PROJE BİLGİLERİ

Teknolojiden Sorumlu Yetkili Kişi: Çağlar Yılmaz / Chakra IT Director

- Kurumunuzun faaliyette olduğu sektörleri/alanları belirtiniz.

  Luxury Home & Bathroom Textile

- Kurumunuzun toplam çalışan sayısı kaçtır?

  100 +

- Projenizin içeriğinden detaylı olarak bahseder misiniz?

  Chakra Defendry (Chakra Siber Güvenlik Alt Yapı ve Yetenek Geliştirme Projesi) projesinde, SOC merkezinden 7/24 izlenilebilir, yönetilebilir ve bir tehdit oluşması durumunda anında aksiyon alınarak müdahale edilebilir bir güvenlik sistemi kurulması hedeflenmiştir. Antivirüs, DLP, EDR, SIEM ve DAM teknolojileri satın alınarak implemente edilmiştir.

  Bütün ürünler bir arada kullanılırken doğan yönetim ihtiyacı ve her ürünün ayrı uzmanlık istemesinden dolayı bütün ürünlerin aynı platformdan yönetilebileceği Bilgi Birikim Sistemleri firması ile birlikte McAfee/Trellix ürünü tercih edilmiştir.

  McAfee/Trellix ürününün kurulum ve konfigürasyonundan sonra SIEM üzerinden logların yönetilebildiği bir yapı kurulmuştur. SOC merkezine aktarılan loglar izlenerek, üretilen alarm durumlarına göre False – Positive ayıklanmakta, atak durumlarında Chakra Merkez bilgilendirilmekte, müdahale gereken durumlarda direk müdahale yapılmaktadır. Olay kaydı raporları hazırlanarak, raporlar aylık olarak Bilgi Birikim Sistemleri firması ile değerlendirilmekte ve gereken iyileştirmeler yapılmaktadır. Ayrıca her 6 ayda bir detaylı PEN testler gerçekleştirerek, PEN test sonuçları değerlendirilmektedir. PEN test sonuçlarına göre gereken iyileştirmeler yapıldıktan sonra HEALTH CHECK de yapılmaktadır. Ek olarak, ZAFİYET Testleri yapılmakta ve 7x24 SIEM ve EDR izleme/müdahale yapılmaktadır.

- Projenin başlangıç ve bitiş tarihlerini belirtiniz? (Projelerin başvuru öncesinde tamamlanmış ve uygulamaya geçmiş olması gerekmektedir.)

  Proje, 20.12.2022 tarihinde başlamış olup, ilk PEN test Mart 2023'te yapılmış ve proje hayata geçmiştir.

- Projenizi kurum içindeki bir işleyişi iyileştirmek için mi gerçekleştirdiniz, yoksa yeni bir süreç veya hizmet mi yarattınız?

  Proje ile birlikte hem iyileştirme yapılmış hem de yeni bir süreç tasarlanmıştır. Pandemi ile artan siber saldırılar sebebiyle her şirket verilerini koruma ve kontrol altına almak istemektedir. Bunun yanı sıra güvenlik açıkları ve ön görülemeyen tehditler sebebiyle şirketlerdeki iç süreçler de sekteye uğramaktadır. Bu projenin hayata geçmesi ile birlikte şirketimizin büyüme odaklı stratejisine uygun olarak ihtiyaç duyduğu bilişim alt yapısının öncelikle iyileştirilmesi ve aynı

zamanda siber tehditlere karşı savunma yapabilen bir yapıya sahip olmuştur. Siber güvenlik süreçleri beraberinde yeni süreçleri de getirmiş ve şirket içinde güvenliğe uygun yeni süreçler devreye alınmıştır.

- Proje içindeki en büyük inovasyon nedir? (Yeni bir teknoloji veya var olan teknolojinin farklı kullanımı gibi. IOT, M2M, AI vb.)

  Dinamik IT alt yapısına geçilerek, izlenebilir ve entegre bir alt yapı kurulmuştur. Aşağıda ismi geçen ürünler bir arada kullanılmıştır ve tek bir platformdan 7X24 izlenerek bütün sistemin uçtan uca güvenliği ve sürdürülebilirliği sağlanmıştır.

  - McAfee/Trellix Endpoint Protection,
  - McAfee/Trellix DLP (Data Lost Prevention),
  - McAfee/Trellix EDR (Endpoint Detection and Response),
  - McAfee/Trellix SIEM (Security Information and Event Management),
  - McAfee/Trellix DAM (Database Access Management)

- Proje kurum içindeki hangi bölüme fayda sağlamıştır? (Satış, Pazarlama, Finans, IK, IT, Üretim, Planlama, Satın Alma, Lojistik, Müşteri İlişkileri gibi)

  Başta IT olmak üzere, sistemin sürdürülebilirliğinin sağlanması nedeniyle bütün departmanlara fayda sağlayan bir proje olmuştur.

- Projenin hayata geçirilmesi konusunda üst yönetimin desteğini tam olarak alabildiniz mi?

  Proje başlanmasından itibaren bitine kadar Üst Yönetim tarafından takip edilmiştir.

- Proje sonunda ortaya çıkan sonuçları analiz edebildiniz mi? Rakamsal verilerle ifade eder misiniz? (ROI, maliyetlerde yüzdesel azalma, üretim süresinde azalma, hata payının düşmesi)

  Korelasyon testleri, PEN testler, Zafiyet analizleri yapılmıştır. Çıkan sonuçlardan sonra düzeltme işlemi yapılarak HEALTHCheck yapıldığında sistemden ilk 6 ayda %70 bir iyileşme olmuştur. Ayrıca 7x24 SIEM ve EDR izleme ile erken müdahale yapılabilmektedir.

- Projenizde şirket içinden kaç kişi aktif olarak görev almıştır? Ekip birimleri hakkında kısaca bilgi verir misiniz?

  Projede Chakra içerisinde IT Direktörü, Sistem ve Network Müdürü ve Sistem ve Network Uzmanı olmak üzere 3 kişi çalışmıştır.

- Projenizde (varsa) İş birliği kurduğunuz veya destek aldığınız bilişim şirketlerini belirtiniz.

  Bilgi Birikim Sistemleri iş birliği ile proje tamamlanmıştır.

- Proje sırasında kullandığınız ve spesifik önemi olan markaları (varsa) belirtiniz. (Yazılım veya donanım markaları)
    - McAfee/Trellix Endpoint Protection,
    - McAfee/Trellix DLP (Data Lost Prevention),
    - McAfee/Trellix EDR (Endpoint Detection and Response),
    - McAfee/Trellix SIEM (Security Information and Event Management),
    - McAfee/Trellix DAM (Database Access Management)

- Proje için yatırım yapılan bütçeyi belirtiniz.

  100.000 $