08.12.2025

ÜNİTESİ **:** Satın Alma Direktörlüğü

SAYI **:** 2025 / 14032

KONU **:** Bilgi Güvenliği ve Olay Yönetimi (SIEM, Security Information and Event Management) Sistemi Alımı İşi

SON BAŞVURU TARİHİ **:** 19 Aralık 2025 Saat 16:00

Türkiye Futbol Federasyonu tarafından Bilgi Güvenliği ve Olay Yönetimi (SIEM) alımı için ihale düzenlenecektir. İstekliler, tekliflerini **19 Aralık 2025 saat 16:00'a** kadar ***kapalı zarf*** ile Hasan Doğan Milli Takımlar Kamp ve Eğitim Tesisleri Çayağzı Köyü Riva Beykoz/İstanbul adresinde mukim Türkiye Futbol Federasyonu Satın Alma Direktörlüğüne teslim edebilirler.

İstekliler, ihaleye katılabilmek için teklif bedelinin %5'i (yüzdebeş) tutarında geçici teminat verecektir. Geçici teminat en az 25.01.2026 süreli hükümetçe yetkili kılınan veya milli bir banka tarafından düzenlenmiş geçerli teminat mektubu veya aynı tutara karşılık gelecek nakdi tutarın TFF'ye ait TR 68 0006 2000 1860 0006 2980 38 nolu IBAN hesabına yatırılacak ve nakit ödemeyi gösteren banka dekontu ihale dosyasında sunulacaktır. İhale sonucuna müteakip geçici teminat bedelleri ilgili hesaplara iade edilecektir.

Teknik konularla ilgili detaylı bilgi satinalma@tff.org ve bilgiislemihale@tff.org mail adresinden alınabilir.

İstekliler, hazırladıkları teklife esas evraklarını iki ayrı zarfa koyacaklardır. Bu zarflar, dış zarf ve iç zarf diye anılmaktadır. Teklif mektubu ve geçici teminat kapalı ve mühürlü bir iç zarfa konarak, diğer belgeler ile birlikte dış zarf içinde verilecektir

Teklif Sahibi aşağıda belirtilen belgeleri dosyasında teslim edecektir:

DIŞ ZARF
1) Tebligat için kanuni ikametgah belgesi,
2) Ticaret Odası Faaliyet Belgesi,
3) İmza sirküleri
4) Referans dosyası,
5) Vergi Levhası fotokopisi
6) Vergi borcu olmadığına dair belge (teklif verme tarihinden önce 1 ay içinde alınmış olmalı)
7) Sgk borcu olmadığına dair belge (teklif verme tarihinden önce 1 ay içinde alınmış olmalı)
8) Teknik şartnamede belirtilen taahhüt vb belgeler ile kaşe imzalı olarak teknik şartname

İÇ ZARF
1) Geçici teminat mektubu,
2) Teklif Mektubu

Teklifler kapalı ve mühürlü bir iç zarfa konarak, diğer belgeler ile birlikte dış zarf içinde verilecektir. Dış zarf üzerinde sadece "Bilgi Güvenliği ve Olay Yönetimi (SIEM, Security Information and Event Management) Sistemi Alımı" ibaresi yer alacaktır.

Teklif zarflarının tesliminden sonra İstekli teklifinden vazgeçemez veya değiştirilmesini öneremez. TFF, 2886 sayılı Devlet İhale Kanunu ve 4734 sayılı Kamu İhale Kanunu'na tabi olmayıp, 5894 sayılı yasa ile özel hukuka tabi, özerk bir tüzel kişiliktir. Bu bağlamda, işbu ihale süreci tümüyle özel hukuk hükümlerine tabi olup, TFF verilen teklifleri dilediğince değerlendirme ve İSTEKLİLER ile sözleşme yapıp yapmama konusunda tamamıyla serbesttir. TFF, teklifleri kendi belirleyeceği kıstaslar kapsamında değerlendirme ve serbestçe seçim yapma hakkına sahiptir ve ihaleye katılmak isteyenlerin tekliflerini e-ihale sistemine dahil etme hakkı bulunduğunu da saklı tutar.

TFF ihale aşaması, satın almanın katileştiğinin İSTEKLİ'ye tebliğinden sonra veya sözleşme akdedilmesine ilişkin süreç sırasında İSTEKLİ'ye bildirimde bulunmak kaydıyla tek taraflı ve tazminatsız olarak ihaleden veya sözleşme akdinden sarfınazar edebilir.

Ek: Teknik Şartname

Bilgi Güvenliği ve Olay Yönetimi (SIEM, Security Information and Event Management) Sistemi Teknik Şartnamesi

1. Genel

1.1. Teklif edilecek SIEM çözümü aşağıda belirtilen kriterlere göre lisanslanmalıdır.

1.1.1. Saniyede en az 5000 (EPS) adet olay kaydı toplanmalıdır.

1.1.2. En az 125 adet gelişmiş ajan desteği olmalıdır.

1.1.3. En az 300 adet kaynaktan olay kaydı toplanmalıdır.

1.1.4. Çözüm en az 3 senelik destek lisansı ile tekliflendirilmelidir. Lisansların sahipliği müşteriye ait olacak ve kiralama modeli ile tekliflendirme yapılmayacaktır.

1.2. Teklif edilecek SIEM çözümü, "Bilgi Güvenliği ve Olay Yönetimi – Teknik Özellikler" kısmında belirtilen tüm özellikleri içeren lisansları kapsama ve desteklemelidir.

2. Bilgi Güvenliği ve Olay Yönetimi Teknik Özellikleri

2.1. SIEM çözümü, donanım veya sanal sunucu altyapısında çalışmayı desteklemelidir. Aşağıda belirtilen sanallaştırma altyapılarını desteklenmelidir:

2.1.1. ESX 6.7 U2 ve üstü

2.1.2. Hyper-V 2012 R2 ve üstü

2.1.3. KVM

2.1.4. Microsoft Azure

2.1.5. Amazon Web Services (AWS)

2.1.6. Google Cloud Platform (GCP)

2.2. Önerilecek SIEM çözümü aşağıda belirtilen veritabanları üzerinde olay kaydını depolamayı desteklemelidir.

2.2.1. EventDB

2.2.2. Elasticsearch

2.2.3. ClickHouse

2.3. Önerilecek SIEM çözümü yatayda ölçeklenebilir olmalı ve görev dağılımı belirli işlemler için farklı sunuculara dağıtılabilmelidir, SIEM'in bileşeni olan bu sunucular (Harici toplayıcı ve Harici işleyici) ek yazılım lisansı gerektirmemelidir.

2.4. Önerilecek SIEM çözümü, harici toplayıcı (collector) sunucu kullanarak, farklı sahalardan olay kaydı toplayabilmelidir. Bu şekilde olay kaydı toplama yükü farklı bir sunucuya aktarılabilmelidir. Harici Toplayıcı aşağıdaki özellikleri barındırmalıdır:

2.4.1. Gerektiğinde harici toplayıcılar (collector) ile olay kayıtlarını ajanlı ve ajansız toplamak mümkün olabilmelidir.

2.4.2. Harici toplayıcılar (collector) topladığı olay kayıtlarını korelasyon bileşenine HTTPS protokolü üzerinden gönderebilmelidir.

2.4.3. Harici toplayıcılar (collector) logları merkezi birime gönderemediği durumda ise logları kendi üzerinde tutabilmelidir.

2.4.4. Harici toplayıcılar (collector) topladığı olay kayıtlarını gönderim öncesinde sıkıştırabilmelidir.

2.4.5. Harici toplayıcıların (collector) arızalanması durumunda yeni harici toplayıcılar (collector) sisteme kolaylıkla eklenebilmeli ve kendi üzerinde bir IP yapılandırması dışında bir ayar ve konfigürasyona gerek duymadan hızlıca devreye girebilmelidir.

2.4.6. Harici toplayıcılar (collector) ağ akış bilgisini (flow) alabilmelidir. Aşağıda belirtilen ağ akış (flow) çeşitlerini desteklenmelidir.
- 2.4.6.1. Netflow
- 2.4.6.2. SFlow
- 2.4.6.3. Cisco AVC
- 2.4.6.4. NBAR
- 2.4.6.5. IPFix

2.4.7. Harici toplayıcılar (collector) topladıkları olay kayıtlarını filtreleme özelliğine sahip olmalıdır. Hariç tutulan olay kayıtları, anlık olay kaydı (EPS) lisansından hariç tutulmalıdır.

2.4.8. Harici Toplayıcılar (collector) Diode modda çalışmayı desteklemelidir. “Diode” modda aşağıda belirtilen özellikler desteklenmelidir.
- 2.4.8.1. İnternet bağlantısı olmadan kurulum yapabilme yeteneği
- 2.4.8.2. Merkez sunucuya kayıt olmadan çalışma yeteneği
- 2.4.8.3. Yerel yapılandırma kullanarak syslog, SNMP Trap ve Windows günlüklerini WMI/OMI protokolü aracılığıyla toplama yeteneği
- 2.4.8.4. Syslog protokolü kullanarak olayları başka bir toplayıcıya UDP/514 üzerinden gönderme yeteneği

2.5. Önerilecek SIEM çözümü, kendine olay kaydı gönderen sistemlerin dahil olduğu gruplanmış bir envanter sistemine sahip olmalıdır. Keşfedilen sistemler, log kaynağına dönüştürülebilmeli ayrıca bu sistemlere ait performans verileri toplanabilmelidir. (CMDB)

2.6. Önerilecek SIEM çözümü, verilen ip/subnet içerisindeki sistemleri ajan olmaksızın otomatik olarak en az WMI, VMSDK, snmp, ping yöntemleri ile belirli zaman aralıklarında keşfedebilmelidir. Keşfedilen sistemler dahili bir envanter sistemi (CMDB) veri tabanında takip edilmeli ve log kaynaklarının performans bilgileri izlenebilmelidir.

2.7. Önerilecek SIEM çözümü, belirli türde cihazlar için konfigürasyon yedeğinin alınması ve iki konfigürasyon arasındaki farkın karşılaştırılabilmesini desteklemelidir.

2.8. Önerilecek SIEM çözümü; uygulama, ip adres subnet, VIP ip adresi, proxy ip adresi kriterleri ile keşif yapabilmelidir.

2.9. Önerilecek SIEM çözümü, keşfedilen sistemlere ip/subnet seviyesinde yer (lokasyon) bilgisi girilebilmelidir. Bu bilgiler CSV dosyası olarak da sisteme aktarılabilmedir.

2.10. Önerilecek SIEM çözümü, keşif esnasında SIEM sistemine girilen local SNMP “community” anahtar kelimesi ve Windows AD kullanıcı bilgilerinin yanı sıra harici kullanıcı bilgisi sağlayan sistemler ile entegrasyon sağlayabilmelidir.

2.11. Önerilecek SIEM çözümü, Amazon AWS ve Microsoft Azure sistemlerini de uzaktan keşfedebilmelidir. Amazon AWS ve Microsoft Azure üzerinde aşağıda belirtilen servisler desteklenmelidir:
- 2.11.1. Amazon AWS CloudTrail
- 2.11.2. Amazon AWS CloudWatch
- 2.11.3. Amazon AWS EC2
- 2.11.4. Amazon AWS ELB
- 2.11.5. Amazon AWS Kinesis
- 2.11.6. Amazon AWS RDS
- 2.11.7. Amazon AWS SQS
- 2.11.8. Amazon Security Hub
- 2.11.9. Microsoft Azure Audit
- 2.11.10. Microsoft Azure Compute
- 2.11.11. Microsoft Azure Event Hub

2.12. Önerilecek SIEM ürünü, keşfedilen sistemlerde önemli interface, process ve port’lar seçilerek sadece kritik interface, process ve portlara ilişkin oluşacak olay (incident) verisi oluşturabilmelidir.

2.13. Önerilecek SIEM ürünü, keşfedilen sistemlerde istenilen disklerin doluluk durumunu takip edip diskin doluluk oranı belirli seviyeyi geçtiği durumlarda olay (incident) kaydı yaratabilmelidir. Kullanıcı takip edilecek diskler için hariç tutma (exclusion) tanımı yapabilmelidir.
2.14. Önerilecek SIEM ürünü, gerçek zamanlı, memory üzerinde korelasyon yapabilmelidir.
2.15. Önerilecek SIEM ürünü, topladığı olay kayıtlarını sıkıştırılmış şekilde tutabilmelidir.
2.16. Önerilecek SIEM ürünü, toplanan olay kayıtlarını "nosql" veri tabanı üzerinde tutmalı, böylece yapılacak aramalara daha hızlı cevap verebilmelidir. İlişkisel veri tabanı sadece konfigürasyon ve vaka (incident) kayıtlarının depolanması amacıyla kullanılmalıdır.
2.17. Veri toplamak veya cihazlarla haberleşebilmek amacıyla aşağıdaki protokolleri desteklemelidir:
    2.17.1. SNMP
    2.17.2. WMI
    2.17.3. VM SDK
    2.17.4. Telnet
    2.17.5. JDBC
    2.17.6. SSH
    2.17.7. OMI (Open Management Infrastructure)
2.18. Önerilecek SIEM çözümü, WMI üzerinden belirli Windows (Security, System ve Application Events) olaylarını uzaktan çekebilmelidir. Event ID bilgisi tanımlanarak istenmeyen olay kayıtları hariç tutulabilmelidir.
2.19. Önerilecek SIEM çözümü, güncel GeoIP verisine sahip olmalı, belirli aralıklarla otomatik şekilde ilgili liste güncellenebilmelidir.
2.20. Önerilecek SIEM çözümü, dinamik takip listeleri tutabilmelidir. Korelasyon sonucunda bu listelere objeler (IP Adresi, Metin, Rakam, Tarih tipinde) eklenerek, gerektiğinde bu listeler farklı korelasyon kurallarında kullanılabilmelidir.
    2.20.1. Ping
    2.20.2. Traceroute
    2.20.3. TCP
    2.20.4. Http/Https
    2.20.5. SMTP
    2.20.6. POP
    2.20.7. DNS
    2.20.8. SSH
    2.20.9. LDAP
    2.20.10. JDBC
    2.20.11. FTP
2.21. Önerilecek SIEM çözümü, envanter takip sistemi üzerinden XML formatında rapor şablonları dışarıya alabilmelidir.
2.22. Önerilecek SIEM çözümü, dinamik takip listeleri tutabilmelidir. Korelasyon sonucunda bu listelere objeler (IP Adresi, Metin, Rakam, Tarih tipinde) eklenerek, gerektiğinde bu listeler farklı korelasyon kurallarında kullanılabilmelidir.
2.23. Önerilecek SIEM çözümü, zararlı IP, zararlı URL, zararlı domain, zararlı process, zararlı hash bilgilerini aşağıda listelenen 3. parti tehdit istihbarat veri tabanları ile entegre olarak güncelleyebilmelidir.
    2.23.1. ThreatConnect
    2.23.2. ThreatStream
    2.23.3. TruSTAR
    2.23.4. Emerging Threat Malware
    2.23.5. MISP
    2.23.6. OpenCTI
    2.23.7. DigitalSide Threat-Intel

2.24. Önerilecek SIEM çözümü, sistemi anonim (open proxies, tor vb.) network bilgilerini 3. parti tehdit istihbarat veri tabanlarından düzenli olarak indirmeye imkan tanımalıdır.
2.25. Önerilecek SIEM çözümü, zararlı ip ve domain'leri CSV formatında okuyup, sisteme dahil edebilmelidir.
2.26. Önerilecek SIEM çözümü, istenilen ağ, sistem, depolama alanı, servis vb. elemanlarının dahil olduğu birçok servis grubu oluşturabilmelidir. Grup olarak tüm elemanlarının performans, erişilebilirlik, olay kaydı bilgilerini gösterebilmelidir.
2.27. Önerilecek SIEM çözümü, sadece arayüz yardımıyla yeni cihaz ve log ayrıştırıcı (log parser) tanımlarını uzak toplayıcılara gönderebilmelidir. Log ayrıştırıcı testleri, sisteme yüklenen örnek kayıtlar ile gerçekleştirebilmelidir.
2.28. Önerilecek SIEM çözümü, sisteminde olmayan cihazlar için log ayrıştırıcı (log parser) yöntemi bilinen bir yazım sistemi (örneğin XML) ile yazılarak sisteme dahil edilebilmelidir.
2.29. Önerilecek SIEM çözümü Windows ajanı yardımıyla ilgili sunucularda uzaktan powershell scripti işleterek sonuçlarını olay kaydı olarak sisteme alabilmelidir.
2.30. Önerilecek SIEM çözümü, sistem üzerinde belirtilen bir klasöre SFTP veya SCP protokolü üzerinden yüklenen PCAP dosyalarını analiz edip olay kaydına dönüştürebilmelidir.
2.31. Önerilecek SIEM çözümü, belirli cihazlardan gelen log kayıtlarını başka cihazlara toplanan log kaydının tipine göre syslog veya netflow formatında yönlendirebilmelidir.
2.32. Önerilecek SIEM çözümü, Windows ajanı yardımı ile önceden tanımlanan dosya, dizin ve Microsoft Windows Registry değişikliklerini takip edebilmeli ve bu değişikliğe bağlı olay kaydı yaratabilmelidir.
2.33. Önerilecek SIEM çözümü, belirli log kayıtlarını giriş esnasında hariç tutma yeteneğine sahip olmalıdır. Hariç tutulan log kayıtları EPS lisansına etki etmemelidir.
2.34. Önerilecek SIEM çözümü, bir syslog paketindeki çok satırlı syslog kayıtlarını birleştirebilmelidir.
2.35. Önerilecek SIEM çözümü, Alınan log içerisindeki bilgilerin zenginleştirilmesini desteklemelidir. Örneğin hedef adresin hangi ülke ve şehirde bulunduğu bilgisini log kaydının gösterimi sırasında gösterebilmeli ve bu bilgiyi kullanarak analiz yapılabilmesini mümkün hale getirebilmelidir.
2.36. Önerilecek SIEM çözümü, hali hazırda en az 3500 adet rapor şablonundan oluşan raporlama kütüphanesine sahip olmalıdır.
2.37. Önerilecek SIEM çözümü, aşağıdaki uyumluluk süreçleri için hazır raporlar oluşturabilmelidir:
    2.37.1. PCI
    2.37.2. HIPAA
    2.37.3. SOX
    2.37.4. FISMA
    2.37.5. ISO 27001
    2.37.6. COBIT
    2.37.7. ITIL
    2.37.8. NIST800-53
    2.37.9. NIST800-171
    2.37.10. CIS
2.38. Takip amaçlı görüntülüme ekranlarına sahip olmalı istenirse "sunum" görünümünde olabilmelidir.
2.39. Gösterge paneli görüntülemesi sırasında aşağıdaki tiplerde verinin görüntülenmesi desteklenmelidir:
    2.39.1. Bar Chart
    2.39.2. Pie Chart
    2.39.3. Line Chart
    2.39.4. Table Chart
    2.39.5. Treemap Chart

2.39.6. Scatter graph
2.39.7. Gauges Chart
2.39.8. Geographical Map

2.40. Vaka oluşması durumunda script çalıştırma özelliği bulunmalıdır. Sistem üzerinde hazır script'ler bulunmalıdır. Bu script'ler ile en az aşağıda belirtilen aksiyonlar alınabilmelidir.
2.40.1. Aynı üreticiye ait güvenlik duvarı üzerinde IP Adresi bloklanması
2.40.2. Linux sistemi üzerinde servisin tekrar başlatılması
2.40.3. Microsoft Windows Active Directory üzerinde kullanıcının hesabının askıya alınması

2.41. Önerilecek SIEM çözümü, aşağıda belirtilen ITSM çözümleri ile entegre olabilmelidir.
2.41.1. ConnectWise
2.41.2. ServiceNow
2.41.3. Salesforce

2.42. Önerilecek SIEM çözümü, anahtar kelime bazlı arama tüm log alanlarında veya istenilen bir alan dahilinde yapılabilmelidir.

2.43. Önerilecek SIEM çözümü, geçmişe yönelik arama yapılabilmesi desteklenmelidir.

2.44. Önerilecek SIEM çözümü, arama yapılırken boolean filtreler, gruplamalar, zaman bazlı filtreler, regex kullanımı desteklenmelidir.

2.45. Önerilecek SIEM çözümü, istatiksel profiller desteklenmelidir. Örneğin sistemin network kullanımında olağan dışı bir artış olduğunu anlayabilmeli ve alarm üretebilmelidir.

2.46. Önerilecek SIEM çözümü, sistem veri karıştırma (obfuscation) özelliğine sahip olmalı, müşteri verilerinin olduğu kısımları gerekli ayarlamalarla arayüzünde karıştırılmış olarak gösterebilmelidir.

2.47. Önerilecek SIEM çözümü, sistem karıştırılmış (obfuscation) verileri gerektiğinde bir yetkilendirme ile arayüzde gösterebilmelidir.

2.48. Önerilecek SIEM çözümü, zamanlanmış raporların oluşturulması desteklenmelidir. Bu raporlar CSV veya PDF formatında dışarı alınıp eposta ile de gönderilebilmelidir.

2.49. Önerilecek SIEM çözümü, korelasyon kuralları ile toplanan olay kayıtları üzerinde sorgu çalıştırarak vaka oluşturmayı desteklemelidir. Korelasyon kuralları aşağıdaki özellikleri desteklemelidir.
2.49.1. Sistem üzerinde en az 2600 adet korelasyon kuralı bulunmalıdır.
2.49.2. Korelasyon kuralları içerisinde farklı korelasyon kurallarını kullanmayı desteklemelidir.
2.49.3. Mitre Attack Framework Kategorileri ile eşleşen korelasyon kurallarında Mitre Attack "Taktik" kategorisi ve Mitre Attack "Teknik ID" belirtilmelidir.
2.49.4. Korelasyon kuralların "and", "or", "and not", "followed by", "not followed by" şeklinde ilişkilendirme özellikleri bulunmalıdır.
2.49.5. Korelasyon kuralları tetiklenmesi sonucunda script çalıştırılarak aksiyon alınabilmelidir.
2.49.6. Korelasyon kuralları içinde hariç tutma (exclusion) listeleri kullanılabilmelidir.
2.49.7. Korelasyon kuralları için zaman aralığı tanımı yapılarak örneğin son 10 dakika içerisinde çalışma koşulu belirtilmelidir.
2.49.8. Ürün güncellemesi yapılmadan "GeoLocation" veritabanı, "korelasyon kuralları", "Log Ayrıştırıcı" (Parser) ve rapor şablonları çözümün içerisinde bulunan paket dağıtımı modülü sayesinde güncellenebilmelidir.

2.50. Önerilecek SIEM çözümü, güvenli web arayüz üzerinden yönetilebilmelidir.

2.51. Önerilecek SIEM çözümü, log kaynaklarından toplanan envanter bilgisi, performans verisi, güvenlik olaylarını aynı ekrandan üzerinden analiz edilmesini sağlayabilmelidir.

2.52. Önerilecek SIEM çözümü, rol temelli yönetim desteği olmalıdır, yönetici, standart kullanıcı, sadece görüntüleme özelliklerinin yanı sıra aşağıdaki şekilde roller oluşturulabilmelidir.

2.52.1. Sadece Network sistemlerinin kayıtlarını yönetebilme
2.52.2. Sadece Windows sistemlerinin kayıtlarını yönetebilme
2.52.3. Sadece Unix sistemlerinin kayıtlarını yönetebilme
2.52.4. Sadece Güvenlik sistemlerinin kayıtlarını yönetebilme

2.53. Önerilecek SIEM çözümü, kullanıcı kimlik doğrulamasını yerel veritabanı veya harici LDAP, Radius, SAML, Okta, Duo sistemlerinden yapabilmelidir.

2.54. Önerilecek SIEM çözümü, raporlarında firma logosunun konulmasına izin vermelidir.

2.55. Önerilecek SIEM çözümü, kendi sistemine ait kaynak kullanımlarını (hafıza, CPU, disk vb.) ve process bilgilerini ayrıntılı şekilde gösterebilmelidir. Olağan dışı artışlarda alarm oluşturulabilmelidir.

2.56. Önerilecek SIEM çözümü, arayüz üzerinden arşivleme politikası özelliği ile belirtilecek gün sayısına istinaden olay kayıtlarının arşivlenmesini desteklemelidir.

2.57. Önerilecek SIEM çözümü, olay kayıtlarını bir parmak izi algoritması ile (örneğin sha256) kaydedip, sonrasında bütünlüğünü doğrulayabilmelidir.

2.57.1. Davranış analizi modülü, uç noktada kullanılan ajan sayısına göre lisanslamalıdır.

3. Kurulum ve Destek Paketi

3.1. Üretimi bitmiş (End of Life) yazılım temin edilmeyecektir. Tüm ürünler yeni ve kullanılmamış olacaktır.

3.2. Yüklenici Log Yönetim Sisteminin yazılım ve donanım bileşenlerinin kurulum, log kaynaklarının eklenmesi, özel kurallar, raporlar, korelasyon kurallarının oluşturulması (varsayılan olarak tanımlı gelenler haricinde) ve özel ayrıştırıcıların (parser) yazılması ile ilgili eğitim ve teknik destek hizmetlerini sunacaktır.

3.3. Yüklenici kurulumda yapacağı işlemleri Log Korelasyon ve Yönetim Sisteminin yöneticilerine örnek uygulamalarla “iş üzerinde” (hands-on) gösterip İdare’ye devredecektir.

3.4. Yüklenici sistem ile beraber gelen raporlar haricinde, 25 (yirmi beş) adet İdare tarafından talep edilen özel rapor, dashboard (gösterge paneli) veya kayıtlı arama şablonu hazırlayacaktır. Raporlama özellikleri, sistem yöneticilerine örnek uygulamalarla “iş üzerinde” (hands-on) yüklenici tarafından gösterilip devredilecektir.

3.5. Kurulum çalışmaları, sertifika sahibi veya konusunda en az 2 (iki) yıl tecrübeli yüklenici veya üretici personeli tarafından yapılacaktır.

3.6. Yüklenicinin temin edilen SIEM ürünü için en az 3 (üç) personelinin geçerli sertifikaya sahip olması gerekmektedir.

3.7. YÜKLENİCİ, ISO 9001, ISO 27001, ISO 20000-1 ve TSE A tipi Sızma Testi sertifikasına sahip olmalıdır.

3.8. Kurulum kapsamındaki entegrasyonlar, proje süreci boyunca İdare tarafından teslim edilecek log kaynakları listesi üzerinden yüklenici tarafından yapılacaktır. Yüklenici her log kaynağı tipine göre entegrasyonu sağlayacak ve İdare’nin Log Yönetim Sistemi yöneticilerine “iş üzerinde” (hands-on) uygulamalarla gösterip devredecektir.

3.9. Log Yönetim Sistemi teslimatı, kurulumu, devreye alma işlemleri ve kritik işlemler yüklenici veya üretici personeli tarafından İdare’nin göstereceği yerde yapılacaktır. Kritik işlemler haricîndeki diğer işlemler (açılış toplantısı, ilerleyiş toplantısı, kaynak ekleme, ayrıştırıcı (parser) yazma/ekleme, versiyon yükseltme, vb.) İdare ve yüklenici karşılıklı anlaşarak yerinde veya uzaktan yapılacaktır.

3.10. Yüklenici, İdare’ye SIEM kurulumu kapsamında,

- Başlangıç toplantısının düzenlenmesini sağlayacaktır.
- Proje planını paylaşacaktır.
- Temel ürün kurulumlarının gerçekleştirilmesini sağlayacaktır.
- Log kaynaklarının eklenmesi, pars işlemleri, izleme listeleri vb. SIEM üstündeki geliştirmeleri yapacaktır.

- 30 (otuz) adete kadar özel korelasyon kuralı hazırlama desteği verecektir. (Korelasyon kuralı yazma özellikleri, sistem yöneticilerine "iş üzerinde" (hands-on) gösterip devredecektir.)

3.11. Yüklenici, İdare'ye ihale dokümanında belirtilen süreyle SIEM bakımı kapsamında,

- Mesai saatleri içinde yerinde veya uzaktan destek verecektir.
- Mesai saatleri içinde sınırsız telefon desteği verecektir.
- 7. Maddedeki SLA'ler içerisinde destek süreçlerini yürütecektir.
- Destek süreci kurulum tamamlanıp ürün devereye alındıktan sonra başlayacaktır. Kurulum süreci SIEM şartname maddelerinin tamamlanması, bileşenlerinin kurulması, ayarlarının yapılması ve sözleşmede belirtilen sayıda log kaynağının eklenmesi ile tamamlanmış sayılacaktır.

3.12. Yüklenici, İdare'ye sağlayacağı bakım hizmeti kapsamında uygulanacak olan talep ve değişiklik süreçlerini web üzerinden erişilebilen destek portalı platformu üzerinden takip edecektir. İdare tarafından iletilecek olan talep ve değişiklik isteklerini iletmek için İdare ile önceden belirlenen iletişim kanalları (Destek portalı, Çağrı Merkezi, E-mail) seçeneklerini kullanacaktır.

3.13. Log Yönetim Sistemi kurulumu, İdare'nin belirleyeceği mesai içi ve/veya mesai dışı saatlerde yapılacaktır. Tüm bu kurulumlar için ilave hizmet, ulaşım, konaklama gibi bedeller yükleniciye ait olacaktır.

3.14. Log Yönetim Sistemi kurulumuna ilişkin olarak İdare'ye özel dokümantasyon hazırlanarak teslim edilecektir.

3.15. Yüklenici, aşağıda belirtilen hizmetleri ve yükümlülüklerini yerine getirebilmesi için yetkin personeller ile destek hizmeti sağlayacaktır.

3.16. Yüklenici güncelleme ve yenileştirme çalışmalarını İdare'nin onayı dâhilinde, yüklenici ve İdare tarafından belirlenecek uygun bir zamanda yapacaktır.

4. SLA

Önem Seviyeleri	
Önem seviyesi	**Açıklama**
Kritik	İş süreçlerine ağır etki eden. Ana iş sürecinin çalışmasını engelleyen. Uygulamalara erişilemiyor olması ve/veya hasar görmüş olması. Ana iş süreçlerinin fonksiyonlarının yerine getirilememesi. Uygulama sunucularına veya veri tabanlarına erişilemiyor olması.
Yüksek	İş süreçlerine etkisi büyük. Kritik uygulamaların bir kısmı çalışmıyor ve/veya ciddi etkilenmiş. Kritik fonksiyonların yerine getirilemiyor olması. Kullanıcıların çalışabilmesi ancak verimlilik seviyelerini düşüren etkenler.
Orta	İşle ilgili küçük talepler, yeni donanım kurulum, değişim talepleri. Önemli nitelikte olan, ancak yüksek öncelikli olarak eylem yapılmasını gerektirmeyen herhangi bir talep ve problemler. Hizmet üretken durumdadır, ancak Hizmet Talebinin yerine getirilmemesi durumunda, bu göz ardı edilemeyecek etkiye yol açar. İş süreçlerine etki eden ancak üretimi engellemeyen durumlar.
Düşük	Planlanabilecek herhangi bir talep veya problem. Arıza veya sorunun kullanıcıya etkisinin min. Düzeyde olduğu durumlar. Planlama ile çözülebilecek problem ve/veya talepler.

Hizmet Seviyeleri Müdahale Süreleri		
Önem Derecesi	**Olay Yönetimi**	**Talep Yönetimi**

Kritik (Critical)	2 Saat	4 Saat
Yüksek (High)	4 Saat	8 Saat
Orta (Medium)	8 Saat	16 Saat
Düşük (Low)	16 Saat	32 Saat