ManageEngine
EventLog Analyzer

AB Genel Veri Koruma Düzenlemesine uymak için tüm bilmeniz ve yapmanız gerekenler

İçindekiler

Giriş 2

Zorluklar, gereksinimler ve eylem planları

GDPR sınırsızdır 3

Genişletilmiş kişisel veri kapsamı 4

Yeniden tanımlanan veri koruma ilkeleri 5

Sorumluluk ve mali yükümlülük 7

Veri ihlali bildirimi 9

Veri sahiplerinin hakları 10

Uyumluluk ihlali cezaları 11

EventLog Analyzer hakkında 12

EventLog Analyzer ve kuruluşları GDPR'ye uygun hale getirmedeki rolü 13

Giriş

Veri ihlallerinin sayısındaki, ölçeğindeki ve maliyetindeki artışlar, dünya genelinde hükümetlerin vatandaşların kişisel verilerini korumak için katı uyumluluk yasalarını yürürlüğe koymasına neden oldu. Avrupa'da istisna yoktur. Avrupa Komisyonu, 2012 yılından itibaren, veri işleme yöntemlerini geliştirebilen, veri güvenliğini iyileştirebilen ve aynı zamanda, gizli verileri tüm Avrupa ülkelerinde koruma konusunda uyum getirebilen yeni veri korumaları hazırlamaktadır.

Yeni Genel Veri Koruma Düzenlemesi (GDPR), mevcut veri koruma kurallarında yapılan birçok değişiklikle birlikte daha fazla ilgi çekmektedir. AB GDPR yapısının, yeni sorumluluk ilkeleri, ihlal bildirim prosedürleri ve uluslararası veri akışları için katı kurallarla birlikte uygulaması karmaşıktır. Bu yeni düzenlemeye uyum sağlamak için sadece birkaç ay kalmakla birlikte, kuruluşların güvenlik stratejilerini yeniden değerlendirme zamanı gelmiştir.

Bu kılavuz, GDPR'ye uygunluğu sağlamak için kuruluşların yapması gereken kilit değişikliklere, zorluklara ve eylem planlarına dikkat çekmektedir.

Değişiklikler, gereksinimler ve eylem planları

GDPR sınırsızdır

GDPR, yalnızca AB'de faaliyet gösteren şirketlerin ötesine geçen küresel bir veri koruma yasasıdır. AB'deki tüketicileri hedef alan, AB vatandaşlarının kişisel verilerini işleyen veya AB veri sahiplerinin davranışını izleyen herhangi bir kuruluş, GDPR gereksinimlerine uymak zorundadır.

Gereksinimler:

- Şimdi şirketlerin güvenlik yapılarını ve ilkelerini yeniden değerlendirme zamanı. AB içinde faaliyet göstermeyen ancak AB verileriyle ilgilenen kuruluşların, yeni GDPR'ye uyum sağlamak için adımlar atması gerekecektir.
- AB'de faaliyet gösteren ve mevcut AB veri koruma yasasına uyum sağlayan kuruluşlar da, yeni GDPR'nin katı gereksinimlerini karşılamasını sağlamak için güvenlik yapılarını yeniden değerlendirmelidir.

Eylem planları

- Kuruluşunuz mal veya hizmet tedarik ediyorsa veya AB vatandaşlarının davranışını izliyorsa, 25 Mayıs 2018 tarihinden veya bu tarihten önce GDPR gereksinimlerine uyum sağlamalıdır.
- Güvenlik ilkelerinizi yeniden değerlendirin ve kişisel verileri kullanırken aşağıda özetlendiği gibi uygun adımları attığınızdan emin olun.
- Kişisel verilerini işlemek amacıyla bireylerin açık ve kesin onayını almak için kullanılabilen uygun gizlilik notlarını ve diğer belgeleri tasarlayın. Söz konusu belgeleriniz zaten varsa, bunları yeni düzenlemeye uygun olarak revize edip gözden geçirmeyi düşünün.
- Toplanan kişisel verilerin gizliliğini ve güvenliğini sağlamak için alınan teknik ve kurumsal önlemleri izleyin.
  Gerekirse, veri işlemlerini izleyebilen ve kişisel ve gizli verilerin güvenliğinden sorumlu olan görevliler atayın.

Genişletilmiş kişisel veri kapsamı

Yeni düzenleme, kişisel ve gizli verilerin tanımını genişletiyor.

GDPR'ye göre, kişisel veriler "tanımlanmış ve tanımlanabilir bir gerçek kişi ile ilgili herhangi bir bilgi"dir. Aynı zamanda, IP adresleri ve çerez tanımlayıcıları gibi "çevrimiçi tanımlayıcılar" da içerir.

GDPR, kişisel verilerin tanımlanmasının dışında, kişisel verilerin bir kısmını gizli kişisel veriler olarak sınıflandırır. GDPR'ye göre gizli kişisel veriler, "ırksal veya etnik kökene, politik görüşlere, dini veya felsefi inançlara, sendika üyeliğine, sağlık veya cinsel yaşam ve genetik ve biyometrik verilere ilişkin herhangi bir veri"dir.

Yeni gereksinimler, kuruluşların kişisel verilerini işleme koymadan önce "veri sahipleri"nden geçerli onay almasını da uygulamaya koymaktadır.

Zorluklar:

- Kişisel verilerin bu geniş tanımı ve "çevrimiçi tanımlayıcı"nın dahil edilmesi, veri analizi, davranış analizi, reklamcılık ve sosyal medyayla ilgilenen kuruluşları GDPR'ye uymaya zorlamaktadır.

Eylem planları

- Kuruluşunuzun ilgilendiği verilerin kapsamını tanımlayın.
- Veriler GDPR'nin "kişisel veriler" tanımına giriyorsa, daha fazla veri işleme için bireylerin açık ve kesin onayını talep eden bir gizlilik notu veya belge hazırlayın.
- Verileri işleme koymak için zaten onay istiyorsanız, bunları yeni uyumluluk gereksinimlerine uygun olarak revize edip gözden geçirmeyi düşünün.

Yeniden tanımlanan veri koruma ilkeleri

GDPR gereksinimlerinin temelini oluşturan veri koruma ilkesi, önceki uyumluluk düzenlemesi olan Veri Koruma Yasasında belirtildiği gibi aynı kalır ve sepetine bir kaç unsur daha eklenir.

Altı veri koruma ilkesi, kişisel veriler ve gizli kişisel veriler hususunda şunları özetlemektedir;

- Adil, yasal ve şeffaf bir şekilde işlenmesi gerektiğini.
- belirlenmiş, açık ve meşru amaçlar için toplanması ve yukarıda belirtilen amaçlara aykırı şekilde işlenmemesi gerektiğini. Verilerin kamu yararına veya bilimsel, tarihsel ya da istatistiksel amaçlar için ileride arşivlenmesinin önceki amaçlarla bağdaşmadığı düşünülmemelidir.
- İşlendiği amaca ilişkin olarak gerekli olana uygun, bununla ilgili ve sınırlı olması gerektiğini.
- Doğru ve güncel olması gerektiğini. Doğru olmayan kişisel verileri silmek veya düzeltmek için adımlar atılmalıdır.
- İşlendiği amaçlar için gerekli olandan daha uzun süre veri sahiplerinin kimlik saptamasına izin veren bir biçimde korunması gerektiğini. Arşiv, kamu yararını veya bilimsel, tarihsel ya da istatistiksel amaçları destekliyorsa, daha uzun süre arşivlenebilir. Ayrıca, kuruluşlar bireylerin hak ve özgürlüklerini korumak amacıyla teknik önlemler almalıdır.
- Yasa dışı işlem, rastlantısal kayıp, bozulma veya hasara karşı koruma da dahil, uygun güvenlik sağlayan doğru teknik ve kuruluş önlemleri ile işlenir.

Yeni GDPR, veri denetleyicilerinin a) veri koruma ilkelerinin yürürlükte olmasından sorumlu tutan ve b) kuruluşun GDPR'ye uygun olduğunu gösteren katı sorumluluk gereksinimlerini özetlemektedir.

Gereksinimler:

- Veri koruma ilkelerini bu şekilde karşılamak dışında, şirketler açıkça veri işlemedeki rollerini (ör. denetleyiciler veya işlemciler) tanımlamalı ve sorumluluklarını yeni düzenlemeye uygun olarak ele almalıdır.
- Kuruluşlar, GDPR'nin yeni sorumluluk gereksinimlerini karşılamak için veri denetim akışlarını gözden geçirmelidir.

- Şirketler tarafından, yüksek riskli kişisel veriler işliyorlarsa, yeni, riske dayalı bir yaklaşım benimsenmelidir. Veri denetleyicileri, kişisel verilerin işlenmeden önce bile ilişkili olan riski belirlemek için veri koruma etki değerlendirmelerini (DPIA'lar) yerine getirmelidir. DPIA, meydana gelebilecek maliyet zararını azaltmak amacıyla önceki bir aşamada veri ihlallerinin tanımlanmasını ve azaltılmasını sağlar.
- Kişisel verilerle ilgilenen bir proje başlatıldığında, kuruluşlar veri ihlali riskini azaltmak için bir tasarımla gizlilik yaklaşımı benimsemelidir.

Eylem planları

- Veri işleme ile ilgili tüm bilgileri aşağıdakiler dahil olmak üzere belgeleyin:
  - Ne tür kişisel veriler toplanıyor.
  - Nasıl toplanır, kullanılır, iletilir ve depolanır.
  - Her adımda açıklamadan nasıl korunur.
- Şirketler, verilerin nerede saklandığı ve verilere kimin sahip olduğu dahil olmak üzere bilgileri belgelemenin dışında, aşağıdaki gibi faaliyetleri sürekli olarak izlemelidir:
  - Kişisel verilere kim erişir.
  - Veriler kiminle paylaşılır.
- Yetkisiz veya geçersiz erişim denemelerini anında tanımlamak ve bildirmek amacıyla verilerin depolandığı dosyayı veya klasörü sürekli olarak izleyin.
- Verilerin ne kadar süreyle depolanacağına ilişkin bir kayıt tutun. Ve depolanırken, verilerin şifrelenip kurcalamaya dayanıklı olmasını sağlayın.

Sorumluluk ve mali yükümlülük

Kişisel veya gizli veriler işleyen her kuruluş, ya bir denetleyici ya da bir işlemci gibi davranır. GDPR, mali yükümlülüğü sağlamak için, eşit ölçüde uyumlu olmalarından sorumlu tutarak, denetleyicilerin ve işlemcilerin rolleri arasındaki dengeyi bulur.

Veri denetleyicileri

- GDPR'ye göre, "Denetleyiciler, tek başına veya başkalarıyla birlikte çalışarak kişisel verilerin nasıl ve neden işlendiğini belirleyen herhangi bir tüzel kişidir."
- Denetleyiciler şunlardan sorumludur:
  - Tüm veri işleme faaliyetlerini gözden geçirmek.
  - Tüm veri işleme faaliyetlerinin ilgili belgelerini muhafaza etmek.
  - Yüksek riskli işlemler için veri koruma risk değerlendirmeleri yürütmek.
  - Veri korumasını tasarıma göre ve varsayılan değer olarak yerine getirmek.
  - Veri işlemcileri atamak ve verilerin nasıl işleneceğine ilişkin talimatları tanımlamak.
  - Herhangi bir veri ihlali durumunda yetkilileri bilgilendirmek.

Veri işlemcileri

- GDPR'ye göre, bir veri işlemcisi, “veri denetleyicisi adına verileri işleyen herhangi biridir (veri denetleyicisinin çalışanı dışında).”

  Veri işlemcileri şunları yapar:

  - Verileri yalnızca denetleyiciden gelen belgelenmiş talimatlara göre işler.
  - Veri ihlallerini engellemek için güvenlik önlemleri ve kurumsal önlemler alır.
  - İşleme sonunda ve denetleyiciden gelen talimatlara göre tüm kişisel verileri siler.
  - Denetleyiciler adına gerçekleştirilen işleme etkinliklerinin yazılı bir kaydını tutar.
  - Gerekli yerlerde bir Veri Koruma Görevlisi (DPO) atar.
  - Veri ihlali üzerine hemen denetleyicileri bilgilendirir.
  - Uyumluluk göstermek ve denetimlerin denetleyici tarafından yürütülmesini sağlamak için gerekli olan tüm bilgileri denetleyicilere sağlar.

Gereksinimler:

- İşletmeler, değişen sorumluluk gereksinimlerini karşılamak için mevcut veri işleme sözleşmelerini dikkatlice gözden geçirmeli ve değerlendirmelidir. Yeni sözleşmelerin tümü yeni GDPR gereksinimlerine uymalıdır.
- Hem işlemciler hem de denetleyiciler, GDPR'nin yeni gereksinimlerini karşılamak için güvenlik, denetim ve veri ihlal ilkelerini yeniden değerlendirmelidir.
- Kuruluşlar, veri ihlallerini önlemek için alınan önlemlerin kayıtlarını tutmak zorundadır.

Eylem planları

- Kuruluş içindeki veri akışının açık bir kaydını tutun - veriler nasıl toplanıyor, verilere nasıl erişiliyor, veriler nasıl paylaşılıyor ve verilerin sahibi kim.
- Veri ihlallerini engelleyebilecek çerçeve güvenlik ilkeleri. Şunu içerir:
  - Herhangi bir sorunu tespit etmek için kuruluşun ağını izleme.
  - Kullanıcı davranışlarını, özellikle kişisel verileri işleme erişimi olan ayrıcalıklı kullanıcıları takip etme.
  - İçinde kişisel verilerin depolandığı dosyayı ve klasörü denetleme. Kişisel verilere herhangi bir uygunsuz veya yetkisiz erişim denemesi olduğunda anında bilgi alın.
  - Şirket ağını saldırılardan ve tehditlerden korumak için doğru kurumsal ve teknik önlemler alınmasını sağlayın.

Veri ihlali bildirimi

GDPR, bir kişisel veri ihlalini “kişisel verilerin bozulmasına, kaybolmasına, değiştirilmesine, yetkisiz olarak açıklanmasına veya söz konusu kişisel verilere erişilmesine yol açan bir güvenlik ihlali” olarak tanımlar.

Bu, bir veri ihlalinin sadece veri kaybından daha fazlası olduğunu açıklar. Düzenleme, ayrıca kuruluşları 72 saat içinde "fazla gecikmeden ve uygun yerde" veri ihlallerini bildirmeye de zorlar.

Gereksinimler:

- Kuruluşlar, uygun bir iç ihlal raporlama prosedürüne sahip olmalıdır.
- Kuruluşlar, yeni güvenlik gereksinimlerini karşılamalarını sağlamak için tedarik zinciri incelemeleri ve düzenli denetimler yürütmelidir.
- Şirketler, anlık veri ihlali tespitini kolaylaştıran uygun bir teknik ve güvenlik sistemi kullanmalıdır. Sistem, ayrıca yanıtın hızlandırılması için ayrıntılı bilgi sağlamalı veya erken aşamada ihlali kontrol altına almalıdır.

Eylem planları

- Ağda güvenlik ihlallerine neden olan uzlaşma göstergelerini (IOC) tanımlayın ve bunları savunmak için güvenlik ilkeleri hazırlayın.
- Güvenlik saldırılarını önlemeye yardımcı olabilecek güvenlik duvarları ve IDS/IPS gibi güvenlik sistemleri kullanın.
- Güvenlik ihlallerini anında tespit edebilen, uyarı gönderebilen ve rapor edebilen kuruluşlar için güvenlik çözümleri uygulamayı düşünün. Ayrıca, çözümler herhangi bir aksilik veya ihlal denemesi gerçekleştiğinde gerçek zamanlı olarak uyarı göndermelidir.
- Aşağıdaki yetkisiz işlemleri tanımlayarak veri bütünlüğü sağlamaya yardımcı olan güvenlik ilkelerini yürürlüğe koyun:
    - Erişim veya erişim denemeleri
    - Silme
    - Paylaşma
    - Kişisel verileri kopyalama veya kopyalama denemeleri
- Kimlik hırsızlığı durumunda normal olmayan etkinlikleri tanımlamak için ayrıcalıklı kullanıcıların (örneğin: kişisel verilere erişimi olan kullanıcılar) davranışını izleyin ve bunları hemen bildirin.

Veri sahiplerinin hakları

Veri ile gerçekleştirebileceğiniz herhangi bir eylem, veri işleme sayılır. Bununla birlikte, GDPR, kuruluşların yapabildiği ve topladıkları kişisel bilgilerle yapamadıkları eylemler konusunda katı sınırlar tanımlar.

Bilgilendirilme hakkı: Veri toplama noktasından başlar. Kuruluşlar, veri sahiplerine, onlardan toplanan bilgilerin şeffaf ve adil bir şekilde bir gizlilik notu ile işleneceğini bildirmelidir. Ayrıca kuruluşların, basit bir dille düzenlenmiş bir onay belgesi ile, veri sahiplerinden kişisel bilgilerini işlemek için açık ve geçerli onay almaları zorunludur.

Erişim hakkı: Veri sahiplerine veya bireylere, kendi kişisel bilgilerine herhangi bir zamanda erişim hakkı verilmelidir. GDPR, bu gereksinimle bireylerin kendi bilgilerini adil bir şekilde işleme konduğunu kontrol etme ve doğrulama hakkına sahip olmasını sağlar.

Düzeltme hakkı: Bireyler kendi kişisel verilerinin eksik veya yanlış olduğunu düşünürlerse, kuruluştan kişisel verilerinin düzeltilmesini isteme hakkına sahiptir. Bir düzeltme talebinde bulunulduğunda, ilgili bireylere fazla gecikmeden istek üzerinde yapılan işlemler hakkında bilgi sağlamak denetleyicinin sorumluluğundadır.

Veri işlemesini kısıtlama hakkı: Veri işlemesi kısıtlandığında, denetleyici sadece kişisel verileri depolamalıdır, veriler üzerinde herhangi bir işlem yapamaz. Bireyler, aşağıdaki durumlarda veri işlemelerini kısıtlayabilir:

- Verilerin yanlış veya eksik olduğu tespit edildiğinde.
- Veriler yasa dışı olarak işlendiğinde.
- Denetleyicinin, kişisel verileri işlemek için artık herhangi bir nedeni olmadığında (veri koruma ilkelerine uygun olarak).

Veri taşınabilirliği hakkı: Bireyler, herhangi bir zamanda, herhangi bir engel olmadan, kendi verilerini elde edebilir ve işlemesi için başka bir denetleyiciye aktarabilir. Bu hak, bireylerin kişisel verileri güvenli bir şekilde bir ortamdan diğerine kolaylıkla taşımasını, kopyalamasını veya aktarmasını sağlar.

Unutulma hakkı: GDPR, bireylere kendi kişisel verilerinin silinmesini veya kaldırılmasını talep etme hakkı verir. Aşağıdaki şartlar altında veri silme talebinde bulunulabilir:

- Kişisel veri depolamasının ilk başta toplandığı veya işlendiği amaçla ilgili olarak artık gerekli olmadığı yerde.
- Kişi veri işleme onayını geri çektiğinde.
- Veri sahibi, yasa dışı veri işleme nedeniyle veya bir veri ihlali olduğunda veri işlemeyi durdurma talebinde bulunduğunda.
- Bir yasal zorunluluğa uymak amacıyla verilerin silinmesi gerekiyorsa.

Eylem planları

- Kişisel verilerin işlenmesi için bireylerden açık ve kesin onay alabilen uygun bir onay alma formu veya gizlilik notu hazırlayın.
- Erişim haklarını kullanarak aradıklarında bireylere verebilmeniz için veri işleme tekniklerini ve akışlarını belgeleyin.
- Kişisel verileri, amacı yerine getirildikten sonra, otomatik olarak silmek için teknik önlemler alın.
- Veriler depolanırken, verilerin şifrelenmesiyle bütünlüğünün korunmasını sağlayın.
- Gerekirse, veri sahiplerine vermek için şifreleme bilgilerini belgeleyin.

Uyumluluk ihlali cezaları

Kuruluşlar GDPR ile uyumlu olmadığında veya GDPR gereksinimlerini ihlal ettiğinde, yöneticiler, ***10 milyon € veya şirketin önceki mali yılın dünya genelindeki yıllık toplam cirosunun %2'sine kadar,*** hangisi daha fazla ise, cezalandırılabilir. Denetleyiciler ve veri işlemcileri, aşağıdaki koşullar ihlal edildiğinde bu yüksek para cezasına karşı sorumludur:

- Temel veri koruma ilkeleri
- Şahsi olmayan veri işleme koşulları
- Onay koşulları
- Hassas kişisel veri işleme koşulları
- Veri sahiplerinin hakları

Para cezasını uygulamaya koyan veri koruma yetkilisi, ihlalin niteliğini ve yoğunluğunu, alınan azaltma önlemlerini, uygulanan teknik ve kurumsal önlemleri ve ceza miktarını belirlemek için daha fazlasını göz önünde bulundurur.

ManageEngine'in BT güvenlik çözümleriyle GDPR uyumluluk gereksinimlerini karşılama

ManageEngine'in BT güvenlik çözümü portföyünde, kurumların GDPR'ye uyum sağlamalarına yardımcı olan geniş yelpazede araçlar bulunmaktadır. Paketimizde şunlar bulunmaktadır:

- **Log360**, kurumların veri ihlallerini saptamalarına, saklı kişisel verilerin ve kişisel verilere erişim yollarının güvenliğini sağlamalarına ve böylece hesap verebilirlik gereksinimlerine uymalarına yardımcı olan kapsamlı bir SIEM (Güvenlik Bilgisi ve Olay Yönetimi) aracıdır.
- **File Audit Plus**, saklı kişisel verilerin bulunduğu dosya ve klasörlerde yapılan her kritik değişikliğin izlenmesine yardımcı olan, gerçek zamanlı bir dosya denetleme ve izleme aracıdır.

Çözümlerimiz GDPR gereksinimlerini karşılamanıza nasıl yardımcı oluyor?

- **Güvenlik ihlallerini savunmak veya azaltmak için teknik ve kurumsal önlemler:** Log360 ve File Audit Plus'ın kullanılması, kuruluşların güvenlik ihlallerini savunmak veya azaltmak için kullandıkları teknik önlem olabilir. Bu çözümler, ağınızdaki tüm aygıtların ve kullanıcıların etkinliklerini izleme özelliğine sahiptir ve sorunları yöneticilere anında bildirir. Güvenlik uzmanı, daha sonra olayı kapsamlı raporlarıyla araştırır ve eğer olayın bir güvenlik ihlali (veya ihlal denemesi) olduğu tespit edilirse, bunu erken aşamada kontrol altına almak için acil adımlar atabilir.
- **Veri denetimi:** File Audit Plus'ın gerçek zamanlı dosya bütünlüğü izleme özelliği, kritik verilerdeki değişiklikleri sürekli olarak izler. Ayrıca, verilere kimin eriştiği, ne zaman erişildiği ve nereden erişildiği hakkında kapsamlı bilgiler de sağlar. Bu ayrıntılı rapor, veri erişimleri hakkında veri sahiplerine bilgi sağlamaya yardımcı olur ve veri akışlarını da izler.
- **Denetim kaydı yürütme:** Log360'ın güçlü günlük arama özelliği, adli çözümlemeyi kolaylıkla yürütür. Anında düzeltmek için, veri ihlalinin veya ihlal denemesinin temel nedenini ortaya çıkarmak için GDPR'nin gereksinimlerinden biridir. Çözümümüz, birkaç dakika içinde günlük verisi terabaytlarını arayarak bir veri ihlalinin temel nedenini bulmanıza yardımcı olabilir. Çözüm, ayrıca arama sonuçlarını, DPO'lara gönderilebilmesi için, bir adli rapor olarak dışarı aktarmak için bir seçenek de sunar. Ayrıca, arama sorgusu gelecekteki aynı tür güvenlik saldırılarını azaltmak için bir uyarı profili haline dönüştürülebilir.

- **PIA/DPIA gereksinimini karşılama:** Log360'ın kapsamlı raporları ve uyarı profilleri, herhangi bir ağ sorununu ve güvenlik ihlali denemesini anında tespit eder. Bu, veri ihlalinin erken bir aşamada kontrol altına alınmasına ve veri hasarını ve maruz kalınan maliyeti de en aza indirmeye, böylece GDPR'nin PIA/DPIA gereksinimini karşılamaya yardımcı olur.

- **İhlal bildirimi gereksinimi:** Log360, yöneticilere veri ihlalleri hakkında gerçek zamanlı e-posta veya SMS uyarıları gönderir. Bu, fazla gecikmeden, üst düzey yetkililere ihlali rapor etmelerine yardımcı olur. Bu çözüm, önceden belirlenmiş 600'den fazla uyarı profili ile birlikte gelir çeşitli IOC'lere dayanır. Bu, ihlal denemelerinin anında çok fazla çaba sarf etmeden tespit edilmesine yardımcı olur. Çözüm, ayrıca iç güvenlik gereksinimlerini karşılamak amacıyla özel uyarı profilleri oluşturmak için bir seçenek de sunar.

ManageEngine Hakkında

ManageEngine, bir IT ekibinin gerçek zamanlı hizmetler ve destek için bir kuruluşun ihtiyacını karşılamasına izin veren gerçek zamanlı IT yönetim araçlarını sunar. Dünya genelinde, 60.000'in üzerinde yerleşik ve yeni kuruluş - Fortune 500'ün yüzde 60'ından fazlası dahil - ağlar, sunucular, uygulamalar, masaüstü bilgisayarlar ve daha fazlası dahil, kritik IT altyapılarında en iyi performansı sağlamak için ManageEngine ürünlerine güveniyor. ManageEngine, Amerika Birleşik Devletleri, Birleşik Krallık, Hindistan, Japonya ve Çin de dahil olmak üzere dünya genelinde ofislere sahip, Zoho Corp.'un bir bölümüdür.

Geliştirici hakkında

Subhalakshmi Ganapathy, şu anda ManageEngine'de IT Güvenlik Çözümleri için Üst Düzey Ürün Pazarlama Analisti olarak çalışmaktadır. Bilgi güvenliği ve uyumluluk yönetimi konusunda engin bilgiye sahiptir. Güvenlik Bilgileri ve Olay Yönetimi (SIEM), ağ güvenliği ve veri gizliliği konusunda kuruluşlara stratejik rehberlik sağlamaktadır.

Subha'ya şu adresten ulaşın: subhalakshmi.g@manageengine.com.

E-posta:
support@eventloganalyzer.com

Veya

Ücretsiz Arayın:

ABD: +1 888 720 9500 İngiltere: 0800 028 6590

AVUS: +1 800 631 268 CN : +86 400 660 8680

Uluslararası: +1 925 924 9500

Veya

Çözüm ve özellikleri hakkında ayrıntılı bilgi için www.eventloganalyzer.com adresini ziyaret edin.