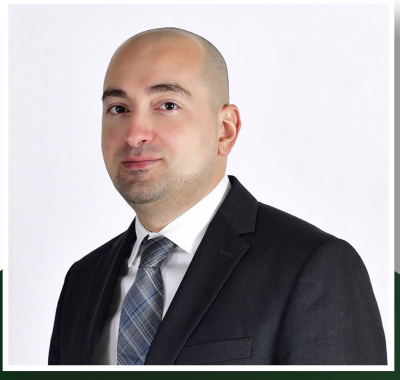
MAYIS 2021
plus
Redington

BİR BAŞARI HİKAYESİ:

Kredi Kayıt Bürosu Kurumsal Performansını Splunk ile Takip Ediyor

Kredi Kayıt Bürosu (KKB), Siber Güvenlik ve Tehdit İzleme Merkezi'nin geliştirilmesi ve Anahtar Performans Göstergeleri'nin (KPI) görselleştirilmesine yönelik olarak başlattığı kapsamlı projesinde, Splunk'ın IT Service Intelligence ve Enterprise Security çözümlerini kullanmayı tercih etti. Bu projede, Splunk iş ortağı Seynur ile birlikte çalışan KKB, hayata geçirdiği KPI altyapısını 2020 yılının ilk aylarından itibaren kurumsal süreç performansını anlık olarak ölçerek kurumsal iş verimliliğinin takibine yönelik kullanmaya başladı.

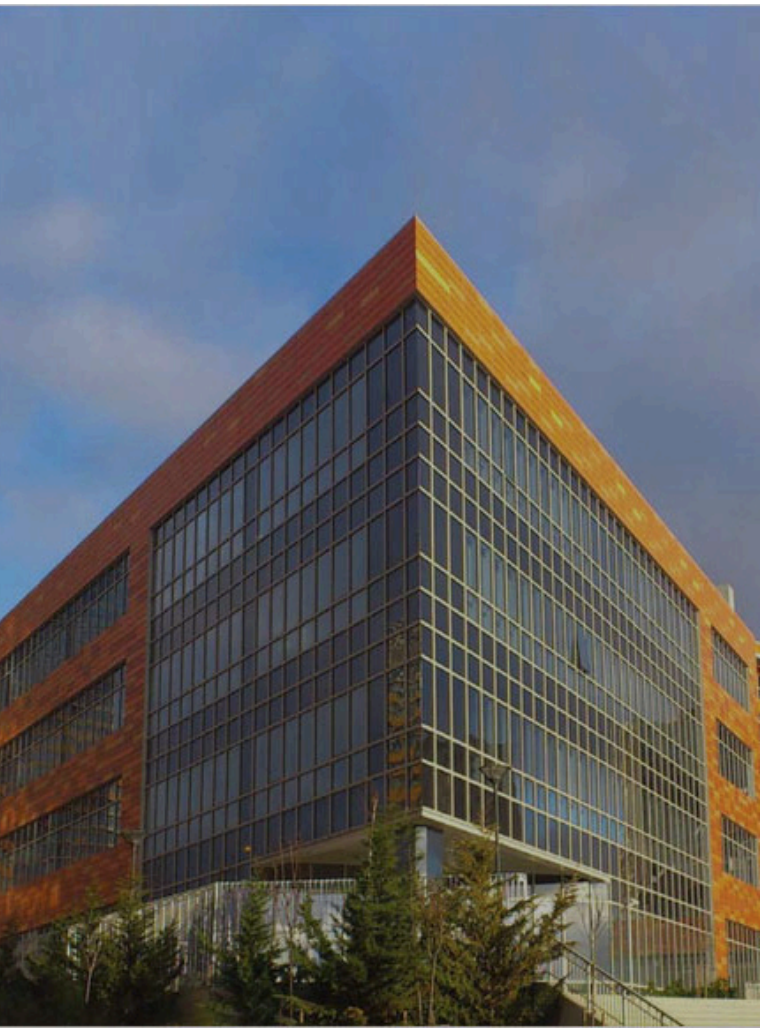


"Splunk ile kurmuş olduğumuz KPI izleme altyapısı, bize güçlü ve entegre bir kurumsal performans görselleştirme olanağı sunarken, bilgi güvenliği süreçleri kapsamında da makine öğrenmesi kullanan daha olgun bir yapıya geçmemizi sağladı."

H. SERDAR ÇOLAK
Risk Yönetimi Genel Müdür Yardımcısı
KREDİ KAYIT BÜROSU

Splunk teknolojileri ile gerçekleştirdiğiniz projenin ayrıntılarına geçmeden önce Kredi Kayıt Bürosu'nun faaliyetlerine değinebilir miyiz?

SERDAR ÇOLAK (Kredi Kayıt Bürosu-Risk Yönetim Genel Müdür Yardımcısı): Kredi Kayıt Bürosu (KKB), sektörün önde gelen 9 bankasının ortaklığı ile 1995 yılında kuruldu.Kurulduğu günden bu yana da finansal teknoloji alanında yürüttüğü faaliyetlerini geliştirerek sürdürüyor. Bankalar, tüketici finansman şirketleri, leasing, faktoring ve sigorta şirketleri olmak üzere 200'e yakın üyesi bulunuyor. KKB, üyelerinden toplandığı müşteri bilgilerini birleştirerek, yine üyelerinin kredi risk yönetim süreçlerinde kullanabileceği bilgileri üreten bir yapıya sahip. Üyelerimizden topladığımız müşteri bilgilerini birleştirerek, yine üyelerimizin kredi risk yönetim süreçlerinde kullanabileceği bilgiler üretiyoruz. Gücünü teknoloji altyapılarından alan bu yapı, gelişmiş ürün ve hizmet portföyü ile finans sektörünün yanı sıra reel sektörün ve bireylerin de risk yönetim süreçlerine katkı sağlıyor. Kişi ve kurumların finansal itibarlarını yönetebilmeleri için önemli araçlar sunan KKB, 2014 yılında hayata geçirdiği finansal hizmet platformu Findeks ile, artık bir bankayla yolu kesişmiş, hayatına kredi kartı ya da kredi ürünleri girmiş olan herkes tarafından biliniyor. Findeks platformunun faaliyete geçmesinin hemen ardından, gerekli düzenlemelerle Findeks Karekodlu Çek Sistemi geliştirildi. Daha şeffaf ve güvenli bir ticaret hayatı için oldukça önemli adımlar atılması sağlandı. Bununla birlikte, başta bankacılık ve finans sektörü olmak üzere kurumlara yönelik veri merkezi ve olağanüstü durum merkezi olarak hizmet veren KKB Anadolu Veri Merkezi de 2016 yılı Aralık ayında faaliyete başladı.



Finans dünyasında çok önemli roller üstlenen ve bir FinTech şirketi olarak görebileceğimiz KKB'yi, Splunk ve Seynur ile bir araya getiren ihtiyaçlar nelerdi?

S. ÇOLAK: Gerçekten de KKB'nin, Türkiye'nin FinTech kapsamında değerlendirilebilecek en köklü firmalarından birisi olduğunu söyleyebiliriz. Bankaların merkezinde konumlanmış ve odağında teknolojinin yer aldığı, ürün ve hizmetlerini yazılımlar ve veri merkezi kapsamında sağladığı altyapılar ile en üst sürdürülebilirlik seviyesinde sağlayan bir yapımız var. Bu doğrultuda, iş yapma tekniklerimizi karşılaştırabilmek, kendimizi kıyaslayabilmek ve geliştirebilmek amacıyla, finans ve teknoloji kurumlarına "benchmark" ziyaretleri gerçekleştiriyoruz. Splunk altyapısını, Siber Güvenlik ve

Tehdit İzleme Merkezi çalışmaları hakkında yaptığımız bir referans ziyaretinde yakından inceleme fırsatımız oldu. İlk etapta siber güvenlik için oluşturduğumuz yapının desteklenmesi kapsamında bazı hayallerimiz vardı. Splunk'ın, verileri toplamanın yanı sıra analiz ve gösterge panelleri ile görselleştirme konularında da oldukça güçlü olduğunu farkettik. 3 plus 2021 Mayıs Bu noktada, Anahtar Performans Göstergeleri (KPI) projesinde de faydalı olabileceğine dair değerlendirmelerimiz oluştu. Şirketimizin kurumsal anlamda üretim hattı süreçlerinin performansını izleyerek verimliliğini daha üst seviyeye çıkarabilmek adına benzer altyapıyı kullanabileceğimizi değerlendirdik. Dolayısıyla iki ana konu başlığında da Splunk ile ilerleyebileceğimizi düşündük. Sırasıyla KPI projemizi hayata geçirdik ardından da Siber Güvenlik ve Tehdit İzleme Merkezi altyapımızı daha olgun bir seviyeye getirdik.

Söz konusu projeler için hangi Splunk çözümlerini hayata geçirdiniz?

S. ÇOLAK: KKB bünyesinde, Splunk'ın IT Service Intelligence ve Enterprise Security çözümlerini kullanıyoruz. Splunk ile çalışmaya başladığımızda önceliklerimizden birisi, KPI'ların doğru ölçülmesi ve görselleştirilmesiydi. Bu nedenle öncelikle IT Service Intelligence çözümü üzerinde ilerledik. Yazılım kurulumları kapsamlı bir proje yönetimi sonucunda gerçekleştirildi.

"Makine öğrenmesi, sisteme uygulanabilir bir şekilde dahil ediliyor"

SELİM SEYNUR
Genel Müdür
Seynur BT

Kredi Kayıt Bürosu'nda (KKB) hayata geçirilen bilgi güvenliği ve KPI projesinin başarısını değerlendiren Seynur BT Genel Müdürü Selim Seynur, bir projenin başarısını, en klasik tabirle, 'insanlar', 'süreçler' ve 'teknoloji' unsurlarının uyumlu bir şekilde bir araya gelerek, olabildiğince düzgün bir üçgen oluşturabilmesine bağlıyor ve "Kredi Kayıt Bürosu'nda hayata geçirilen projede bu üç unsur, güzel bir üçgen oluşturmayı başardı. KKB'nin zaten kendi içinde çok yetkin, çoğu finansal kurum ve bankaya örnek olabilecek seviyede, oldukça geniş bir güvenlik ekibi var. Süreçlere, sorulacak sorulara, alınması gereken cevaplara son derece hakim bir ekip. Biz ise teknolojiyi derinlemesine bilen ekip olarak, neler yapılabileceğini çok iyi biliyorduk. Hep birlikte, ekipler arasında çok başarılı bir işbirliğinin gerçekleştiğine tanıklık ettik. Proje başarısında bu unsurlar çok önemliydi" diyor.

Selim Seynur, Splunk teknolojisinin ve sahip oldukları uzmanlığın yarattığı farkı ise şöyle özetliyor: "Elimizde Splunk gibi bir aracımız var. İnovatif indeksleme/sorgulama teknolojisi ve makine öğrenmesini gerçekten uygulanabilir biçimde sisteme dahil edebilmesiyle, gelenekselleşmiş yapılardan daha ileri bir yaklaşım vaat ediyor. Daha proaktif çalışabilen bir altyapı, bir veri analiz platformu sağlıyor. Bunun üzerine, hem Seynur olarak bizim kendi müşterilerimizden, eğitim süreçlerimizden edindiğimiz deneyimi hem de Splunk'ın tüm dünyada hayata geçirdiği örnek uygulamalardan kazanılmış olan bilgi birikimini ekliyoruz."

Süreç sahipleri ile birlikte KPI'lar belirlenirken, sistem analizi çalışmaları ile veri toplanacak sistemler tespit edildi ve yapılması gereken entegrasyonlar ortaya çıkarıldı.

Bu entegrasyonlar ile birlikte, verilerin en doğru şekilde gösterilebileceği grafikler ve Splunk uygulamasının sahip olduğu farklı görselleştirme araçları seçilerek gösterge panelleri hazırlandı. Sonrasında hazırlanan gösterge panelleri üzerinden, süreç sahipleri ile birlikte sonuçların teyidi gerçekleştirildi.

KPI Projesi ile hedefiniz neydi?

S. ÇOLAK: Hedefimiz, Anahtar Performans Göstergeleri'nin (KPI) belirlenmesi ve verimliliğimizde, kurumsal başarımızda önemli rol oynayan süreçlerimizin performansının gerçek zamanlı gösterge panelleri üzerinde izlenebilir olmasıydı. Bir finans ve teknoloji şirketi olarak, tüm süreçlerimize ilişkin performans göstergelerinin belilrenmesinin yanı sıra "Fikirden Ürüne" olarak adlandırdığımız bir fikrin oluşmasından gerçekleşmesine kadar gerçekleştirilen süreçler ile bu süreçlerin çıktılarına zaman ve kalite olarak doğrudan etkisi olan süreçlerin izlenmesi projedeki önceliğimiz oldu. Bu kapsamda 7 aylık bir çalışmanın sonunda tüm süreçlere ilişkin toplam 697 KPI belirlenerek, Ürün Geliştirme, Ürün Yönetimi, Yazılım Geliştirme, Bilgi Teknolojileri Proje Yönetimi, Değişiklik Yönetimi ve Talep Yönetimi süreçlerine ilişkin gerçek zamanlı izlenebilir gösterge panelleri hazırlandı.

Ne kadar süredir tüm gösterge panelleri kullanılır durumda?

S. ÇOLAK: Tüm süreçlerin üzerinden geçilmesi, hepsinin analizlerinin gerçekleşmesi, arka tarafta hangi verilerin nasıl alınacağının hesaplanması, tasarımların oluşturulması, entegrasyonların yapılması, zaman alan ve titizlikle yürütülmesi gereken bir çalışmaydı. Alanında uzman ekiplerimizin yoğun çalışmalarıyla yaklaşık 7 ay içerisinde tamamlanan proje sonucunda üst yönetim dahil olmak üzere yöneticilere yönelik farklı gösterge panelleri ve raporlamaları sunmaya başladık. 2020 yılının başından itibaren de gösterge panellerimizi, KKB'nin kurumsal anlamda genel performansını ölçebilecek düzeyde verimli olarak kullanıyoruz.

PROJE HEDEFİ

Genel anlamda bütün bilgi güvenliği, siber güvenlik altyapısının istenilen seviyede izlenebilir olması. Anahtar Performans Göstergeleri'nin (KPI) belirlenmesi ve Ürün Geliştirme, Ürün Yönetimi, Yazılım Geliştirme, Bilgi Teknolojileri Proje Yönetimini kapsayan "Fikirden Ürüne" süreçlerinin ve bu süreçlere zaman ve kalite bakımından doğrudan etkisi olan Değişiklik ve Talep Yönetimi süreçlerinin performansının gerçek zamanlı gösterge panelleri üzerinde izlenebilir olması.

Güvenlik tarafında Splunk'ı nasıl konumlandırıyorsunuz?

S. ÇOLAK: KKB'yi özellikle finansal kurumların bireysel veya kurumsal müşterilerinin kredili ürünlere ilişkin geçmiş ödeme performanslarını görüntüleyebildikleri, finans dünyasına yönelik bir veritabanı olarak düşünebiliriz. Kurum olarak bulunduğumuz stratejik konum nedeniyle barındırdığımız verilerin güvenliğini sağlamak adına deneyimli ve uzman ekibin yanı sıra üst düzey koruma altyapı sistemlerine sahibiz. Kurumumuzun öncelikleri arasında yer alan bilgi güvenliği konusunda zaman içerisinde değişen ihtiyaçlara uygun olarak farklı teknolojileri devreye alıyor ve güvenlik altyapımız ile koruma sistemlerimizi sürekli geliştiriyoruz.

Son olarak bulunduğumuz noktada güvenlik yapımız içerisinde Splunk, merkezi olarak konumlandırdığımız kritik ürünlerden biri olarak yer alıyor.

Splunk'ın bu şekilde konumlandırılması, nasıl bir fark yarattı güvenlik ve koruma anlayışınızda?

S. ÇOLAK: Gelişen teknolojilerle birlikte yeni tehdit ve riskler de hayatımıza giriyor, biz de altyapımızı bu doğrultuda güncelliyoruz. Splunk ile beraber, kendi kendine öğrenen bir sisteme geçmiş olduk. Belli başlı trendleri sistem kendisi anlayıp bize uyarılarda bulunuyor. Bu yeni yapıyı oluşturmak için Splunk'ın bize sağlamış olduğu en iyi referansların bilgi birikiminden yararlandık. Yurtdışından farklı tecrübelere sahip ekiplerin geliştirmiş olduğu, farklı atak türlerini tespit etmeye yönelik yöntemleri de kendi sistemlerimiz içerisine almış olduk. Splunk sadece bir güvenlik olay yönetimi aracı değil aynı zamanda büyük veri analiz platformu olmasından dolayı güvenlik analizi süreçlerine, tehdit avcılığına (threat hunting) oldukça hız kazandırdı.

PROJE ADIMLARI

- >> Güçlü uygulamalar, global kütüphaneler kullanılarak ve süreç sahipleriyle düzenli toplantılar yapılarak, Anahtar Performans Göstergeleri (KPI) belirlendi.
- >> KPI'ların hesaplama metotlarına uygun olacak şekilde sistem entegrasyon ve geliştirme gereksinimleri analiz edildi.
- >> KPI'lar, kişisel, organizasyonel ve stratejik hedeflerle olan ilişkilerine göre sınıflandırıldı.
- >> Kapsamda belirtilen KPI'lara ait gösterge panelleri tanımlandı.
- >> Oluşturulan KPI'ların ölçümlenmesiyle birlikte, süreç sahipleri ile sonuçlara dair mutabakatlar yapıldı.

Hayata geçirdiğiniz bu projelerin ardından üst yönetim tarafında nasıl bir dönüşüm yaşandı?

S. ÇOLAK: KKB'nin, genel müdüre bağlı genel müdür yardımcıları ve direktörlerden oluşan bir Üst Yönetimi bulunuyor. Splunk ile hayata geçirdiğimiz KPI izleme altyapısını kurum içerisinde kullandığımız pek çok uygulama ile entegre ettik. Üst Yönetimimizi oluşturan yöneticilerimiz, böylece süreçsel ve operasyonel performansı izleyebilecekleri bir görselleştirme altyapısına kavuşmuş oldular. Dolayısıyla Üst Yönetimimizi yeni

analiz yetenekleri ile desteklemiş olduk. Ayrıca bilgi güvenliği tarafında da üst yönetim ile iletişim anlamında önemli kazanımlar elde edildi.

Bilgi güvenliği tarafında üst yönetimi etkileyecek ne gibi kazanımlar elde edildi?

S. ÇOLAK: Belirttiğim gibi daha önce de merkezi olarak adreslediğimiz bir güvenlik sistemimiz vardı. Dolayısıyla bizim beklentimiz mevcut sistemi hem geliştirebilecek hem de mevcut sistemdeki tüm noktaları kapsayacak bir altyapıya ulaşmaktı. Bilgi Güvenliği ölçülmesi zor bir kavramdır. Splunk ile beraber Bilgi Güvenliği süreçleri için yüzden fazla metriği ölçmeye başladık. Bu sayede kurumumuzun güvenlik görünümünün sürekli olarak gelişimini, iyileşmesini sağlayabiliyoruz. Bugünün metrik değerlerinin, dünden, yarının değerlerinin de bugünden iyi olması için öncelikle sağlıklı bir ölçüm mekanizması gereklidir.

Zaafiyet Yönetimi, Yazılım Güvenliği, Sistem Güvenliğine dair tüm kritik süreçlerin metriklerini Üst Yönetim ile paylaşıyoruz. Bu da güvenlik süreçlerinde şeffaflığı sağlarken aynı zamanda güvenlik süreçlerine üst yönetimin aktif katılımını sağlıyor.

Buna neden ihtiyaç duydunuz?

S. ÇOLAK: Finans dünyasında bilgi güvenliği, yönetim kurulu seviyesinde tartışılan, yatırım kararları en üst seviyelerde alınan bir konu haline geldi. Dolayısıyla buradaki riskleri daha güçlü bir şekilde ön plana çıkarabilmek için anlaşılır bir şekilde sunabilmek gerekiyor. Bunun da en iyi yolu, gerçek verilerden oluşan raporlamaları

ELDE EDİLEN SONUÇLAR VE FAYDALAR

- >> Yaklaşık 400 insan/gün ile gerçekleştirilen bir çalışmanın sonucunda, 773 iş süreci için 697 KPI belirlendi.
- >> KPI'ların %86'sı sistemlerde oluşan verilerden beslenecek şekilde uygulamalara adreslendi.
- >> Belirlenen KPI'ların %74'ü doğrudan performans ölçümü, %26'sı ise bilgi sağlayıcı olarak sınıflandırıldı.
- >> Performans KPI'larının türlerinin dağılımı %54'ü zaman, %39'u kalite ve %7'si maliyet ölçümüne yönelik olacak şekilde belirlendi.
- >> "Fikirden Ürüne" süreçlerini kalite ve zaman açısından doğrudan etkileyen süreçleri kapsayan 301 KPI, gösterge panelleri üzerinde görselleştirildi.
- >> Tüm bu çalışmaların paralelinde, yazılım ve sistem güvenliğine yönelik KPI'lar da ayrıca takip edilmeye başlandı.
- >> Üst yönetimin objektif kararlar verebilmesini destekleyen ve üst yönetim tarafından çok sık kullanılan bir KPI izleme ve raporlama yapısı kurulmuş oldu.
- >> Süreçlerde verimliliğin düşük olduğu noktalar tespit edilerek, iyileştirme yapılması sağlandı.
- >> Üretim kalitesini ve hızını artırıcı bir etki yaratıldı.
- >> Yatırım kararlarının verilmesi kolaylaştı ve daha fazla veriye dayalı hale getirildi.

üretebilmekten, bir bakışta anlaşılabilecek gösterge panelleri tasarlamaktan geçiyor. Biz de buna yönelik bir çalışma yaptık.

Projelerin hayata geçiriliş sürecinde, Splunk iş ortağı Seynur ile yürütülen işbirliğini değerlendirir misiniz?

S. ÇOLAK: Seynur, Splunk uygulaması konusunda Türkiye'deki en eski danışmanlık firmalarından biri. Bünyesinde son derece yetkin veri madencileri bulunuyor. KPI projesi kapsamında Seynur'dan etkin bir destek aldık. Gereksinim analizlerinin yapılması, entegrasyonlar ve Splunk uygulaması üzerinde tanımlanan gösterge panellerinin tanımlanması çalışmalarında çok yakın çalışma imkânı bulabildik. Bu da proje sürecinde karşımıza çıkan değişikliklere ve güncellemelere hızlı bir şekilde adapte olabilmemizi sağladı.

Merkezinde Splunk çözümlerinin yer aldığı geleceğe yönelik planlarınız var mı?

S. ÇOLAK: Mevcut durumda yöneticilerimiz, Splunk uygulaması üzerinde tanımlanmış KPI'lardan faydalanmaya başlamış durumdalar. Önümüzdeki dönemde, sistem üzerinden görüntülenip raporlanabilecek KPI'lar ve gösterge panelleri önceliklendirilerek, kurumdaki tüm süreçlere yaygınlaştırılması sağlanacak. Ayrıca, tanımlanan gösterge panellerine ilişkin ihtiyaç duyulacak yeni KPI ve/veya gösterge panellerinin oluşturulmasına yönelik çalışmalar yürütülmesi de gündemimizde yer alıyor.

KREDİ KAYIT BÜROSU HAKKINDA

Kredi Kayıt Bürosu (KKB), sektörün önde gelen 9 bankasının ortaklığı ile 11 Nisan 1995 tarihinde kuruldu. KKB'nin, bankalar, tüketici finansman şirketleri, leasing, faktoring ve sigorta şirketleri olmak üzere 200'e yakın üyesi bulunuyor. KKB, üyelerinden topladığı müşteri bilgilerini birleştirerek ürettiği bilgileri, kredi risk yönetim süreçlerinde kullanılmak üzere yine üyeleri ile paylaşmayı sağlayan bir yapıda hizmet sunuyor.

2013 yılı Ocak ayında hayata geçirdiği Çek Raporu ve Risk Raporu hizmetleri ile KKB, yalnız finansal kuruluşlara değil aynı zamanda bireylere ve reel sektöre yönelik hizmetler de sunmaya başladı. Kişi ve kurumların finansal itibarlarını yönetebilmeleri için önemli araçlar sunan KKB, 2014 yılında bireylere ve reel sektöre yönelik olarak tasarlanan finansal hizmet platformu Findeks'i kullanıma açtı. 2015 yılında hayata geçen, 2016 yılında yasa ile kullanımı zorunlu hale gelen ve 1 Ocak 2017 itibarıyla yürürlüğe giren Findeks Karekodlu Çek Sistemi ile KKB daha şeffaf ve güvenli bir ticari hayat için oldukça önemli bir adım atılmasını sağladı. Bununla birlikte, 2016 Aralık ayında faaliyete başlayan KKB Anadolu Veri Merkezi ile başta bankacılık ve finans sektörü olmak üzere kurumlara yönelik veri merkezi ve olağanüstü durum merkezi hizmetlerini sunan KKB, finansal teknoloji alanında yürüttüğü faaliyetlerini geliştirerek sürdürüyor. 2020 yılı itibarıyla hayata geçirilen KKB Ar-Ge Merkezi ile KKB, yenilikçi ürün ve hizmetlerini inovasyon ve teknolojiyi merkeze alarak geliştirmeye devam ediyor.

Pandeminin etkilerini ve buna yönelik gösterge panellerinde ortaya çıkan sonuçları sormak istiyoruz. Splunk altyapısından bu süreçte de yararlandınız mı?

S. ÇOLAK: Elbette yararlandık. Veriye ve bilgiye ihtiyaç bu süreçte de kendisini gösterdi. Özellikle kriz dönemlerinde ne kadar çok veriye sahip olursanız ve bunu ne kadar çok bilgiye çevirebilirseniz, işinize hâkimiyetiniz o kadar artıyor. Biz de pandemi ile beraber iş yapış şeklimizi değiştirdik ve uzaktan çalışma modeline geçtik. Dolayısıyla uzaktan erişimi sağlayan sistemlerden almamız gereken farklı raporlama ihtiyaçları doğdu. Uzaktan çalışma sürecini destekleyen altyapıların performansı ve güvenliği yakından takip ettiğimiz konular olarak ön plana çıktı. Pandemi sürecinin başından itibaren Splunk ile farklı gösterge panelleri ve raporlamalar tasarladık. Hatta şirketin genel olarak pandemi sürecindeki verimliliğini, yani uzaktan çalışma etkisini değerlendirebileceğimiz üst düzey raporlar oluşturduk. Özetle, Splunk sistemini kullanarak, çeşitli değerlendirmeler ve analizler yapma fırsatı elde ettik.

SEYNUR HAKKINDA

2006 yılında kurulan ve 2010 yılından bu yana Splunk ile iş ortaklığı olan Seynur, güvenlik, veri analizi ve veri inceleme alanlarındaki uzmanlığı ile öne çıkıyor ve müşterilerine veri odaklı çözümler sunmayı hedefliyor. Redington ekosisteminin değerli bir üyesi olan Seynur, Türkiye'yi Splunk ile ilk kez 2010 yılında tanıştıran teknoloji şirketi olarak da biliniyor.

Verimlilik sonuçları nasıldı?

S. ÇOLAK: Pandemi döneminde, üye ve müşterilerimizden gelen talepleri karşılama noktasında iş hacmimizin artış göstermesiyle birlikte verimliliğimizin de aynı oranda artış sağladığını söyleyebiliriz.

Bu süreçte gerçekleştirdiğimiz verimlilik değerlendirme ve analiz çalışmaları sonucunda özellikle 2020 yılı Mart ve Temmuz ayları arasında üretim hattı performansında yüksek oranda bir artış tespit ettik.

SPLUNK HAKKINDA

Splunk, veri ve eylem arasındaki engelleri ortadan kaldırarak, Veri Çağında herkesin başarılı olması için tasarlanan dünyanın ilk "Veriden Her Şeye" platformunu sunuyor. Splunk, IT operasyonlarının yönetimi/izlenmesi ve yüksek güvenlik ihtiyaçlarına çözüm getiren web tabanlı bir yazılım platformu. Log dosyaları, config dosyaları, diğer uygulamalardan gelen uyarı mesajları gibi onlarca farklı kaynaktan gelen bilgileri gerçek zamanlı olarak analiz edip indeksliyor, içerisinde arama yapılmasını sağlıyor ve bunlardan grafikler, raporlar, uyarılar ve izleme ekranları oluşturabiliyor. Kuruluşların IT'ye yönelik güvenlik risklerini ortadan kaldıran, kullanımı kolay, bakım gerektirmeyen Splunk, dünyada kurumsal big data projelerindeki başarılı kullanımı ile de dikkat çekiyor.

BT, DevOps ve güvenlik ekiplerini, kuruluşlarının dijital dönüşümünü, herhangi bir kaynaktan, herhangi bir zaman ölçeğinde sağlanan verilerle gerçekleştirebilmeleri için güçlendiriyor.

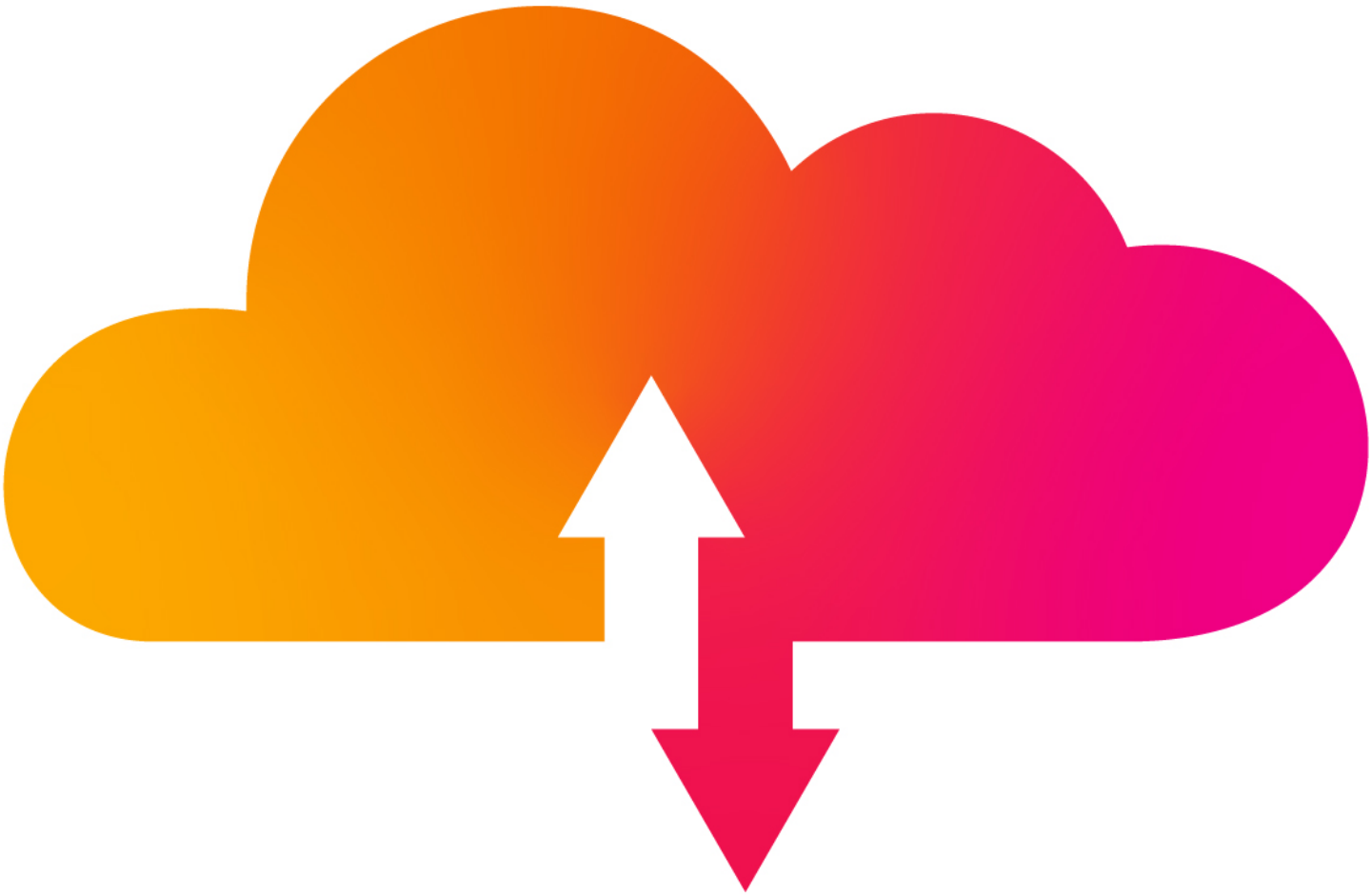
Redington | splunk>

360º VERİ ANALİZİNDE

TÜM ÇÖZÜMLER TEK ADRESTE

SPLUNK CLOUD

Şirketinizin iş ve müşteri anlayışını derinleştirmek, siber güvenlik risklerini azaltmak, hizmet performansını iyileştirmek ve maliyet avantajı sağlamak için 360º veri analizi ve faydaya dönüştürülebilir içgörüler sunan Splunk Cloud'u tercih edin. "All-in cloud" çözümü sunan Splunk Cloud ile, ihtiyacınız olan tüm güvenlik ve analize tek çözümle sahip olun.



- Bulut hizmeti aracılığıyla sıfır altyapı maliyeti
- 2 gün içinde yayına erişim
- %100 çalışma süresi garantisi
- 700 üzerinde zengin splunkbase uygulaması
- Çoklu bulut özelliği

Bilişim ekosisteminin birleştirici gücünü yakından tanımak için,
redington.com.tr • 0216 316 50 50

“Güçlü bir distribütörün varlığı pazarın büyümesine de katkıda bulunuyor”

Seynur BT, Redington ekosisteminin alanında uzmanlaşmış, global platformlarda da kabul gören, bilgisine başvurulan değerli bir üyesi. Seynur BT Genel Müdürü Selim Seynur ile Redington Türkiye ekosisteminde yer almanın kendilerine sağladığı katkılar, Splunk teknolojileri ve Splunk üzerinde geliştirdikleri MITRE ATT&CK App hakkında görüştük.

Seynur BT’nin Splunk uzmanlığı, artık global platformlarda da bilinen bir durum. Öncelikle, sahip olduğunuz deneyim hangi yıllara uzanıyor öğrenebilir miyiz? 2021 yılına hangi yollardan geçerek geldiniz?

SELİM SEYNUR (Seynur BT-Genel Müdür): Aslında, bir kaç cümleye sığacak şekilde anlatabileceğim bir hikayemiz var. Splunk, bilindiği gibi 2004 yılında kurulmuş, yıkıcı/yenilikçi teknolojisi ile dikkat çekmiş ve bugüne gelmiş bir teknoloji şirketi. Benim Splunk ile tanışmam 2005 yılında oldu. O sırada, yine bilgi güvenliği alanında, yurtdışında çalışıyordum. Bir proje vesilesiyle değerlendirdiğimiz SIEM (Security Information and Event Management – Güvenlik Bilgileri ve Olay Yönetimi)

SELİM SEYNUR
Genel Müdür / Seynur BT

ürünleri arasında Splunk da yer alıyordu. O zaman, daha ilk versiyonu bile Beta halindeydi ama ilgimi çekmişti. 2006 yılının sonuna doğru Türkiye'ye döndüm ve sonrasında 2008'de Teknokent'te Security as a Service modelinde bir projemiz için Splunk'ı değerlendirdik. O yıllarda Splunk henüz bilinmiyordu ama benim Splunk ile iletişimim hep devam etti. 2010 yılına geldiğimizde Splunk ile bir anlaşma yaptık ve iş ortağı olduk. 2011 yılında da Splunk'ın Türkiye'deki ilk müşterisi için hizmet verdik.

> "Redington'ın Türkiye'ye gelmesiyle birlikte, hem ticari taraftaki çoğu finansal soru işaretlerini, hem de müşteri tarafındaki çekinceleri ortadan kaldıran bir yapı oluştu. Ayrıca, iş ortağı ağının büyümesi, pastanın büyümesine de katkıda bulundu."

Splunk iş ortağı olarak Redington Türkiye çatısı altına girmeniz nasıl gerçekleşti?

S. SEYNUR: O yıllarda Splunk'ın Türkiye'de yaygınlaşma konusundaki en önemli engeli güçlü bir distribütörünün olmayışıydı. 2016 yılında, o zamanki adıyla LinkPlus şimdiki adıyla Redington Türkiye ile bir distribütörlük anlaşması imzalandı. Bu gelişmeyle birlikte de hakikaten Splunk'ın sektördeki bilinirliği ve yaygınlığı artmaya başladı.

Sizin için Redington Türkiye'nin nasıl etkileri, avantajları oldu?

S. SEYNUR: Güçlü bir distribütörün varlığı pazarın büyümesine de katkıda bulunuyor. Redington'ın Türkiye'ye gelmesiyle birlikte, hem ticari taraftaki çoğu finansal soru işaretlerini, hem de müşteri tarafındaki çekinceleri ortadan kaldıran bir yapı oluştu. Ayrıca, iş ortağı ağının büyümesi, pastanın da büyümesine katkıda bulundu. Belki bizim rakiplerimiz arttı ama genele bakıldığında bunun olumlu etkilerini yaşadığımızı düşünüyorum. Bunun elbette bizim iş yapma anlayışımızla da yakından ilgisi var.

Türkiye'deki sistem entegratörü mantığıyla, ürün yelpazesini genişletip çok satış yapmaya odaklanan bir yapımız yok. Biz dikey bir yaklaşımla iş yapıyoruz. Bu pazarda, sahip olduğumuz uzmanlık ve entelektüel sermayenin ciddi bir değeri var. Derinleştiğimiz hizmetlerle öne çıkıyoruz. Dolayısıyla iş ortağı ağının artması pastanın büyümesi ve iş fırsatlarının artması anlamına da geliyor. Ayrıca, farklı iş ortaklarıyla sinerji yakalamamız, iş ortaklığı yapmamız da mümkün oluyor.

Bunların dışında Redington Türkiye distribütörlüğünün, pazarlama ve tanıtım faaliyetleri açısından da olumlu etkilerini yaşadık. Örneğin, pandemi öncesinde düzenlenen Splunk Dicovery Day, Splunk uzmanlarını, Splunk müşterilerini ve iş ortaklarını bir araya

> **“Redington Türkiye distribütörlüğünün, pazarlama ve tanıtım faaliyetleri açısından da olumlu etkilerini yaşadık. Örneğin, pandemi öncesinde düzenlenen Splunk Dicovery Day, Splunk uzmanlarını, Splunk müşterilerini ve iş ortaklarını bir araya getiren çok verimli bir etkinlik oldu.”**

getiren çok verimli bir etkinlik oldu. Bu tip etkinliklerin çok faydası olduğuna inanıyorum ve pandemi sonrasında yeniden bu tip etkinliklerde buluşmayı özlemle bekliyoruz.

Splunk’ın en eski kullanıcısı ve iş ortağı olarak, Türkiye pazarındaki gelişimine yakından tanıklık ettiniz. Bize biraz izlenimlerinizi anlatır mısınız?

S. SEYNUR: Splunk çok başarılı bir üretici. Ürünün kendisi de pazarlaması da çok başarılı. Biz de bunun avantajlarını yaşıyoruz. Elbette Türkiye’de tanınmasında Seynur olarak bizim de katkımız oldu. Kapı kapı dolaşıp Splunk anlattığım bir dönemin birikimi de var mutlaka. Bütün bunlar ve distribütörün de katkısı bir araya gelince, ayrıca Gartner gibi bağımsız araştırma kuruluşlarının raporları da liderliğini tescilleyince, Türkiye’de kaçınılmaz bir başarı elde etmeye, talep görmeye başladı. Öyle ki müşteri aramaya vaktimiz olmuyor, gelen talepler doğrultusunda ilerliyoruz. Sadece kaliteli hizmet vermeye odaklanıyoruz ve Splunk da bize bunu sağlıyor. Müşteri tarafında güven uyandıran bir distribütörün desteği de olunca, ilerlemek herkes için çok daha kolay oluyor.

Splunk’ın bir çok alanda kullanılması mümkün ama istisnaları olsa da siz daha çok IT Opersyonu ve Güvenlik alanında uzmanlaştınız. Neden?

S. SEYNUR: Çünkü, her şeyi yapabilirsiniz ama her şeyi iyi yapamazsınız. “İyi olduğumuz alanda derinleşmek daha değerlidir” diye düşünüyoruz. Evet, bizim asıl derinleştiğimiz alan güvenlik olsa da Splunk aslında bir veri platformu ve bu platform ile ‘n’ tane farklı kullanım senaryosuna dokunabilirsiniz. Hatta başlangıçta, “Bu veri platformunu nasıl kullanırız, BI’da kullanır mıyız IoT’de kullanır mıyız” diye inceledik. Sonra odağımızı sınırlamamız gerektiğine karar verdik. Son üç dört yıldır da IT Operasyonu ve Güvenlik alanlarında hizmet veriyoruz. Elbette “Splunk ve IoT kullanım senaryosu” için bize gelen bir talebi de reddetmiyoruz ama açıkça asıl uzmanlık alanımızı belirtiyoruz. Lisans satmaktan çok, çözüm üretmeye odaklıyız. Çözüm üretebildiğimiz sürece de lisans satışı zaten kendiliğinden geliyor.

IT Opreasyonu ve Güvenlik konularında çözüm geliştiriyorsunuz. Peki IT ve Güvenlik orkestrasyonu tarafında çözümü var mı Splunk’ın?

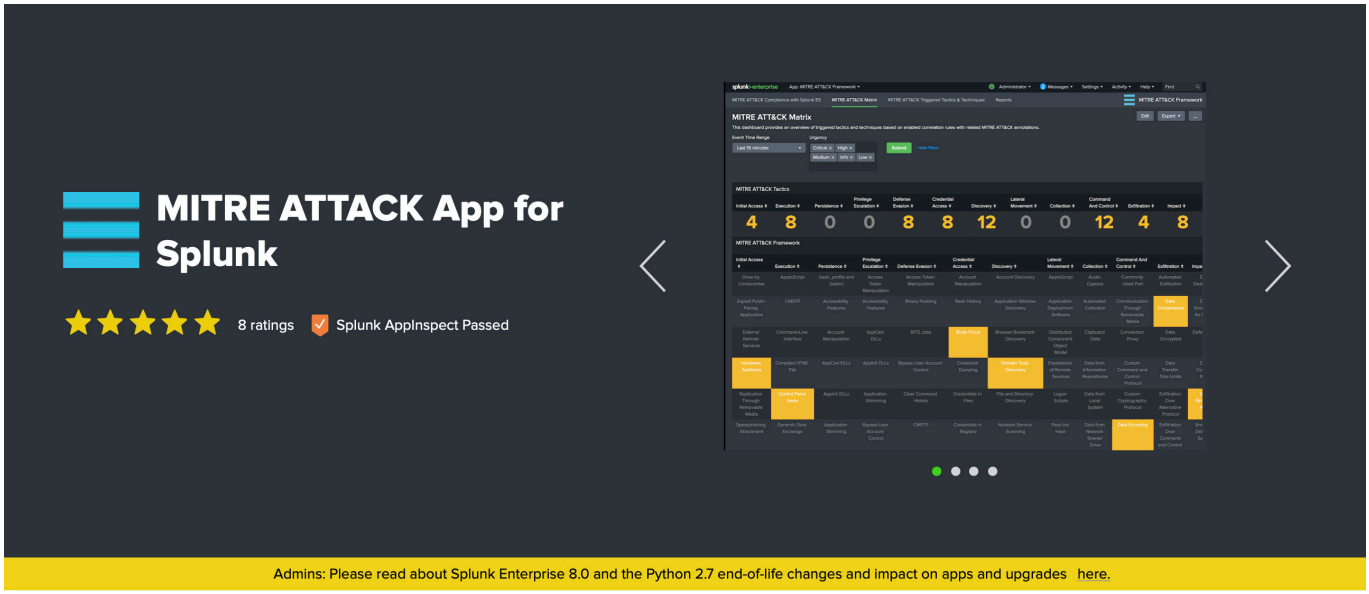
S. SEYNUR: Splunk’ın Güvenlik Orkestrasyonu ve Otomasyonu

konusunda Phantom adını verdiği bir ürünü var. IT Operasyonu tarafındaki orkestrasyon için de VictorOps diye bir ek ürünü daha var. Hatta bu ürün, son olarak Splunk On-Call adını aldı. Fakat bunların piyasada yaygınlaşması için biraz daha zaman var. Henüz kuruluşlar bu tarz yaklaşımlar için hazır değiller. Az sayıdaki kuruluş merak ediyor ve ilgileniyor ancak tıpkı yapay zeka ve makine öğrenmesinde olduğu gibi daha işin çok başındalar. Elbette zaman içerisinde bu konuları da müşterilerimizle değerlendireceğiz. Her kuruluş, belli olgunluk seviyelerine geldikçe, ihtiyaçları da artacak. Biz de o ihtiyaçları destekleyecek bilgiyi ve ürünleri sağlayabileceğiz.

Sizin Seynur olarak Splunk uzmanlığınızı bir anlamda tescilleyen ve global bilinirliğinize de katkıda bulunan bazı uygulamalarınız da var. Biraz bu konudan da söz edebilir miyiz?

S. SEYNUR: Splunk için geliştirdiğimiz MITRE ATT&CK aplikasyonu, özellikle Amerika'da epey talep gördü. İndirilme sayısı 6 bin 500'e ulaştı. İlk versiyonunu Haziran 2019'da, son versiyonunu ise 14 Nisan'da (2021) yayımladık. Güncellemeye de devam ediyoruz. MITRE (mitre.org), Amerika'da devletle yakın çalışan bir araştırma organizasyonu. Burada, MITRE ATT&CK adı altında, güvenlikle ilgili atakların incelendiği bir framework de var. Bu yapı altında pek çok çalışma yapmak ve aplikasyon geliştirmek mümkün. Güvenlikle ilgilenen mühendisler, Güvenlik Operasyon Merkezi tarafında çalışan analistler, araştırmacılar, MITRE ATT&CK altyapısını kullanarak, atağın süreci, atak süresince neler olduğu ve bunların nasıl belirleneceğiyle ilgili araştırmalar yapıyorlar. Bizim geliştirdiğimiz "MITRE ATT&CK for Splunk" ile yaptığımız da bu framework'ü Splunk üzerinde uygulanabilir hale getirmek oldu. Bu da aslında, bir müşterimizden gelen talep üzerine oldu. Bize, "Gelen saldırıları görselleştirmek istiyoruz, nasıl yapabiliriz" diye bir soru ile geldiler. Orada framework'ün kendi içinde kullandığı görseller, araçlar var. Biz bunları ilk etapta Splunk üzerinde görselleştirdik. Splunk'ın zaten SIEM modülü de var. Onunla entegre olacak şekilde işe başladık, daha sonra gelen taleplerle beraber işin boyutu değişti. Dediğim gibi Nisan sonu itibariyle MITRE ATT&CK for Splunk, yaklaşık 6500 indirilme sayısına ulaştı. Aktif kurulumu ise 2 bin 100 civarında.

"Splunk için geliştirdiğimiz MITRE ATT&CK aplikasyonu, özellikle Amerika'da epey talep gördü. İndirilme sayısı 6 bin 500'e ulaştı. İlk versiyonunu Haziran 2019'da, son versiyonunu ise 14 Nisan'da (2021) yayımladık."



İndirmelerin bölgelerdeki dağılımı nasıl?

S. SEYNUR: İndirmelerin yaklaşık yüzde 50'si Amerika kaynaklı. Türkiye'den indirme sayısı maksimum 20 adede ulaşıyor ki bu da normal. Kalanı ise İngiltere, Almanya, Fransa, Avusturya gibi daha çok Avrupa ülkelerinde dağılıyor.

Bu gelir getirici bir faaliyet olamamakla birlikte Seynur isminin global çapta bilinirliği için önemli olmalı, değil mi?

S. SEYNUR: Gelir elde etme amacı gütmeyen çalışmalar bunlar ve açık kaynak kodlarla yer aldık zaten. İndirenler, uygulamayı bütün kodlarıyla indiriyorlar. Bizim burada eklediğimiz bir değer de söz konusu. MITRE framework'te, gelen saldırıların fark edilmesini sağlayan kuralların belirlenmesi konusu var. Splunk'ın Enterprise Security çözümü, hazır kurallarıyla geliyor. Bu kuralların MITRE framework kurallarına uygun olanları, yani eşleşenleri var. "MITRE ATT&CK for Splunk", şu aşamada genişletilmiş kuralların olduğu kendi aplikasyonumuzla entegre durumda. Belli sayıda kuralı zaten Splunk kullanıcısı olmasanız da ücretsiz olarak MITRE üzerinden indirip kullanmanız mümkün. Biz de bunlara ek olarak kendi geliştirdiğimiz API (www.seynur.com/api) hizmeti ile indirilebilen yeni kurallar yazıyoruz bir yandan ve bu iş için belli bir kaynak ayırıyoruz. Belki ileride bu kurallarla zenginleştirdiğimiz kendi aplikasyonumuzu ticari bir ürüne dönüştürme şansımız da olabilir.

Ancak sizin de dediğiniz gibi bu çalışmanın bilinirliğimize katkısı olduğunun biz de farkındayız. Dünyanın farklı ülkelerinden e-posta ile sorular gelmesinden ve bu sorulara cevap vermekten memnuniyet duyuyoruz.