**BİLGİ GÜVENLİĞİ MERKEZİ LOG YÖNETİM SİSTEMİ**

1. **Amaç**
   1. Bu Teknik Şartnamenin amacı, BİLGİ bilişim sisteminde bulunan donanımlar ile kullanılan yazılımların tarafından üretilen logların ya da idare tarafından belirlenen verilerin merkezi olarak tek bir noktada toplanması ve bu loglar ve veriler üzerinde analiz yapılabilmesi ve İDARE tarafından belirlenen korelasyon kurallarına uygun alarm üretilmesi amacıyla gerekli olan donanım ve yazılımların alınmasıdır.
2. **Tanımlar ve Kısaltmalar**
   1. İDARE/BİLGİ: İSTANBUL BİLGİ ÜNİVERSİTESİ Bilişim Teknolojileri Dairesi Başkanlığı.
   2. YÜKLENİCİ/FİİRMA: Üzerine ihale yapılan ve sözleşme imzalanan kuruluş.
   3. HİZMET: Bu Teknik Şartname kapsamında Yüklenicinin gerçekleştireceği bütün faaliyetlerdir.
   4. KURULUM: Bu teknik şartname kapsamında olan donanım ve yazılımların yine bu teknik şartname kapsamında belirtilen şekilde, proje planında belirtilen sürelerde BİLGİ Sistem Merkezinde çalışır duruma getirilmesi.
   5. VERİ: BİLGİ Bilgi Sistemi içerisindeki tüm bilgi varlıkları.
   6. EPS (Event Per Second): Saniyede üretilen olay sayısı
   7. BAĞLANTI SAĞLAYICI (COLLECTOR): Her bir log ve veri kaynağında üretilen log ve verileri toplamak için kullanılan donanımsal ya da yazılımsal araç.
   8. EKLENTİ (PLUGIN): Sistemler tarafından üretilen loğların merkezi sisteme tanıtılması ve entegre edilmesini sağlayan yazılım parçası.
   9. DASHBOARD ( PANEL ): Özet veriler, raporlar ve analizlerden oluşmuş gelişmiş görüntüleme arabirimi.
   10. KORELASYON: Farklı veri kaynaklarından İdarenin belirlediği kurallara uygun olarak verilerin derlenmesi ve raporlandırılmasıdır.
   11. GERÇEK ZAMANLI LOG VEYA VERİ: BİLGİ Bilişim Sisteminde çekilebilir hale gelen kaydın Log Yönetimi yazılımı tarafından maksimum 30 dakika gecikme ile Merkezi Log Yönetimi yazılımına aktarılacak olan log ya da veridir.
   12. LOG: BİLGİ Bilgi sistemi içerisinde bulunan donanım ve yazılımların üzerinde yapılan işlemlere ait detay ve zaman bilgisi içeren kayıtlardır.
3. **Merkezi Log Sistemi Kurulumu**
   1. Yüklenici, bu T.Ş. kapsamındaki Merkezi Log Yönetimi Sistemi kurulumu ile gerekli yazılım ve gerekli görülmesi halinde donanımların temininden sorumlu olacaktır.
   2. Sistem, İdaremizde bulunan Firewall/UTM, Anti virüs Sistemi, IPS/IDP/IDS ( atak tanıma ve engelleme sistemleri) , içerik filtreleme sistemleri, Veri tabanı sistemleri, Kablosuz Erişim Cihazları, Windows Sunucu işletim sistemi ve Windows / Linux Uygulama Sunucu ( Exchange, DHCP, IIS, Apache ) gibi LOG ve bilgi üreten sistemlerinden sınırsız LOG kaynağından LOG toplayacak şekilde lisanslanmalıdır.
   3. Yüklenici Merkezi Log Yönetimi Sistemini oluşturan tüm yazılım lisanslarının tedarikinden sorumlu olacaktır, İdareden ayrıca bu lisanslar için ücret talep edilmeyecektir. Sağlanacak olan lisans saniyede maksimum 25.000 EPS değerini veya günlük 200 GB büyüklüğünde log/veriyi karşılayacak şekilde olacaktır. Lisansların tamamı İdare adına kayıt edilecektir. Lisanslar ile alakalı web sayfası hesapları İdarenin belirleyeceği kişiler adına oluşturulacaktır.
   4. Merkezi Log Yönetimi sistemi ve ek bileşenlerinin 1 yıl sürüm güncelleme lisansı olacaktır.
   5. Kurulumlarda zorunlu haller dışında root ve ya admin kullanıcı hesapları ile kurulum yapılmayacaktır. Bu tür kurulum yapılması gerektiği durumlarda önceden İdareden onay alınacaktır. Kurulumların hiçbirisi varsayılan (default) kullanıcı adı ve şifresi ile yapılmayacaktır. Kullanıcı adları ve şifreler tutanak ile İdareye teslim edilecektir.
4. **Merkezi Log Yönetimi Yazılımı Özellikleri**
   1. **Genel Özellikler**
      1. Merkezi Log Yönetimi Yazılımına ait işlemler tek bir yönetim ekranı üzerinden yapılmalı ve toplanan tüm loglar bu yönetim ekranı aracılığıyla yönetilebilmelidir.
      2. Merkezi Log yönetimi yazılımı raporlama, alarm, korelasyon ve analiz yeteneklerine sahip olacaktır.
      3. Yönetim ekranına web tarayıcı üzerinden erişilebilecektir. Raporlama, alarm, korelasyon, panel, arşiv yönetimi özelliklerinin tümü bu web yönetim birimi ile kullanılabilmelidir. Yüklenici hangi internet tarayıcıları ile erişimi desteklediğini belirtecektir.
      4. Sistemin tüm menüleri ve menü içindeki önemli fonksiyonlar kullanıcı bazlı yetkilendirilebilecektir. Böylelikle kullanıcılar sadece kendilerine özel menüleri görebilecek ve sistem üzerinde kendilerine verilen kadar yetkiye sahip olacaklardır.
      5. Tüm raporlar kullanıcı group yada profillleri bazlı yetkilendirilebilecektir. Raporlama kullanıcıları sadece kendilerie ait raporları görebilecektir. Bu raporlar içindeki silme ve düzeltme gibi ana işlevler yetkilendirilebilecektir.
      6. Yüklenici sistemin bütünleşik çalışacağı HDFS dağıtık dosya sistemini kurum tarafından belirtilen sanal yada gerçek donanımlar üstüne en az 5 makine olacak şekilde kurmalıdır.
      7. Log Yönetim Sistemi kurulan dağıtık dosya sistemine tam entegre çalışmalı, verilerini bu sistem üstünde tutmalı, rapor alarm ve korelasyon gibi işlevleri bu sistem üstünde tutulan veri ile yapabilmelidir.
      8. Kurulan dağıtık dosya sistemi bir kopyadan fazla veri yedeği tutacak şekilde konfigüre edilmelidir.
      9. Çözüm, güvenlik sınıflandırması güncellemeleri, sağlayıcı firmanın kural güncellemeleri, aygıt desteği, vb gibi konfigürasyon bilgilerinin minimum kullanıcı müdahalesiyle otomatik olarak güncellenmesini desteklemelidir.
      10. Merkezi Log Yönetimi Yazılımı yönetim ekranı üzerinde farklı yetkilendirmeler yapılabilmelidir. Kullanıcılar yapılan yetkilendirme dâhilinde kendileri ile alakalı kayıtlara erişebilmeli, gerçek zamanlı ve geriye dönük sorgulama yapabilmelidir.
      11. Sistem güvenlik cihazlarından gelen verileri inceleyecek IP, URL, MAIL alanlarını kontrol ederek botnet , smtp black list, ip reputation gibi mesajlar üreterek ikinci bir güvenlik katmanı olarak çalışacaktır. Bu özelliği desteklemeyen üreticiler kendi ürünleri ile tam entegre çalışan üçüncü parti bir ürün teklif etmek zorundadır.
      12. Yetkilendirme işlemi sadece yöneticiler tarafından yapılabilmelidir..
      13. Yetkilendirme işlemi kişi ya da grup bazlı yapılabilmelidir.
      14. IP aralığı, Sunucu türüne göre yetkilendirme yapılabilmelidir.
      15. Merkezi Log Yönetimi Yazılımı LDAP entegrasyonu olmalıdır. Raporlama kullanıcıları Active Directory, Kimlik Yönetimi Sistemi ya da BİLGİ bünyesinde kullanılan LDAP ile entegrasyonu ile sisteme giriş yapabilmelidir.
      16. Merkezi Log Yönetimi Yazılımı yönetim ekranı üzerinde tüm sisteme ait veriler tek bir dashboard içerisinde ya da aynı ekran üzerinde farklı sekmeler altında görüntülenebilecektir.
      17. Merkezi Log Yönetimi Yazılımı yönetim ekranı üzerinde kullanıcılar kendilerine ait dashboard oluşturabilecek ve bu dashboarda Merkezi Log Yönetimi Sistemi içerisinde gelen seçenekler kapsamında değişiklik yapabilmelidir. Yapılan değişiklikler kaydedilebilecektir.
      18. Merkezi Log Yönetimi Yazılımı içerisinde yapılan önemli iş/işlemlere ve değişikliklere ilişkin kayıtlar tutulmalı ve bu iş/işlemlere ait sorgulama ve raporlama yapılabilmelidir.
      19. Toplanan loglar zaman damgası ile damgalanacaktır. Zaman damgası 5070 sayılı Elektronik İmza kanununda belirtilen niteliklere uygun olacaktır. Bu özelliği ürün desteklemiyor ise Yüklenicinin ürün ile entegre edeceği ek bir yazılım ile zaman damgalaması yapılabilecektir.
      20. Toplanan loglar zaman damgası ile damgalanacaktır. Sistem Telekomünikasyon kurumu tarafından otorite kabul edilmiş kurumların zaman damgası sistemine entegre edilerek teslim edilecektir. Sistem ile birlikte 3 yıl içerisinde kullanılacak en az 15000 adet zaman damgası birlikte verilecektir
      21. Merkezi Log Yönetimi Yazılımı aynı anda birden fazla farklı networkten veri toplayabilmeli ve tek merkezde birleştirebilmelidir.
      22. Merkezi Log Yönetimi Yazılımı yönetim ekranı üzerinde tüm alarmlar görülebilecektir.
      23. Merkezi Log Yönetimi Yazılımı yönetim ekranı üzerinden Log Yönetimi Sistemine ait bileşenler monitör edilebilecektir. Bu monitörde Merkezi Log Yönetimi Sistemini oluşturan bileşenlere ait CPU, memory, Disk I/O, Disk Kapasite gibi bileşenler izlenebilecektir.
      24. Merkezi Log Yönetimi Sistemi monitör ekranı üzerinde alarmlar tanımlanabilecek ve tanımlanan alarmlar meydana geldiğinde İdarece bildirilecek kişilere e-posta atabilecektir.
   2. **LOG ve Verilerin toplanması**
      1. Merkezi Log Yönetimi Yazılımı syslog, ssh, wmi, ossec protolleri ile veri toplamayı desteklemelidir.
      2. Merkezi Log Yönetimi Yazılımı dosya paylaşımı ve eklenen disk üzerinden veri/log toplama özelliklerini desteklemelidir.
      3. Merkezi Log Yönetimi Yazılımı SQL ve ORACLE veri tabanlarındaki tablolardan doğrudan veri toplamayabilecektir.
      4. Merkezi Log Yönetimi Yazılımı SQL ve ORACLE veri tabanlarının Windows işletim sistemi log mimarisine ve text ortamlara yazdığı verileri toplayabilecektir.
      5. Yüklenici Log/veri toplanacak her bir kaynaktan ne şekilde Log/veri toplayacağını detaylı bir şekilde İdareye tutanak ile bildirecektir.
      6. Merkezi Log Yönetimi Yazılımı yönetim ekranı üzerinden log/veri toplayan tüm sunucular görülebilecektir. Merkezi Log Yönetimi Yazılımı yönetim ekranı üzerinde IP aralığı, sunucu türü, veri grubu ve log kaynağına göre listeleme ve gruplama yapılabilmelidir.
      7. Merkezi log yönetim sistemine entegre edilmiş ürünlere ait raporlanması istenen yeni alanlar var ise Yüklenici bu işlemi garanti süresince yapacağını taahhüt etmelidir.
      8. Log/veri toplama işlemi ajanlı veya ajansız olarak yapılabilecektir.
      9. Log/veri toplama işlemi yapılırken üretilen logun/verinin merkezi log toplama yazılımına kopyasının gönderilmesi sağlanacak, log/veri toplanan donanım ya da yazılımın logu/verisi kendi üzerinde tutması engellenmeyecektir. Log/verinin alındığı kaynak sistemde bu loglar/veriler silinse veya değiştirilse bile toplanan loglar/veriler bundan etkilenmemelidir.
      10. Log/veri toplama işlemi yapılırken üretilen logun/verinin Merkezi Log Yönetimi Sistemi log/veri alma ve log/veri oluşma zamanı verileri ayrı ayrı kayıt altına alınmalıdır. Sorgulama ve raporlama işlemleri log/veri oluşma zamanına göre yapılabilmelidir.
      11. Merkezi Log Yönetimi Sistemi log/veri toplama işlemi için uzak noktalarda bulunan Log/veri kaynaklarından Log/veri toplanması durumunda ağ üzerinde çok büyük bant genişliğini kullanmaması için bir seferde kaç adet satır okuyacağı veya bant genişliği ayarı veya zamanlama ayarı yapılabilecektir.
      12. Merkezi Log Yönetimi Yazılımı standardında olmayan, desteklemediği bir veri kaynağından (log/veri formatı bilinen) log/veri toplayabilecektir. Toplanan log/verinin anlamlı hale getirilmesi için gerekli olan işlemler ( plugin yazılması vs. ) Yüklenici tarafından kabul çalışması başlamadan ücretsiz olarak yapılacaktır.
      13. BİLGİ Bilişim Sistemi veri tabanlarından log/veri çekilmesi durumlarında tablolarda bulunan İdare tarafından istenilen kayıtlar çekilecektir. İlgili tablo bölünmüş ise ya da belirli bir tarihten öncesi farklı bir tabloya atılmış ise bu tablolarda çekilecektir.
      14. Toplanan loglar /veriler grafiksel olarak görüntülenebilmelidir. Toplanan loglar/veriler ile alakalı kullanıcı kendisine özel grafik tasarımı yapabilmelidir ya da bu amaçla kullanılan yazılım geliştirme kiti ücretsiz olarak sağlanmalıdır.
      15. Merkezi Log Yönetimi Sistemi üzerinde sıkıştırma özelliği olmalıdır. Sıkıştırma oranı en az 1/10 olmalıdır. Toplanan log/veriler işlendikten sonra sıkıştırılarak Log Yönetimi Sistemi üzerinde tutulabilmelidir. Kullanıcı sıkıştırılmış log/veri üzerinde işlem yapması gerektiği durumlarda, kullanıcıya operasyonel bir yük getirmeden otomatik olarak ilgili kaydın getirilmesi sağlanacaktır. Sıkıştırma işlemi; varlık etiketi (asset tagging) verilmiş olan sunucu ismine göre, ip bilgisine göre veya tarih bazlı yapılabilecektir.
      16. Kayıt altına alınan loglar/veriler istendiği durumlarda farklı disk alanlarında saklanabilmeli ve bu farklı disk alanlarından Merkezi Log Yönetimi yazılımı içerisinden otomatik olarak çağrılabilmeli ve tüm işlemler yapılabilmelidir.
      17. Merkezi Log Yönetimi Yazılımı internet ile ilgili log kayıtlarında ülke / lokasyon bilgilerini IP tabanlı olarak gösterebilen ve bu bilgiyi sürekli olarak güncelleyen bir “Geo Location” sistemine üye olacak ve bu bilgiyi raporlarında gösterebilecektir.
      18. Merkezi Log Yönetimi Yazılımı internet tehditlerine ve riskli IP bloklarına karşı, sürekli olarak güncellenen ve global olarak kullanımı yaygın olan bir “IP Reputation” sistemine üye olacak ve buradan sağlanıp sürekli güncellenen bilgileri korelasyonlarında kullanabilir olacaktır. IP Reputation sistemine üyelik için gerekli olan tüm masraflar yüklenici tarafından ücretsiz olarak sağlanacaktır.
      19. Merkezi log yönetimi yazılımı log toplama sırasında filtreleme, aynı verileri birleştirme, sınıflandırma özelliklerine sahip olacaktır.
   3. **Korelasyon ve Alarm**
      1. Toplanan loglar/veriler üzerinde korelasyon yapılabilmelidir. Belirli bir zaman için farklı log/veri kaynaklarında alınan kayıtlar üzerinde İdarece belirlenen kurallara uygun işlemler gerçekleştiğinde yönetici ekranında görüntüleme ve istenen durumlarda e-posta gönderme işlemi yapılabilecektir.
      2. Merkezi Log Yönetimi Yazılımı hazır korelasyon kurallarının bulunduğu bir kütüphane sunacaktır ve ürün üzerinde özel korelasyon kuralları yazılabilecektir. Yüklenici hazır korelasyon kurallarının listesini son teslim tarihine kadar İdareye bildirecektir. Özel korelasyon yazılması gereken durumlar için Yüklenici ayrıca ücret talep etmeyecektir. Bu tür korelasyonlar son teslim tarihine kadar tamamlanacaktır.
      3. Merkezi Log Yönetimi Yazılımı iki farklı korelasyon sonucuna göre yeni farklı bir alarm oluşturabilecektir.
      4. İlişkilendirilecek loglarda/verilerde her hangi bir sınır ya da limit olmamalıdır. Farklı kaynaklardan gelen loglar/veriler ve/veya yapıları ile (N) adet farklı seviyede ilişkilendirilebilmelidir.
      5. Log/veri toplanan herhangi bir kaynağa ait bir olay gerçekleştikten sonra belirli bir süre içerisinde aynı Log/veri toplanan herhangi bir kaynağa ait farklı olaydan bir ya da belirli sayıda olay gerçekleşirse ve daha sonra aynı olay kaynağına ait bir ya da belirli sayıda farklı olay gerçekleşirse bu yapı ve/veya bağlaçları ile istenildiği kadar tanımlama yapılabilmelidir. (Örn: Sunucuya 5 dakikada 7 başarısız erişim girişimi olduktan sonra aynı IP den başarılı erişim olmuş ise)
      6. “Log/veri toplanan herhangi bir kaynağa ait bir olay gerçekleştikten sonra belirli bir süre içerisinde diğer bir Log/veri toplanan başka bir kaynağa ait, bir ya da birden çok olay gerçekleşirse” şeklinde yinelenen olay sayısı kadar tanımlama yapılabilmelidir. (Bu yapı ve/veya bağlaçları ile istenildiği kadar devam edebilir.) (Örn: Güvenlik Duvarından gelen loglar/veriler ile IDS, Web ve Database sunucu log/verilerin ilişkilendirilmesi gibi.)
      7. Merkezi Log Yönetimi Sistemi trend analizi yapabilmelidir. İstenen olay tiplerinin tanımlanan süre aralıklarında oluşma değerleri hesaplanabilmeli, ilgili değerlerin tanımlanan bir süre için ortalamalarını alarak bu değerler üzerinden, tanımlanabilen bir sapma değeri oluştuğunda özel bir alarm üretebilmelidir. İlgili hesaplamalar yapılırken tanımlanabilen belirli günlerin hesaplamalar dışında tutulması sağlanabilmelidir. Yüklenici bu işlem için ayrı bir yazılım ya da donanım kullanabilir. Bu yazılım ya da donanım log yönetimi yazılımı ile uyumlu olmak zorundadır.
      8. Sistemde kolay alarm hazırlamak için bir alarm hazırlama sihirbazı bulunacaktır.
      9. Log/verilerin içeriklerine bağlı olarak alarm tanımı yapılabilecektir.
      10. Log/verilerin içerisindeki birden fazla bilginin içeriğine bağlı olarak alarm tanımlanabilecektir.
      11. Alarm kuralı oluşumunda “içeriyorsa, içermiyorsa, büyüktür, küçüktür, başlıyorsa, bitiyorsa” gibi ifadelere bağlı olarak kurallar tanımlanabilmelidir.
      12. Birden fazla log/veri kaynağına bağlı ortak log/veriye dayalı alarm tanımı yapılabilmeli, bunlar arasında SQL cümlesi ile belirtilen koşullara bağlı ilişkiler kurulabilmelidir.
      13. Belirli log/verilerin sık şekilde tekrarlanmasından kaynaklı alarmlar oluşturulabilmelidir. Sisteme ulaşan bir logun/verinin doğrudan alarm üretmemesi ancak aynı içerikli logun/verinin belirli bir zaman diliminde belirlenen bir sayıda sisteme ulaşması durumunda kullanıcının tanımlayacağı şekilde bir alarm üretilebilmelidir. (Örn:5 dakikada 300 adet olay olursa.)
      14. Alarmlar önem derecesine göre seviyelendirilebilmelidir.
      15. Hangi alarm tanımının hangi seviyede olacağı kullanıcı tarafından ayarlanabilmelidir.
      16. Tüm alarmlar, alarma kaynaklık eden log/verinin oluşma zamanını göstermelidir.
      17. Tanımlanan alarmlar daha önce belirlenen kişilere mail veya SMS ile uyarı mesajı olarak gönderebilmelidir.
      18. Log/veri toplanan yazılım ya da donanıma erişimin kaybolması bir alarm olarak tanımlanabilmelidir. Erişilemeyen yazılım ya da donanıma dair sistemde alarm oluşmalıdır.
      19. Alarm üretilen her durum geçmişe yönelik olarak detaylı bir şekilde sorgulanabilmeli ve raporlanabilmelidir.
      20. Belirtilen bir alarm grubuna dair alarm geçmişi listelenebilmelidir. Alarm verileri için raporlar alınabilmelidir.
      21. Bir sisteme ait belirli bir olay gerçekleşirse alarm üretilebilmelidir. (Örn: Router ve switch logların silinmesi gibi.)
      22. Alarmı oluşturan ham log/veri bilgisi alarm ile birlikte görülebilmelidir.
      23. Hangi kuraldan dolayı alarm oluştuğu bilgisi yönetici ekranda görülmelidir.
   4. **Sorgulama Kriterleri**
      1. Loglar/veriler üzerinde kullanıcı kendi istediği parametrelere uygun olarak sorgu yapabilmelidir. Yapılan sorgular daha sonra kullanılmak üzere kayıt altına alınabilmelidir.
      2. Güncel (30 günden daha yeni olan log/veriler) ve 30 günden daha eski log/verilere dair kayıtlar tarih, saat ya da içerik olarak gerçek zamanlı ya da geriye dönük olarak sorgulanabilmelidir.
      3. Güncel veri üstünde ( En az son 1 Milyar veri ) 20 adet eş zamanlı sorgu çalıştırabilmeli ve sorgu yanıt süresi 10 dakikanın altında kalmalıdır.
      4. Merkezi Log Yönetimi Yazılımı içerisinde toplanan tüm log/veri, tiplerine göre filtreleme yapılabilmelidir.
      5. Merkezi Log Yönetimi Yazılımı içerisinde tanımı yapılan tüm log/veri formatlarına ait tüm kolonlar için arama kriteri eklenebilmelidir.
   5. **Raporlama**
      1. Log/verilerden belirlenen formatlarda (pdf, xls, html) rapor alınabilmeli ve bu rapora dair kurallar tekrar kullanım için saklanabilmelidir.
      2. Log/veri aramasında tarih aralığı veya belirli bir süreyi ifade edecek şekilde raporlama yapılabilmelidir.
      3. Sistemde kolay rapor hazırlama için bir rapor hazırlama sihirbazı bulunacaktır.
      4. Tanımlanan rapor gruplarına göre filtreleme yapılabilmeli, rapor içerisinde belirlenen rapor grubundan gelen logların/verilerin yönetici ekranından görüntülenmesi sağlanabilmelidir. İstenirse ilgili rapor bilgisayara aktarılabilmelidir.
      5. Raporda hangi içeriğin görüntüleneceği belirlenebilmelidir. Kolon ekleme ve kaldırma işlemi yapılabilmelidir.
      6. Sisteme tanımı yapılmış log/veri formatları içerisinde herhangi bir kolon rapora kolon olarak eklenebilmelidir.
      7. Raporda kullanılacak sıralama kriterleri bir veya daha fazla alana göre belirlenebilmelidir.
      8. Sistem, güncel veri üzerinde matematiksel ve istatistiksel hesaplar yapabilmelidir. Değer gruplamaları, sayısal verilerin toplamları, değerlerin zamansal dağılımları, benzersiz değerlerinin sayısı gibi hesaplamaları yapabilmelidir. Bu hesaplamalar istenildiği anda güncel veri üzerinde tüm loglar ve logların tüm kolonları için yapılabilmelidir. Örn: Bir Ip Adresinin kullandığı bant genişliği, yaptığı bağlantı sayısı,kullandığı farklı port ve eriştiği farklı IP sayısının hesaplanması
      9. Raporların gönderim zamanı günlük, haftalık ya da aylık olarak ayarlanabilmelidir. Raporların çalışma saatleri kullanıcı tarafından ayarlanabilmelidir.
      10. İstenilen rapor ve grafik ekranlar birleştirilerek özel izleme ekranı tasarımları yapılabilmeli ve bunlar daha sonra kullanmak üzere kaydedilebilmelidir.
      11. İdare tarafından özel rapor istenmesi durumunda istenilen rapora ait özellikler Yükleniciye tutanak karşılığında verilecektir. Bu raporlar muayene kabul işleminin sonuna kadar İdareye gösterilecektir.
   6. **Logların Merkezi Olarak Görüntülenmesi**
      1. Merkezi Log Görüntüleme sistemi her bir kenar noktaya tek tek erişerek raporları merkezi olarak görüntüleyebilecektir. Bu işlemi yaparken merkeze veri kopyalaması yapılmayacaktır.
      2. Merkezi Log Görüntüleme Sistemi her bir kenar noktaya tek tek erişerek aldığı verileri dashboardlar üzerinde görüntüleyebilecektir. Bu işlemi yaparken merkeze veri kopyalaması yapılmayacaktır.
      3. Merkezi Log Görüntüleme Sistemi kenar noktalarda oluşan alarmları merkezi olarak tek tek görüntüleyebilecektir. Bu işlemi yaparken merkeze veri kopyalaması yapılmayacaktır.
   7. **Eğitim**
      1. İdare tarafından belirlenecek 3 kişiye Merkezi Log Yönetimi Sistemini oluşturan her bir bileşen (Sunucu işletim sistemi, kullanılan veri tabanı, varsa web sunucusu vb.) için temel seviye eğitim verilecektir. Ayrıca Merkezi Log Yönetimi Yazılımına ait sunucu ve yazılım kurulumlarını içerir temel seviye ve ileri seviye kullanıcı eğitimleri verilecektir. Eğitim alacak personel ile birlikte İdare tarafından belirlenen yönetici sıfatını haiz görevliler de bu eğitimlere nezaret edebilecektir.
      2. Eğitimin süresi en az 3 iş günü olacaktır. Eğitim zamanı ve yeri idarenin onayı alınarak belirlenecektir. Eğitimler son kabul öncesi bitecek şekilde planlanacaktır.
      3. Eğitime ilişkin tüm giderler Yüklenici tarafından karşılanacaktır.
      4. Eğitim verecek kişi Merkezi Log Yönetimi Sistemi üretici firmanın elemanı olacak ve Merkezi Log Yönetimi Yazılımı ile alakalı en az 3 yıl tecrübeye sahip olacaktır. Üretici firmanın elamanı olmaması durumunda Merkezi Log Yönetimi Sistemi konusunda sertifika sahibi eleman olacaktır.
      5. Eğitim dokümanları Türkçe olacaktır. Kullanım kılavuzları Türkçe olarak hazırlanacaktır.
      6. Yüklenici tarafından her katılımcı için ayrı ayrı eğitim dokümanı sağlanacaktır.
5. **Gizlilik ve Güvenlik**
   1. Gizlilik gerektiren bilgi, materyal ve dokümanlar istenen şartlar doğrultusunda korunacak, İdare yazılı olarak izin vermedikçe üçüncü firma/şahıslara aktarılmayacaktır.
   2. Yüklenici, bilgi ve dokümanların görsel, işitsel ve yayın yolu ile üçüncü şahıslara karşı güvenliğini sağlamaktan sorumlu olacaktır.
   3. Bu projedeki hiçbir teknik doküman kısmen veya tamamen Yüklenici tarafından başka projelerde kullanılmayacaktır.
   4. Yüklenici personeli veya yetkilileri İdare adresinde yapacakları her türlü çalışma sırasında İdare’nin koymuş olduğu kurallara mutlak surette uyacak ve gizlilik kurallarını ihlal etmeyecektir.
   5. Yüklenici işe başlamadan önce idare tarafından hazırlanan gizlilik sözleşmesini imzalayacaktır.
6. **Teslim Muayene ve Kabul**
   1. Yüklenici bu teknik şartname konusu ürünlerin kurulumunu yaparak, sorunsuz ve çalışır vaziyette idareye teslim edecektir
   2. İdare işe başlama sözleşmesinin imzalanması esnasında log/veri toplanacak olan sunucu ve uygulamalara ait listeyi tutanak karşılığında yükleniciye teslim edecektir.
   3. Yüklenici tarafından kurulum ve muayene ve kabul işlemlerine ilişkin iş planı işe başlamadan önce İDARE ile paylaşılacak ve iş planı içerisinde belirtilen aralıklarda İDAREYE rapor verilecektir.
   4. Yüklenici bu şartname kapsamında talep edilen her maddenin nasıl karşılandığını detaylı şekilde açıkladığı belgeyi kabul öncesinde elektronik ortamda idareye teslim edecektir. Bu doküman ürünü yönetecek personelin görevlerini ve iş tanımlarını da içerecektir.
   5. Muayene ve kabul, teknik şartnamenin uygulamalı olarak gösterilebilecek tüm maddelerinin uygulamasının muayene ve kabul komisyonuna gösterilmesi suretiyle yapılacaktır. Bu maddelerin uygulaması, hazırlanması ve gösterilmesi yüklenici tarafından sağlanacaktır. Uygulamalı olarak gösterilemeyecek maddeler ise yüklenici tarafından belgelendirilecektir. Ayrıca ihale dokümanında belirtilen ve muayene kabule kadar yerine getirilmesi gereken yükümlülüklerin yerine getirilip getirilmediğine bakılacaktır.
7. **Garanti ve Bakım Şartları**
   1. Verilen tüm garantiler belgelendirilecek ve bu belgeler teslim ile birlikte idareye sunulacaktır.
   2. Yüklenici, T.Ş kapsamında alınacak tüm yazılımlara yerinde destek olacak şekilde en az 1 (iki) yıl garanti verecektir. Tedarik edilen ürünün standart garantisi bu sürenin üzerinde olması halinde üretici firma garanti süresi uygulanacaktır.
   3. Yüklenici garanti süresince BİLGİ Bilişim Sistemi içerisinde yeni bir log/veri kaynağı eklenmesi durumunda ilgili log/veri kaynağından log/veri toplayabilecek ve bu T.Ş. kapsamında istenen diğer sorgulama, raporlama ve korelasyon işlemleri yapılabilecektir. Yüklenici Merkezi Log Yönetimi Yazılımında gerekli güncellemeyi en geç 180 takvim günü içerisinde temin edecektir.
   4. Ürüne ait hazır plugin olmaması durumunda yeni bir plugin hazırlama aşamaları çıkarılarak İDAREYE CD/DVD ortamında tutanak karşılığında teslim edilecektir.
   5. Yüklenici garanti süresince yeni korelasyon yazılması gereken ek durumlar için ücretsiz destek hizmeti verecektir. Garanti süresi zarfında BİLGİ Bilişim Sisteminde kullanılmaya başlayacak olan yeni bir ürün için korelasyon yazılması gerektiği durumlarda Yüklenici bu işlemi en fazla 30 takvim günü içerisinde tamamlayacaktır. Süre sonrasında arıza kayıt işlemleri için geçerli olan cezai şartlar uygulanacaktır.
   6. Bu teknik şartname kapsamında tedarik edilen tüm donanım ve yazılımların garanti başlangıcı kesin kabul tarihi olacaktır. Garanti süresince, garanti kapsamındaki her türlü bakım ve onarım hizmetleri işçilik dâhil olmak üzere, yerinde ve ücretsiz yapılacaktır.
   7. Garanti süresince Merkezi Log Yönetimi sistemi ve bu sistemin parçası olan donanım ve yazılımlarda meydana gelecek arızalar iletişim araçlarından (telefon, faks, e-posta, vb.) birisi kullanılarak Yüklenici’ye bildirilecektir. Yüklenici arıza bildirim anından itibaren en geç 24 saat içinde arızaya müdahale edecektir.