platin
Bilişim Teknolojileri

www.platinbilisim.com.tr

LC Waikiki* Platin Bilişim Uzmanlığında

Log Yönetimini İleri Seviyeye Taşıyarak İş Verimliliğini Artırdı!

Endüstri: Moda Perakende

LC Waikiki Hakk ında:

1985 yılında kurulan ve 1997 yılından bu yana Türkiye'de LC Waikiki Mağazacılık çatısı altında hizmet veren LC Waikiki, "İyi giyinmek herkesin hakkı" misyonu ve "ulaşılabilir moda" anlayışıyla Türkiye'yi giydiriyor. LC Waikiki, büyüme serüvenini 18 yıldır hem yurt içi hem de yurt dışında sürdürüyor. Perakende moda sektörünün lideri LC Waikiki, bugün 25 ülkede 530'u aşkın mağazası ve 25.500 çalışanıyla hizmet veriyor. Firma hakkında daha detaylı bilgiye www.lcwaikiki.com sitesi üzerinden erişilebilir.

"Platin Bilişim desteğinde başlayan proje planıyla beraber 1 aylık kısa bir zamanda kritik durumdaki tüm log kaynaklarımızdan logların sağlıklı bir şekilde toplanması sağlandı."

BT Altyapı Teknolojileri Geliştirme ve Operasyon Müdürü,

Osman YALÇINTEPE

Değerinizi Korur I Saves Your Value

Çözüm:

Öncelikle, kapsamlı bir analiz gerçekleştirilerek proje geçiş safhaları belirlendi. Ardından, LC Waikiki bünyesinde 2 Güvenlik Grubu çalışanı ve IT yönetimi olmak üzere Platin Bilişim ile birlikte olan toplam 8 kişilik bir ekiple birlikte 1 aylık bir süreç içerisinde IBM QRadar SIEM kurulumu tamamlanarak LC Waikiki'nin kritik durumdaki tüm log kaynaklarından logların sağlıklı bir şekilde toplanması sağlandı bu yeni yapıya geçiş gerçekleşti.

Sonuç:

- **LC Waikiki, 5651 No'lu yasa kapsamında kanuni olarak değiştirilemez şekilde log kaydı alınmasını ve zaman damgası ile damgalanmasını sağlamış oldu.**
- **LC Waikiki bünyesinde tüm operasyonel cihazlarının loglarının toplanarak gizililiği, bütünlüğü ve erişilebilirliği sağlandı.**
- **Uygulama ve Yönetim kolaylaşmış oldu.**
- **Daha az bakım ihtiyacı ve yönetimsel ihtiyaç oluştu. Daha geniş iş hacmi için hizmet**

emniyeti daha güvenilir bir hale geldi.

Platin Bilişim – IBM QRadar çözümü ile LC Waikiki'nin Log Yönetimi ihtiyaçlarının eksiksiz bir biçimde karşılanmasına ve firmanın yeni nesil teknolojilere hazır olmasına yardımcı oldu.

Hazır giyim sektörünün lider firmalarından LC Waikiki, log yönetimi ve güvenlik zekası çözüm ortağı olarak Platin Bilişim'i tercih etti. Platin Bilişim'in uzman ekibi tarafından kurulumu yapılan IBM QRadar SIEM ile birlikte, LC Waikiki log yönetiminde daha iddialı bir hale gelirken, hem operasyonel süreçlerini daha iyi yönetecek hem de 5651 yasasına tam uyum sağladı.

Giderek dijitalleşen dünya, internet kullanımının yaygınlaşması ve BYOD (kendi cihazını getir) gibi farklı iş modellerinin gelişimiyle birlikte tüm kurumsal şirketlerde log yönetimi ve güvenlik zekası çözümleri artan bir ihtiyaç haline dönüştü. "İyi Giyinmek Herkesin Hakkı" felsefesi ile bugün 25 ülkede 531 mağazada uygun fiyata kaliteli ürünler sunarak müşterilerine ulaşılabilir modanın keyfini yaşatma iddiasındaki LC Waikiki firması da hem kanuni açıdan kritik kaynaklara ait logların değiştirilemez bir şekilde 5651 sayılı yasaya uyumluluk sağlayabilmek adına toplanması ve zaman damgasıyla imzalanması için hem de güvenlik açısından düşünüldüğünde ise tüm operasyonel cihazlarının loglarının toplanarak gizililiğinin, bütünlüğünün ve erişilebilirliğinin sağlanması ve tüm kaynakların korelasyon/uyarı mekanizmalarının oluşturularak proaktif bir güvenlik olay izleme yapısı kurmak amacıyla gelişmiş ve etkin bir log yönetimi çözümüne ihtiyaç duymaktaydı.

Bu noktada pazarda kapsamlı bir araştırma yaparak potansiyel çözümleri inceleyen LC Waikiki yetkilileri, Platin Bilişim hizmetleri uzmanlığında sunulan ve kullanım kolaylığına ek olarak, ağa yayılmış binlerce aygıt uç noktasından ve uygulamadan gelen günlük kaynağı olay verileriyle birleştirebilen ve gerçek tehditleri hatalı pozitif sonuçlardan ayırmak amacıyla işlenmemiş verilerde anında normalleştirme ve ilişkilendirme etkinlikleri gerçekleştirebilen IBM QRadar SIEM çözümünü tercih ettiler.

LC Waikiki, Platin Bilişim uzmanlığında kurulumu yapılan IBM QRadar çözümü ile hem kanuni yükümlüklerini eksiksiz olarak yerine getirirken hem de tüm kaynakların korelasyon/uyarı mekanizmalarının oluşturularak proaktif bir güvenlik olay izleme yapısına kavuştu. LC Waikiki, üstün hizmet anlayışlarından dolayı gelecekte de Platin Bilişim ile birçok konuda çalışma planları bulunduğunu ve kesintisiz destek ve hizmet anlayışlarından dolayı kendilerine teşekkür ettiklerini belirtti.

Projenin Zorlukları:

Projede karşılaşılan en temel zorluk, her gün 100'lerce mağazasında satış işlemleri devam eden ve binlerce sevkiyat gerçekleştiren LC Waikiki'nin operasyonel süreçlerinde herhangi bir kesinti olmaksızın mevcut log yönetimi sisteminin devre dışına alınarak IBM QRadar kurulumunun hızlı ve etkin bir biçimde kurulumunun sağlanmasıydı. Bu sayede firmanın sadece 5651 No'lu Kanun ile belirlenen kanuni gereksinimlere tam uyum sağlanmasıyla yetinilmeyerek teknolojik açıdan daha proaktif, güven veren bir yapıya kavuşması sağlanacaktı. LC Waikiki bünyesinde 2 Güvenlik Grubu çalışanı ve IT yönetimi olmak üzere Platin Bilişim ile birlikte toplam 8 kişilik bir ekiple birlikte 1 aylık bir süreç içerisinde bu yeni yapıya geçiş sağlandı.

"Kurumsal şirketlerde log kayıtlarını doğru bir biçimde saklayabilmek veanaliz edebilmek de giderek daha kritik hale geliyor."

Ayhan Bamyacı, Platin Bilişim Genel Müdürü

Platin Bilişim Uzmanlığında Gelen Çözüm!

Öncelikle, kapsamlı bir analiz gerçekleştirilerek proje geçiş safhaları belirlendi. Ardından, LC Waikiki bünyesinde 2 Güvenlik Grubu çalışanı ve IT yönetimi olmak üzere Platin Bilişim ile birlikte toplam 8 kişilik bir ekiple birlikte 1 aylık bir süreç içerisinde IBM QRadar SIEM kurulumu tamamlanarak LC Waikiki'nin kritik durumdaki tüm log kaynaklarından logların sağlıklı bir şekilde toplanması sağlandı bu yeni yapıya geçiş gerçekleşti.

Konu hakkında açıklama yapan LC Waikiki Mağazacılık BT Altyapı Teknolojileri Geliştirme ve Operasyon Müdürü Osman Yalçıntepe şu ifadeleri kullanıyor: *"LC Waikiki olarak halihazırda yapımızda kullanmakta olduğumuz Log Yönetimi uygulamamız tam anlamıyla beklentilerimizi karşılayamıyordu. Kullandığımız çözüm, kanuni açıdan gereksinimlerimizi yani kritik kaynaklara ait logların değiştirilemez bir şekilde 5651 sayılı yasaya uyumluluk sağlayabilmek adına toplanması ve zaman damgasıyla imzalanması ihtiyacını karşılamakla birlikte; network üzerindeki anormalliklerin ve güvenlik olaylarının gözlemlenemediği bir çözümdü. Tüm operasyonel cihazlarımızın loglarının toplanarak gizililiğinin, bütünlüğünün ve erişilebilirliğinin sağlanması ve tüm kaynakların korelasyon/uyarı mekanizmalarının oluşturularak proaktif bir güvenlik olay izleme yapısı kurmak amacıyla kapsamlı bir çözüme ihtiyacımız vardı. Bu konuda piyasadaki ürünleri araştırdığımızda karşımıza uluslararası platformda üç ürün çıktı. Bu ürünler ile tek tek POC çalışmaları yapıldı. Güvenlik Mühendislerimizin titiz çalışmasının ardından IBM QRadar SIEM ürününe karar verildi. Ardından Platin Bilişim desteğinde başlayan proje planıyla beraber 1 aylık kısa bir zamanda kritik durumdaki tüm log kaynaklarımızdan logların sağlıklı bir şekilde toplanması sağlandı.*

”Platin Bilişim Genel Müdürü Ayhan Bamyacı ise şu açıklamayı yapıyor: *“Kurumsal şirketlerde log kayıtlarını doğru bir biçimde saklayabilmek ve analiz edebilmek de giderek daha kritik hale geliyor. Güvenlik zekası çözümleri şirketlerin network trafik verilerini işleyebilmelerini ve toplanan diğer standart loglar ile birlikte korelasyonlara tabi tutabilmelerini sağlıyor. Ancak bu çözümü sağlayan ürünlerde kullanım kolaylığı önemli bir kriter. Arka planda çok kompleks işler söz konusu. Qradar, bu karmaşık yapıyı kullanıcıların önüne kolay bir arayüzle sunmayı başarabiliyor. Kullanıcılar, Outlook’ta kural oluşturmaya benzeyen basit adımlarla kendi ihtiyaçlarına uygun yapıları kurgulayabiliyor. LC Waikiki ile bu projeyi hayata geçirdiğimiz ve QRadar ürün kurulumunu gerçekleştirdiğimiz için son derece mutluyuz.”*

Platin Bilişim uzmanlığı ile LC Waikiki için kurulumu gerçekleştirilen IBM QRadar, uygunsuz şekilde kullanılan uygulamaların, şirket içi sahteciliğin ve milyonlarca olayın arasında kaybolmuş olabilecek gelişmiş ve düşük düzeyli ve yavaş gelişen tehditlerin algılanmasına yardımcı olur. Güvenlik aygıtları, işletim sistemleri, uygulamalar, veritabanları ve kimlik ve erişim yönetimi ürünleri de dahil olmak üzere birçok farklı kaynaktan günlükleri ve olayları toplar. Anahtarlardan ve yönlendiricilerden Katman 7 (uygulama katmanı) verileri de dahil olmak üzere ağ akışı verilerini toplar. Kimlik ve erişim yönetimi ürünlerinden ve Dynamic Host Configuration Protocol (DHCP) gibi altyapı hizmetlerinden bilgi edinir ve ağ ve uygulama güvenlik açığı tarayıcılarından güvenlik açığı bilgilerini alır. Uyarıları azaltır ve önceliklendirir, tehdit algılama, uyumluluk raporlaması ve denetim için anında olay normalleştirme gerçekleştirir ve olayları diğer veriler ile ilişkilendirir.

IBM QRadar sayesinde milyarlarca olayı ve akışı, üzerinde işlem yapılabilecek bir avuç dolusu saldırı bilgisine dönüştürür ve işler üzerindeki etkilerine göre bunları önceliklendirir. Uygulamalar, anasistemler, kullanıcılar ve ağ alanları ile ilişkili davranışlardaki değişikliklerin tanımlanması için temel etkinlik çizgileri oluşturma ve olağandışı durum algılama işlemlerini gerçekleştirir.

- LC Waikiki, 5651 No'lu yasa kapsamında kanuni olarak değiştirilemez şekilde log kaydı alınmasını ve zaman damgası ile damgalanmasını sağlamış oldu.
- LC Waikiki bünyesinde tüm operasyonel cihazlarının loglarının toplanarak gizililiği, bütünlüğü ve erişilebilirliği sağlandı.
- Uygulama ve Yönetim kolaylaşmış oldu.
- Daha az bakım ihtiyacı ve yönetimsel ihtiyaç oluştu. Daha geniş iş hacmi için hizmet emniyeti daha güvenilir bir hale geldi.