T.C.
KAYSERİ ÜNİVERSİTESİ REKTÖRLÜĞÜ
Bilgi İşlem Daire Başkanlığı

Sayı : **68056880** 16/10/2020
Konu : Teklif Verilmesi

Sayın .....

Üniversitemiz Bilgi İşlem Daire Başkanlığı bünyesinde kullanılmak üzere aşağıda adı geçen malzemelerin Teknik şartnameye uygun olarak alımına ihtiyaç duyulmaktadır.

4734 Sayılı Kamu İhale Kanununun *22/d* maddesine göre (doğrudan temin) satın alınacak olan, hizmet alım işinin, tarafınızdan temini mümkün ise ***26 Ekim 2020, saat 14.00*** tarihine kadar İdari ve Mali İşler Daire Başkanlığı Satın Alma Bürosuna teklif verilmesi konusunda gereğini rica ederim.

Öğr. Gör. Ayhan RENKLİER
Bilgi İşlem Daire Başkan V.

S. No	Malzemenin Adı	Bakım Sayısı	Birim Fiyat (TL)	Toplam Tutar (TL)
1	Log ve SIEM Yazılımı (Teknik Şartnameye Uygun)	1 Adet		

TOPLAM	
KDV %	
GENEL TOPLAM	

Mevlana Mahallesi 15 Temmuz Yerleşkesi Kümeevler No:5 38280 Talas / Kayseri
Telefon: (0 352) 432 3230 Faks: (0 352) 437 52 80
e-posta: imid@kayseri.edu.tr

KAYSERİ ÜNİVERSİTESİ
Bilgi İşlem Daire Başkanlığı
Log ve SIEM Yazılım Teknik Şartnamesi

1. KONU

Bu teknik şartname, kurumumuzun ihtiyacı için satın alınacak olan Güvenlik Bilgisi ve Olay Yönetim Sisteminin (SIEM) teknik özelliklerini, denetim ve muayene metotlarını ve ilgili diğer hususları konu alır.

2. İSTEK VE ÖZELLİKLER:

2.1. TANIMLAR:

2.1.1. **FİRMA**: İdari şartnamedeki şartlara sahip, teklif verebilen kuruluşlardır.

2.1.2. **DONANIM**: Bir bilgisayar sisteminin gözle görülüp elle tutulabilen her türlü; elektronik, elektromekanik, mekanik ve bunlara benzer birimlerinin her biri veya tamamıdır.

2.1.3. **YAZILIM**: Bir bilgi sisteminin işleyişi ile ilgili bilgisayar programlarının, yordamların kuralların ve gerektiğinde belgelemenin tümüdür.

2.1.4. **MALZEME**: Güvenlik Bilgisi ve Olay Yönetim Sistemine (SIEM) ilişkin tüm donanım ve yazılımlardır.

2.1.5. **DOKÜMAN**: Satın alınacak malzemelerin kurulumunda karşılaşılan sorunlar, çözümler, açıklayıcı ve bilgilendirici bilgileri içeren, yazılımların kurulması, kullanımı, bakım ve onarımı, yapılandırılması ve sorunların giderilmesi konularında kullanılmak üzere üretici ve/veya yetkili temsilci tarafından yayınlanmış her türlü teknik yayın, not, resim, şekil, plan, kitap, CD/DVD ve benzerleridir.

2.1.6. **İŞGÜNÜ**: Resmi tatil günlerine rastlamamak kaydıyla pazartesi, salı, çarşamba, perşembe ve cuma günlerinin her birinde 09.00-18.00 saatleri arasındaki süredir.

2.1.7. **KAYIT (LOG)** : Her türlü bilgisayar, sunucu (etki alanı, dosya, yazıcı, web, uygulama, veritabanı, sistem yönetim sunucuları gibi KAYSERİ ÜNİVERSİTESİ ağında hizmet veren sunucu sistemler), ağ cihazı (anahtarlama cihazı, yönlendirici vb.), yazıcı, disk ünitesi, yedekleme ünitesi, ağ güvenlik sistemleri (ağ güvenlik duvarı (firewall), saldırı tespit/önleme sistemleri (IDS/IPS), Veri Kaybı Önleme Sistemi (DLP), Ağ Erişim Kontrol Sistemi (NAC), antivirüs yazılımı vb.), IP kamera, geçiş kontrol sistemleri vb. elektronik donanıma sahip, üzerinde herhangi bir işletim sistemi ve/veya yazılım çalışan, belirli zamanlarda ve belirli bir formatta bilgi ortaya koyan tüm cihazların (ağ cihazları için ağ üzerindeki veri akış bilgileri (flow data) dahil) ortaya koyduğu sayısal veridir.

2.2. KISALTMALAR:

API : Application Programming Interface,
CSV : Comma Separated Values,
CyBOX : Cyber Observable Expression,
DMZ : De-Militarized Zone,
DOC/DOCX : Dosya Uzantısı (Microsoft Word File),
DLP : Data Loss Prevention,
EPS : Events per Second,
FTP : File Transfer Protocol,

GB	: Giga Byte,
HA	: High Availability,
HIPAA	: Health Insurance Portability and Accountability Act,
HTML	: Hypertext Markup Language,
IDS	: Intrusion Detection System,
IPS	: Intrusion Prevention System,
IP	: Internet Protocol,
ISO 27001	: International Standardization Organization Std.27001,
JDBC	: Java Database Connectivity,
JSON	: JavaScript Object Notation,
LDAP	: Lightweight Directory Access Protocol,
LEA	: Log Export API,
MAC	: Media Access Control,
MD5	: Message Digest 5,
MIME	: Multipurpose Internet Mail Extensions,
MHT	: MIME HTML,
NTP	: Network Time Protocol,
OPSEC	: Open Platform for Security,
PCI DSS	: Payment Card Industry Data Security Standards,
PDF	: Portable Document Format,
RAID	: Redundant Array of Independent Disks,
RBAC	: Role Based Access Control,
Regex	: Regular Expression,
SCCM	: System Center Configuration Manager,
SCP	: Secure Copy,
SDEE	: Security Device Event Exchange,
SHA	: Secure Hashing Algorithm,
SIEM	: Security Information and Event Management,
SNMP	: Simple Network Management Protocol,
SOC	: Security Operations Center,
SFTP	: SSH File Transfer Protocol,
SOX	: Sarbanes-Oxley Act,
SQL	: Structured Query Language,
SSH	: Secure Shell,
SSL	: Secure Sockets Layer,
STIX	: Structured Threat Information Expression,
TAXII	: Trusted Automated Exchange of Indicator Information,
TCP	: Transmission Control Protocol,
TLS	: Transport Layer Security,
UBA	: User Behavior Analysis,
UEBA	: User and Entity Behavior Analytics,
VOIP	: Voice over IP,

VB : Visual Basic,
WAN : Wide Area Network (Geniş Alan Ağı),
WMI : Windows Management Instrumentation,
XLS/XLSX : Dosya Uzantısı (Microsoft Excel Spreadsheet File).

2.3. TEKNİK ÖZELLİKLER :

2.3.1. GENEL HUSUSLAR :

Güvenlik Bilgisi ve Olay Yönetim Sistemi (SIEM); KAYSERİ ÜNİVERSİTESİ ağında yer alan sistemlere ve kayıt kaynaklarına ilişkin olarak, en az aşağıda belirtilen ve özellikleri bu şartname kapsamında detaylı olarak açıklanan işlemleri yapmak üzere gerekli donanım, sanal makine, yazılım ve/veya yazılım bileşenlerini (üzerinde çalıştığı işletim sistemleri dahil) kapsayacak ve en az ilişkilendirme bileşeni dışındaki tüm bileşenleri için yüksek erişilebilirlik (high availability) sağlayacak şekilde kurularak hazır ve çalışır şekilde teslim edilecektir:

2.3.1.1. Genel Özellikler

2.3.1.1.1. Önerilecek sistem yazılım lisansı sınırsız sayıda sistemde üreyen en az 25.000 EPS değerindeki kapasiteye destek verecek özelliklerde olmalıdır.
2.3.1.1.2. Merkezi Log Yönetim sistemi günlük en az 200 GB Log/Veri toplayacak şekilde teklif edilmelidir.
2.3.1.1.3. Merkezi Log Yönetimi Yazılımına ait işlemler tek bir yönetim ekranı üzerinden yapılmalı ve toplanan tüm loglar bu yönetim ekranı aracılığıyla yönetilmelidir.
2.3.1.1.4. Merkezi Log yönetimi yazılımı raporlama, alarm, korelasyon, threat intelligence ve analiz yeteneklerine sahip olmalıdır.
2.3.1.1.5. Merkezi log yönetimi yazılımı genel bilişim endüstriyel standartlarında (ISO 27001, PCI vs) standart rapor üretebilecek kabiliyette olmalıdır.
2.3.1.1.6. Yönetim ekranına web tarayıcı üzerinden erişilebilecektir. Raporlama, alarm, korelasyon, panel, arşiv yönetimi özelliklerinin tümü bu web yönetim birimi ile kullanılabilmelidir.
2.3.1.1.7. Sistemin tüm menüleri ve menü içindeki önemli fonksiyonlar kullanıcı bazlı yetkilendirilebilecektir. Böylelikle kullanıcılar sadece kendilerine özel menüleri görebilecek ve sistem üzerinde kendilerine verilen düzeyde yetkiye sahip olacaklardır. Kullanıcılar yapılan yetkilendirme dâhilinde kendileri ile alakalı kayıtlara ulaşabilme, gerçek zamanlı ve geriye dönük sorgulama yapabilmelidir.
2.3.1.1.8. Önerilen sistem üzerinde yetkilendirilecek yönetici, çözümün çeşitli işlevsel alanlarına rol-tabanlı erişimi tanımlayabilmelidir.
2.3.1.1.9. Çözüm, bir kimlik doğrulama yöntemi olarak 3. Taraf dizin sistemleriyle bütünleşmeyi sağlamalıdır. Merkezi Log Yönetimi sistemine erişim yetkilendirmesi için bir LDAP veya Active Directory çözümüyle bütünleşmeyi sağlamalıdır.
2.3.1.1.10. Çözümde log kaynağı ekleme sınırı olmamalıdır. Gerektiğinde yeni log kaynakları sınır olmadan eklenebilmelidir.

2.3.1.1.11. Çözüm, gelecekteki genişletmeler ve diğer 3. Taraf çözümleriyle entegrasyon ve IOT Cihazları için uygun bir çerçeve sağlamalıdır.

2.3.1.1.12. Çözüm, güvenlik sınıflandırması güncellemeleri, sağlayıcı firmanın kural güncellemeleri, aygıt desteği, vb gibi konfigürasyon bilgilerini otomatik olarak güncellemeyi desteklemelidir. Bu güncelleme yetkili kullanıcı müdahalesi ile kontrollü bir şekilde yapılabilmelidir.

2.3.1.1.13. Yetkilendirme işlemi sadece yetkili yöneticiler tarafından yapılabilmelidir. Yetkilendirme IP aralığı, sunucu türüne göre yada veri kaynağı tipine göre yapılabilmelidir.

2.3.1.1.14. Merkezi Log Yönetimi Yazılımı yönetim ekranı üzerinde tüm sisteme ait veriler tek bir dashboard içerisinde ya da aynı ekran üzerinde farklı sekmeler altında görüntülenebilecektir.

2.3.1.1.15. Sistemde tanımlı kullanıcılar için ayrı ayrı rapor, alarm ve dashboard yetkilendirmeleri yapılabilmelidir.

2.3.1.1.16. Merkezi Log Yönetimi Yazılımı içerisinde yapılan önemli iş/işlemlere ve değişikliklere ilişkin kayıtlar tutulmalı ve bu iş/işlemlere ait sorgulama ve raporlama yapılabilmelidir.

2.3.1.1.17. Toplanan loglar zaman damgası ile damgalanacaktır. Sistem Telekomünikasyon kurumu tarafından otorite kabul edilmiş kurumların zaman damgası sistemine entegre edilerek teslim edilecektir. Zaman damgası 5070 sayılı Elektronik İmza kanununda belirtilen niteliklere uygun olacaktır. Bu özelliği ürün desteklemiyor ise YÜKLENİCİ'nin ürün ile entegre edeceği tüm maliyeti YÜKLENİCİ'ye ait ek bir yazılım ile zaman damgalaması yapılabilecektir ve sözleşme süresi boyunca ihtiyaç olacak zaman damgasını temin edeceğini taahhüt edecektir.

2.3.1.1.18. Merkezi Log Yönetimi Yazılımı sistemi yatay veya dikey olarak genişlemeye uygun olacaktır.

2.3.1.1.19. Merkezi Log Yönetimi Yazılımı yönetim ekranı üzerinde tüm alarmlar görülebilecektir.

2.3.1.1.20. 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.

2.3.1.1.21. Merkezi Log Yönetimi Sistemi oluşacak alarmlar ve bilgilendirme mesajlarını ilgili kişi veya gruplara e-posta/SMS yolu ile iletilebilmelidir.

2.3.1.1.22. Merkezi Log Yönetimi Yazılımı otomatize güvenlik sağlamalıdır. Anomaliler, tehditler vb durumlarda Firewall cihazlarına otomatik aksiyon aldırma özelliğini desteklemelidir. FİRMA hangi marka Firewalllar ile çalıştıklarını belirtmelidir.

2.3.1.1.23. Merkezi Log Yönetimi sistemi toplanan veriler, analiz, korelasyon, collector ve yönetim birimlerinin tümü yedekli mimaride olacaktır.

2.3.1.2. Log ve Verilerin Toplanması

2.3.1.2.1. Merkezi Log Yönetimi Yazılımı aynı anda birden fazla farklı network segmentinden veri toplayabilmeli ve tek merkezde birleştirebilmelidir.

2.3.1.2.2. Merkezi Log Yönetimi Yazılımı syslog, ssh, opsec-lea, sftp, wmi, protokolleri ile veri toplamayı desteklemelidir.

2.3.1.2.3. Merkezi Log Yönetimi Yazılımı CIFS/NFS protokollerini kullanarak veri/log toplama özelliklerini desteklemelidir.

2.3.1.2.4. Merkezi Log Yönetimi Yazılımı Microsoft SQL ve ORACLE veri tabanlarındaki tablolardan doğrudan veri toplayabilecektir.

2.3.1.2.5. Merkezi Log Yönetimi Yazılımı Microsoft SQL ve ORACLE veri tabanlarının Windows ve Linux işletim sistemi log mimarisine ve text ortamlara yazdığı verileri toplayabilecektir.

2.3.1.2.6. YÜKLENİCİ Log/veri toplanacak her bir kaynaktan ne şekilde Log/veri toplayacağını karşılıklı istişare ederek FİRMA ile kararlaştıracaktır.

2.3.1.2.7. 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.

2.3.1.2.8. Merkezi log yönetim sistemine entegre edilmiş ürünlere ait raporlanması istenen yeni alanlar var ise YÜKLENİCİ bu işlemi garanti süresince yapacağını taahhüt etmelidir.

2.3.1.2.9. Log/veri toplama işlemi ajanlı veya ajansız olarak yapılabilecektir.

2.3.1.2.10. 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.

2.3.1.2.11. 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.

2.3.1.2.12. 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.) YÜKLENİCİ tarafından kabul çalışması başlamadan ücretsiz olarak yapılacaktır.

2.3.1.2.13. Merkezi Log Yönetim Sistemi veri tabanlarından log/veri çekilmesi durumlarında tablolarda bulunan ve KAYSERİ ÜNİVERSİTESİ tarafından istenilen kayıtlar çekilecektir. İlgili tablo bölünmüş ise ya da belirli bir tarihten öncesi farklı bir tabloya atılmış ise bu tablolar da çekilecektir.

2.3.1.2.14. Toplanan loglar/veriler grafiksel olarak görüntülenebilmelidir. Toplanan loglar/veriler ile alakalı kullanıcı kendisine özel grafik tasarımı yapabilmelidir ya da bu amaçla kullanılan yazılım geliştirme dokümanı ücretsiz olarak sağlanmalıdır.

2.3.1.2.15. Merkezi Log Yönetimi Sistemi üzerinde sıkıştırma özelliği olmalıdır. Toplanan log/veriler işlendikten sonra sıkıştırılarak Log Yönetimi Sistemi üzerinde tutabilmelidir. 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.

2.3.1.2.16. 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.

2.3.1.2.17. 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.

2.3.1.2.18. Merkezi log yönetimi yazılımı log toplama sırasında filtreleme, aynı verileri birleştirme, sınıflandırma özelliklerine sahip olacaktır.

2.3.1.3. Kayıt Arama/Sorgulama (Log Search/Query)

2.3.1.3.1. Loglar/veriler üzerinde kullanıcı kendi istediği parametrelere uygun olarak sorgu yapabilmelidir. Yapılan sorgular daha sonra kullanılmak üzere kayıt altına alınabilmelidir.

2.3.1.3.2. Güncel ve 730 günden daha eski log/verilere dair kayıtlar tarih, saat ya da içerik olarak gerçek zamanlı ya da geriye dönük olarak sorgulanabilmelidir.

2.3.1.3.3. Güncel veri üstünde 20 adet eş zamanlı sorgu çalıştırabilmeli ve sorgu yanıt süresi 10 dakikanın altında kalmalıdır.

2.3.1.3.4. Merkezi Log Yönetimi Yazılımı içerisinde toplanan tüm log/veri, tiplerine göre filtreleme yapılabilmelidir.

2.3.1.3.5. Merkezi Log Yönetimi Yazılımı içerisinde tanımı yapılan tüm log/veri formatlarına ait tüm kolonlar için arama kriteri eklenebilmelidir.

2.3.1.3.6. Merkezi Log Yönetimi Yazılımı, içeriğinde gelen tanımlanmış ve eklenebilir kısayol arama kelimeleri ile dashboard, log activity ve reports ekranlarında hızlı sorgular yapılmasına olanak sağlamalıdır.

2.3.1.4. Korelasyon (Correlation)

2.3.1.4.1. Toplanan loglar/veriler üzerinde korelasyon yapılabilmelidir. Belirli bir zaman için farklı log/veri kaynaklarında alınan kayıtlar üzerinde KAYSERİ ÜNİVERSİTESİ tarafından belirlenen kurallara uygun işlemler gerçekleştiğinde yönetici ekranında görüntüleme ve istenen durumlarda e-posta/SMS gönderme işlemi yapılabilecektir.

2.3.1.4.2. Merkezi Log Yönetimi Yazılımı hazır korelasyon kurallarının bulunduğu bir kütüphane sunacaktır ve ürün üzerinde özel korelasyon kuralları yazılabilecektir. FİRMA hazır korelasyon kurallarının listesini son teslim tarihine kadar KAYSERİ ÜNİVERSİTESİ'ye bildirecektir. Özel korelasyon yazılması gereken durumlar için FİRMA ayrıca ücret talep etmeyecektir

2.3.1.4.3. 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.

2.3.1.4.4. 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: Kritik sunuculara SSH taraması yapan bir IP adresinin kritik sunucudan herhangi birine başarılı erişimi olursa)

2.3.1.4.5. "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.)

2.3.1.5. Anomali Tespiti (Anomaly Detection)

2.3.1.5.1. 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. FİRMA bu işlem için ayrı bir yazılım ya da donanım kullanabilir. Bu yazılım ya da donanım log yönetimi yazılımı ile uyumlu olmak zorundadır.

2.3.1.6. Alarm ve e-posta/SMS Bilgilendirmeleri,

2.3.1.6.1. Merkezi Log Yönetimi Yazılımı en az iki farklı korelasyon sonucuna göre yeni farklı bir alarm oluşturabilecektir.

2.3.1.6.2. Sistemde kolay alarm hazırlamak için bir alarm hazırlama sihirbazı bulunacaktır.

2.3.1.6.3. Log/verilerin içeriklerine bağlı olarak alarm tanımı yapılabilecektir.

2.3.1.6.4. Log/verilerin içerisindeki birden fazla bilginin içeriğine bağlı olarak alarm tanımlanabilecektir.

2.3.1.6.5. Alarm kuralı oluşumunda "içeriyorsa, içermiyorsa, büyüktür, küçüktür, başlıyorsa, bitiyorsa" gibi ifadelere bağlı olarak kurallar tanımlanabilmelidir.

2.3.1.6.6. Birden fazla log/veri kaynağına bağlı ortak log/veriye dayalı alarm tanımı yapılabilmeli, bunlar arasında SQL cümlesi ile belirtilen koşullara bağlı ilişkiler kurulabilmelidir.

2.3.1.6.7. 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.)

2.3.1.6.8. Alarmlar önem derecesine göre seviyelendirilebilmelidir.

2.3.1.6.9. Hangi alarm tanımının hangi seviyede olacağı kullanıcı tarafından ayarlanabilmelidir.

2.3.1.6.10. Tüm alarmlar, alarma kaynaklık eden log/verinin oluşma zamanını göstermelidir.

2.3.1.6.11. Tanımlanan alarmlar daha önce belirlenen kişilere mail veya SMS ile uyarı mesajı olarak gönderebilmelidir.

2.3.1.6.12. Log/veri toplanan yazılım ya da donanıma erişimin kaybolması bir alarm olarak tanımlanabilmelidir. Erişilemeyen yazılım ya da donanıma dair sistemde alarm oluşmalıdır.

2.3.1.6.13. Alarm üretilen her durum geçmişe yönelik olarak detaylı bir şekilde sorgulanabilmeli ve raporlanabilmelidir.

2.3.1.6.14. Belirtilen bir alarm grubuna dair alarm geçmişi listelenebilmelidir. Alarm verileri için raporlar alınabilmelidir.

2.3.1.6.15. Bir sisteme ait belirli bir olay gerçekleşirse alarm üretilebilmelidir.

2.3.1.6.16. Alarmı oluşturan ham log/veri bilgisi alarm ile birlikte görülebilmelidir.

2.3.1.6.17. Hangi kuraldan dolayı alarm oluştuğu bilgisi yönetici ekranda görülmelidir.

2.3.1.7. Raporlama (Reporting)

2.3.1.7.1. Log/verilerden belirlenen formatlarda (pdf, xls, html) rapor alınabilmeli ve bu rapora dair kurallar tekrar kullanım için saklanabilmelidir.
2.3.1.7.2. Log/veri aramasında tarih aralığı veya belirli bir süreyi ifade edecek şekilde raporlama yapılabilmelidir.
2.3.1.7.3. Sistemde kolay rapor hazırlama için bir rapor hazırlama sihirbazı bulunacaktır.
2.3.1.7.4. Tanımlanan rapor gruplarına göre filtreleme yapılabilmeli, rapor içerisinde belirlenen rapor grubundan gelen logların/verilerin yönetici ekranından görüntülenmesi sağlanabilmelidir. İstenirse ilgili rapor bilgisayara aktarılabilmelidir.
2.3.1.7.5. Raporda hangi içeriğin görüntüleneceği belirlenebilmelidir. Kolon ekleme ve kaldırma işlemi yapılabilmelidir.
2.3.1.7.6. Sisteme tanımı yapılmış log/veri formatları içerisinde herhangi bir kolon rapora kolon olarak eklenebilmelidir.
2.3.1.7.7. Raporda kullanılacak sıralama kriterleri bir veya daha fazla alana göre belirlenebilmelidir.
2.3.1.7.8. 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
2.3.1.7.9. Raporların gönderim zamanı günlük, haftalık ya da aylık olarak ayarlanabilmelidir. Raporların çalışma saatleri kullanıcı tarafından ayarlanabilmelidir.
2.3.1.7.10. İstenilen rapor ve grafik ekranlar birleştirilerek özel izleme ekranı tasarımları yapılabilmeli ve bunlar daha sonra kullanmak üzere kaydedilebilmelidir.
2.3.1.7.11. KAYSERİ ÜNİVERSİTESİ tarafından özel rapor istenmesi durumunda istenilen rapora ait özellikler FİRMA'a tutanak karşılığında verilecektir. Bu raporlar muayene kabul işleminin sonuna kadar KAYSERİ ÜNİVERSİTESİ'ye gösterilecektir.
2.3.1.7.12. Tüm raporlar kullanıcı, grup ya da profil bazlı yetkilendirilebilecektir. Raporlama kullanıcıları sadece kendilerine ait raporları görebilecektir. Bu raporlar içindeki silme ve düzeltme gibi ana işlevler yetkilendirilebilecektir.

2.3.1.8. Yedeklilik (Cluster)

2.3.1.8.1. HDFS mimarisi ile Aktif-Aktif data yedekliliği sağlanabilmelidir.
2.3.1.8.2. Merkezi Log Yönetimi Sistemi üzerinde çalışan tüm servislerin Aktif-Aktif ve yedekli bir şekilde çalışması sağlanabilmelidir.
2.3.1.8.3. Merkezi Log Yönetimi Sistemi, yedekli mimaride bulunan sunuculardan herhangi birinin kapanması veya kesintiye uğraması durumunda veri kaybı olmamalıdır.
2.3.1.8.4. Yedekli çalışan Merkezi Log Yönetimi Sisteminin kesintiye uğramış olan herhangi bir bileşeni tekrar aktif hale geldiğinde otomatik olarak yedekli mimariye dahil olabilmelidir.

3. EĞİTİM

3.1. KAYSERİ ÜNİVERSİTESİ tarafından belirlenecek 3 kişiye Merkezi Log Yönetimi Sistemini oluşturan her bir bileşen (Sunucu işletim sistemi, kullanılan veri tabanı, varsa web sunucusu vb.) için temel ve ileri 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 KAYSERİ ÜNİVERSİTESİ tarafından belirlenen yönetici sıfatını haiz görevliler de bu eğitimlere nezaret edebilecektir.

3.2. Eğitimin süresi en az 1 iş günü olacaktır. Eğitim zamanı ve yeri KAYSERİ ÜNİVERSİTESİ'nin onayı alınarak belirlenecektir. Eğitimler son kabul öncesi tamamlanacak şekilde planlanacaktır.

3.3. Eğitime ilişkin tüm giderler FİRMA tarafından karşılanacaktır.

3.4. Eğitim verecek kişi Merkezi Log Yönetimi Sistemi üretici firmanın personeli olacak ve Merkezi Log Yönetimi Yazılımı ile alakalı en az 3 yıl tecrübeye sahip olacaktır. Üretici firmanın bu konuda uzman personeli olmaması durumunda eğitimler Merkezi Log Yönetimi Sistemi konusunda sertifika sahibi eğitimci tarafından verilecektir.

3.5. Eğitim dokümanları Türkçe olacaktır. Kullanım kılavuzları Türkçe olarak hazırlanacaktır.

3.6. FİRMA tarafından her katılımcı için ayrı ayrı eğitim dokümanı sağlanacaktır.

4. GİZLİLİK ve GÜVENLİK

4.1. Gizlilik gerektiren bilgi, materyal ve dokümanlar istenen şartlar doğrultusunda korunacak, KAYSERİ ÜNİVERSİTESİ yazılı olarak izin vermedikçe üçüncü firma/şahıslara aktarılmayacaktır.

4.2. FİRMA, bilgi ve dokümanların görsel, işitsel ve yayın yolu ile üçüncü şahıslara karşı güvenliğini sağlamaktan sorumlu olacaktır.

4.3. Bu projedeki hiçbir teknik doküman kısmen veya tamamen FİRMA tarafından başka projelerde kullanılmayacaktır.

4.4. FİRMA personeli veya yetkilileri KAYSERİ ÜNİVERSİTESİ adresinde yapacakları her türlü çalışma sırasında KAYSERİ ÜNİVERSİTESİ'nin koymuş olduğu kurallara mutlak surette uyacak ve gizlilik kurallarını ihlal etmeyecektir.

4.5. FİRMA işe başlamadan önce KAYSERİ ÜNİVERSİTESİ tarafından hazırlanan gizlilik sözleşmesini imzalayacaktır.

5. TESLİM MUAYENE ve KABUL

5.1. FİRMA bu teknik şartname konusu ürünlerin kurulumunu yaparak, sorunsuz ve çalışır vaziyette KAYSERİ ÜNİVERSİTESİ'ye teslim edecektir

5.2. KAYSERİ ÜNİVERSİTESİ işe başlama sözleşmesinin imzalanması esnasında log/veri toplanacak olan sunucu ve uygulamalara ait listeyi tutanak karşılığında FİRMA'a teslim edecektir.

5.3. FİRMA tarafından kurulum ve muayene ve kabul işlemlerine ilişkin iş planı işe başlamadan önce KAYSERİ ÜNİVERSİTESİ ile paylaşılacak ve iş planı içerisinde belirtilen aralıklarda KAYSERİ ÜNİVERSİTESİ'ye rapor verilecektir.

5.4. FİRMA bu şartname kapsamında talep edilen her maddenin nasıl karşılandığını detaylı şekilde açıkladığı belgeyi kabul öncesinde elektronik ortamda KAYSERİ ÜNİVERSİTESİ'ye teslim edecektir. Bu doküman ürünü yönetecek personelin görevlerini ve iş tanımlarını da içerecektir.

5.5. Muayene ve kabul, teknik şartnamenin uygulamalı olarak gösterilebilecek tüm maddelerinin uygulamasının muayene ve kabul komisyonuna gösterilmesi suretiyle yapılacaktır. Bu maddelerin uygulaması, hazırlanması ve gösterilmesi FİRMA tarafından sağlanacaktır. Uygulamalı olarak gösterilemeyecek maddeler ise FİRMA tarafından belgelendirilecektir. Ayrıca ihale dokümanında belirtilen ve muayene kabule kadar yerine getirilmesi gereken yükümlülüklerin yerine getirilip getirilmediğine bakılacaktır.

6. GARANTİ ve BAKIM ŞARTLARI

6.1. Verilen tüm garantiler belgelendirilecek ve bu belgeler teslim ile birlikte KAYSERİ ÜNİVERSİTESİ'ye sunulacaktır.
6.2. FİRMA, T.Ş kapsamında alınacak tüm yazılımlara yerinde destek olacak şekilde en az 3(üç) yıl garanti verecektir. Tedarik edilen ürünün standart garantisi bu sürenin üzerinde olması halinde üretici firma garanti süresi uygulanacaktır.
6.3. FİRMA garanti süresince 2 yıl 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. FİRMA Merkezi Log Yönetimi Yazılımında gerekli güncellemeyi en geç 30 takvim günü içerisinde temin edecektir.
6.4. Ürüne ait hazır plugin olmaması durumunda yeni bir plugin hazırlama aşamaları çıkarılarak KAYSERİ ÜNİVERSİTESİ'ye CD/DVD ortamında tutanak karşılığında teslim edilecektir.
6.5. FİRMA garanti süresince yeni korelasyon yazılması gereken ek durumlar için ücretsiz destek hizmeti verecektir. Garanti süresi zarfında 3 yıl Bilişim Sisteminde kullanılmaya başlayacak olan yeni bir ürün için korelasyon yazılması gerektiği durumlarda FİRMA bu işlemi en fazla 15 takvim günü içerisinde tamamlayacaktır. Süre sonrasında arıza kayıt işlemleri için geçerli olan cezai şartlar uygulanacaktır.
6.6. Bu T.Ş. 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.
6.7. 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 FİRMA'ye bildirilecektir. FİRMA arıza bildirim anından itibaren en geç 24 saat içinde arızaya müdahale edecektir.

Salih Murat GÜRBÜZ
Şube Müdürü

Öğr. Gör. Aytun RENKLİER
Bilgi İşlem Daire Başkanı