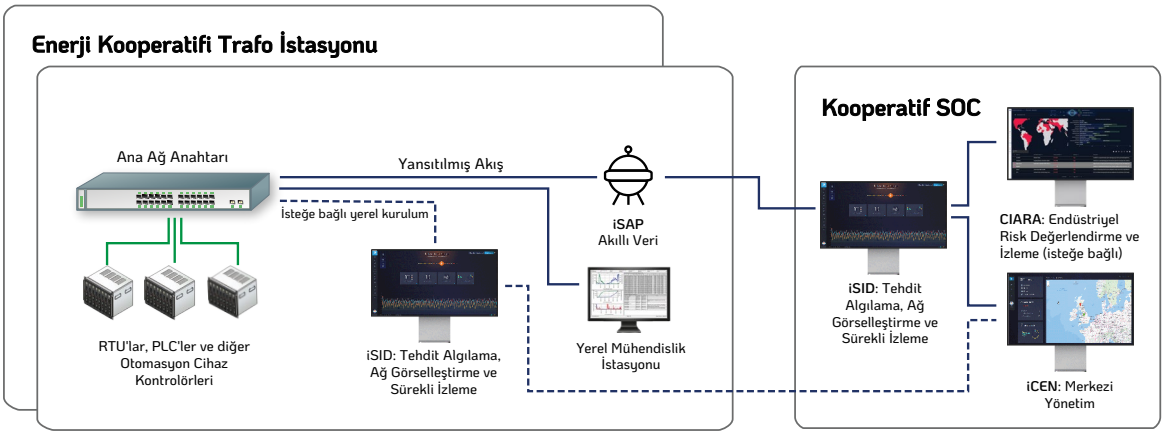
InfoSight, OT ağlarını gözden geçirirken, kooperatifin halihazırda kurulu olan IT ağ izleme operasyonunu desteklemek üzere özellikle ICS/SCADA ağına izleme fonksiyonunun eklenmesini tavsiye etmiştir. InfoSight, izleme çözümü olarak Radiflow'un iSID saldırı tespit sistemini (IDS) tavsiye etmiştir.

InfoSight tarafından belirtildiği gibi, bu sistem Gartner gibi sektör kaynaklarından yüksek puanlar almıştır. Buna ek olarak iSID, NIST'nin NCCoE laboratuvarlarında kurulmuş bir test ortamına dahil edilmiş ve NIST yayını olan SP 1800-7 Elektrik Kurumlarında Durum Farkındalığı'nda yer almıştır. iSID, kooperatife ihtiyaç duyulan mimari esnekliği sağlayabilmiştir. Bu işlem, iSID'nin daha küçük trafo istasyonlarına kurulmasına ilişkin ihtiyacı ortadan kaldırarak, ağ verilerinin analiz için kurumsal SOC'deki tek bir iSID olayına uygun maliyetli, bant genişliği açısından verimli bir şekilde iletimi için uzak konumlarda iSAP Akıllı Veri Toplayıcıların kullanılmasını içermektedir. Bazı birincil konumlarda bağımsız iSID kurulumları kullanılırken, bu kurulumların tümü Radiflow'un iCEN yönetim platformu üzerinden SOC'de merkezi olarak izlenmiştir.

Sonuç ve Mevcut Durum

Kooperatif, muhtemel çözümleri ve ortakları değerlendirdikten sonra Radiflow çözümünü ve bu çözümün uygulanmasına yardımcı olması için InfoSight'ın Profesyonel Hizmetleri'ni tercih etmiştir. Radiflow ekibi, InfoSight çalışanları ve kooperatifin IT ve SCADA personelinden oluşan ekiple yakın iş birliği içinde çalışmıştır.

İlk iSAP'ların trafo istasyonlarına yerleştirilmesi ve ağ trafiğinin iSID'ye geri iletilmesinden sonraki 24 saat içinde, kooperatifin OT LAN'ında istenmeyen trafikler tespit edilmiştir. Yapılan incelemeler, bağlı kooperatiflerin harici ağlarından gelen trafiğin OT ağlarına sızıntıya neden olduğunu, ağ yükünü artırdığını ve potansiyel saldırılar açısından ek bir saldırı vektörü oluşturduğunu ortaya çıkarmıştır. Bu vektörler ve trafik, iletim kooperatifini dağıtım kooperatiflerinden ayıran güvenlik duvarlarındaki ACL kurallarının daha sıkı hale getirilmesiyle ortadan kaldırılmıştır.
Kooperatifin beğenisini kazanan ek faydalardan biri de iSID tarafından sağlanan ağ ve varlık görünürlüğü olmuştur. Kooperatif, yeni çözümden önce trafo istasyonlarındaki varlıklara ilişkin yeterli bilgiye sahipken, yeni çözümle birlikte varlıkları tüm donanımlar, aygıt yazılımı ve güvenlik açığı özellikleriyle birlikte harita formunda net bir şekilde izleyebilir duruma gelmiştir. Tüm iletişim yollarını ve ilgili protokolleri içeren bir haritaya sahip olmaları, güvenlik duvarı kurallarına ilişkin uygun bilgiler elde etmelerini sağlamıştır. Üstelik daha önce uzaktaki bir trafo istasyonunda bir kontrolörün veya başka bir cihazın devre dışı olup olmadığını doğrulamanın hiçbir yolu yokken, iSID, her bir cihazın çalışma durumu ve faaliyetlerine ilişkin görünürlük sağlamıştır.



Kooperatif kurulumuna ilişkin şematik diyagram

Radiflow hakkında

Radiflow, kritik altyapılar ve diğer ICS tabanlı işlemler için benzersiz OT ağ güvenliği ve uzun vadeli risk yönetimi çözümleri geliştirir. Şirket, doğrudan Yönetilen Güvenlik Servis Sağlayıcıları ile iş birliği yaparak ilgili tüm veri güvenliği noktalarının keşfini ve yönetimini denetler. 2009 yılında kurulan Radiflow'un Avrupa, ABD ve Asya-Pasifik bölgelerinde ofisleri ve ortakları bulunmaktadır. Alanında kanıtlanmış çözümleri dünya çapında 6,000'den fazla noktada kullanılmaktadır.

iS5 hakkında

iS5, trafo istasyonlarının, yol taşımacılığının, demiryolu ve endüstriyel uygulamaların zorlayıcı gereksinimlerini karşılamayan,, geleceğe dönük, son teknoloji ürünü platformlar tasarlar ve oluşturur. iS5'in kapsamlı, özel hizmetlerden oluşan paketi, müşteri ihtiyaçlarının değerlendirilmesinden çözüm tasarımına, dağıtım, eğitim ve 7/24/365 desteğe kadar tüm süreçlerde destek sağlar. iS5 çözümleri, elektrik şebekesi, endüstri 4.0 ve Endüstriyel IoT (Nesnelerin İnterneti) gibi kritik altyapılarda dijital dönüşüme olanak tanır.

Radiflow