T.C.
ERCİYES ÜNİVERSİTESİ
DÖNER SERMAYE İŞLETMESİ
TEL : 437 49 20 Fax : 437 52 88

SAYI : 8447197-934-01-
KONU: Teklif Mektubu Hakkında

KAYSERİ
26/06/2024

Üniversitemiz Tıp Fakültesi Hastanemizde Kullanılmak üzere aşağıda cins ve miktarla belirtilen malzemelere ihtiyaç vardır.
Müesseseniz tarafından ilgili malzemelerin temini mümkün ise Yaklaşık Maliyet tespitinde kullanılmak üzere birim fiyatı teklif verilmesini rica ederim.

Tacım DEMİRTAŞ
İşletme Müdürü

HASTANELER GENELİ					
Sıra No	Malzeme Adı	Birimi	Miktarı	Birim Fiyat	Toplam Tutar
1	GÜVENLİK DUVARI LİSANSI(3 YILLIK)	ADET	1		
			GENEL TOPLAM=		

KAŞE - İMZA

	TEKNİK ŞARTNAMESİ EKTEDİR.			
A	SİLİNTİ VE KAZINTI OLAN TEKLİFLER REDDEDİLİR.			
B	TEKLİF MEKTUPLARİ FİRMA BAŞLIKLI KAĞITLARINA YAZILACAK.			
C	ZAMANINDA VERİLMEYEN, AÇIK ADRES, KAŞE VE İMZA OLMAYAN TEKLİFLER DEĞERLENDİRİLMEZ.			
D	TEKLİF ZARFLARI KAPALI OLMALI VE TEKLİF KONUSU ZARFIN ÜZERİNE YAZILI OLMALIDIR.			
E	TEKLİF EDİLEN ÜRÜNLERİN, MARKASI VE AMBALAJ ŞEKLİ YAZILMALIDIR.			
F	TEKLİF EDİLEN ÜRÜNLERİN, BİRİM FİYATI RAKAM VE YAZI İLE YAZILMALIDIR.			

G	*TEKLİF EDİLEN TIBBİ MALZEMELERİN TC. İLAÇ VE TIBBİ CİHAZ ULUSAL BİLGİ BANKASI TARAFINDAN ONAYLANMIŞ ÜRÜN (BARKOD) NUMARASI ÜRÜNÜN ÜZERİNDE, ÜRÜN KODU VE BRANŞ KODU ETİKET VE MARKA ADI TEKLİF MEKTUPLARINDA YAZILI OLACAKTIR.*			
H	İSTEKLİ FİRMALAR; SOSYAL GÜVENLİK KURUMUNUN YAYINLAMIŞ OLDUĞU SAĞLIK UYGULAMA TEBLİĞİ (SUT) HÜKÜMLERİNE GÖRE TEKLİF ETMİŞ OLDUKLARI MALZEMELER İLE İLGİLİ, MALZEMENİN EK-3 LİSTESİNDE OLUP OLMADIĞINI, MALZEMENİN EK-3 LİSTESİNDE OLMASI DURUMUNDA SUT KODUNU FİRMA ORJİNAL ANTETLİ KAĞIDA YAZARAK BİLDİRECEKLERDİR.			
I	ÖDEME SIRASININ VE GÜNÜNÜN BELİRLENMEİSNDE; DÖNER SERMAYELİ İŞLETMELER BÜTÇE VE MUHASABE YMNETMELİĞİNİN 22. MADDESİ HÜKÜMLERİ UYGULANACAKTIR.			
İ	*TEKLİF EDİLEN ÜRÜN FİYATLARININ DEĞERLENDİRİLMESİNDE SUT FİYATLARI DİKKATTE ALICAKTIR.*			

Teklif mektuplarının en geç **02/07/2024** Salı günü mesai bitimine kadar E.Ü.Döner Sermaye İşletmesi'ne bırakılmasını rica eder.

T.C. ERCİYES ÜNİVERSİTESİ
TIP FAKÜLTESİ HASTANELERİ

YENİ NESİL GÜVENLİK DUVARI LİSANS YENİLEME TEKNİK ŞARTNAMESİ

2024

T.C. ERCİYES ÜNİVERSİTESİ
TIP FAKÜLTESİ HASTANELERİ

İçindekiler

T.C. ERCİYES ÜNİVERSİTESİ
TIP FAKÜLTESİ HASTANELERİ

1. AMAÇ VE KAPSAM

Bu şartname T.C. Erciyes Üniversitesi Sağlık Uygulama ve Araştırma Merkezi bünyesinde yürütülen projelerde kullanılmak üzere Kurumun ihtiyacı olan Yeni Nesil Güvenlik Duvarı Lisanslarının yenilenmesi amacıyla hazırlanmıştır.

2. TANIMLAR

2.1. **İDARE/KURUM** : T.C. Erciyes Üniversitesi Tıp Fakültesi Hastaneleri
2.2. **İSTEKLİ** : İhaleye teklif veren firma
2.3. **YÜKLENİCİ** : İşi yüklenecek olan gerçek veya tüzel kişi
2.4. **TARAF** : İDARE veya YÜKLENİCİ
2.5. **ÜRÜN** : İhale kapsamında teklif edilen her türlü malzeme, cihaz
2.6. **SİSTEM** : İhale kapsamında kullanılan her türlü malzeme ve hizmetlerin bütünü
2.7. **AY** : Takvim ayı
2.8. **İŞ GÜNÜ** : Resmî tatiller haricinde haftanın Pazartesi, Salı, Çarşamba, Perşembe, Cuma günleri
2.9. **MÜDAHALE** : Sorunun başlama zamanından itibaren, sorunun çözümüne ilişkin çalışmaların YÜKLENİCİ tarafından başlatılması
2.10. **ÇÖZÜMLEME** : İdare tarafından cihaz sorun bildiriminden itibaren, sorunun çözülmesi ve hizmet işlemine başlaması
2.11. **KABUL İŞLEMİ** : Yüklenici tarafından iş bu şartname maddelerine uygun olarak şartların tamamlanması, idarenin Komisyonu tarafından yapılacak kontroller ile onaylanmasıdır.
2.12. **HİZMET İŞLEMİ** : Cihazların veri kaybına yol açmadan aktif çalışır bir şekilde bağlı bulunduğu sunuculardaki/sistemlerdeki işlemleri gerçekleştirmesidir.

3. GENEL HÜKÜMLER

3.1. İstekli, İdare'nin menfaatleri doğrultusunda çalışmayı ve talimatları doğrultusunda gizlilik esaslarına uygun şekilde hareket etmeyi kabul eder.
3.2. İhale bir bütün olarak düşünülmelidir. Kısmi veya alternatifli teklifler kabul edilmeyecektir.
3.3. Yüklenici, İdare'ye irtibat için telefon numaralarını ve adreslerini sözleşmenin imzalandığı tarihinden itibaren en geç 2 (iki) gün içinde yazılı olarak bildirecektir. Taşınma veya herhangi bir sebeple Yüklenicinin telefon numarasının veya adresinin değişmesi durumunda Yüklenici, İdare' ye yeni adres veya telefon numaralarını en geç 2 (iki) gün içerisinde yazılı olarak bildirecektir.
3.4. İstekli firma TSE Hizmet yeterlilik belgesi, ISO 9001 Kalite Belgesi ve ISO 27001 Kalite Belgesi sahip olmalıdır ve teklif dosyasına eklemelidir.
3.5. Yüklenici, şartnamede belirtilen süreler içerisinde hizmetlerin ifası, cihazların aktif çalışır şekilde teslim edilmesi, garanti şartlarını sağlamak amacıyla yeterli ve her türden kaynağı sağlamakla yükümlüdür.
3.6. Yüklenici, şartnamede belirtilen ürünleri ve hizmetleri İdare'nin teslim öncesinde bildireceği yerde teslim etmekle ve/veya sağlamakla yükümlüdür.

3.7. İşbu şartnamede belirtilen işlerin, şartnamede tarif edildiği şekilde ve anahtar teslimi olarak bitirilmesi esastır. Yüklenici, ihale bedeli dışında hiçbir şekilde ek ücret talep etmeyecektir. Bu sebeple; Yüklenici, işine etki edecek tüm yapısal ve nihai hususları dikkatle gözden geçirmeli ve buna göre tüm aksesuarları temin etmelidir.

3.8. Mücbir sebepler dışında oluşabilecek her türlü zarardan Yüklenici sorumludur.

3.8.1. Mücbir sebepler

a) Doğal afetler.
b) Kanuni grev.
c) Genel salgın hastalık.
d) Kısmi veya genel seferberlik ilanı.
e) Gerektiğinde Kamu İhale Kurumu tarafından belirlenecek benzeri diğer haller.

3.8.2. Yukarıda belirtilen hallerin mücbir sebep olarak kabul edilmesi ve yükleniciye süre uzatımı verilebilmesi için, mücbir sebep olarak kabul edilecek durumun;

a) Yüklenicinin kusurundan kaynaklanmamış olması,
b) Taahhüdün yerine getirilmesine engel nitelikte olması,
c) Yüklenicinin bu engeli ortadan kaldırmaya gücünün yetmemesi,
d) Mücbir sebebin meydana geldiği tarihi izleyen yirmi gün içinde yüklenicinin İdareye yazılı olarak bildirimde bulunması,
e) Yetkili merciler tarafından belgelendirilmesi, zorunludur.

3.9. Şartnamedeki herhangi bir maddeyi sağlayamayan teklifler değerlendirme dışı bırakılacaktır.

3.10. Teklif edilen tüm Ürünlerin teklifte belirtilecek olan teknik özellikleri, üretici Firmaların kendi web sayfalarında veya teklifle birlikte sağlanacak orijinal teknik dokümanlardaki bilgilerle çelişmeyecektir.

3.11. Teklif edilen tüm Ürünler ve şartnamenin ilgili maddelerinde istenilen özellikler ihalenin yapıldığı tarihte ana üreticinin web sayfasından erişilebilen teknik dokümanlarda duyurulmuş, kullanılabilir durumda ve standart üretim olmalı, ihaleye uygunluk açısından değiştirilmiş olmamalıdır.

3.12. İstekli, şartnamenin her maddesinin altına "Okunmuş, anlaşılmış ve kabul edilmiştir" yazacak ve her sayfanın altına kaşe ve imzasını ekleyecektir.

3.13. İstekli, teklif edeceği Ürünleri, varsa sunulan ek özellikleri Teknik Şartname cevaplarında ayrıntılı olarak açıklayacak ve bu özellikleri üretici Firma Ürün broşür ve/veya kullanım kılavuzlarını tekliflerine ENG/TR olarak ekleyerek belgeleyecektir.

3.14. Yüklenici'nin teslim ettiği hiçbir ürün, teklif tarihinde kabul tarihinden sonra en az 6 ay içerisinde "End Of Life" ve 5 yıl içerisinde "End of Support" olmayacaktır. Bu süre içerisinde "End Of Life" olan ürünler bedelsiz olarak yüklenici tarafından yenisi ile değiştirilecektir.

3.15. Yüklenici, teklif ettiği tüm cihazları ve ilgili lisansları, hiç kullanılmamış ve sıfır yeni ürün olarak teslim edilecektir.

3.16. Yüklenici, teklifinde sunduğu Ürünleri ancak İdare onayı sonrası iş bu teknik şartname ile tarif edilen teknik özellikleri karşılayacak şekilde muadilini getirmekle yükümlü olduğu gibi, yeni nesil bir üst sürüm Ürün fiyat farkı talebi olmadan Yüklenici tarafından İdare'ye sunulabilecektir.

3.17. Yüklenici, yapılan inceleme ve testler sonucu istenen teknik özellikleri sağlamadığı belirlenen tüm malzeme ve donanımı herhangi bir ücret talep etmeden, istenen özelliklere sahip malzeme ve donanım ile değiştirmekle yükümlüdür.

3.18. Yüklenici, teklif ettiği ürün ve hizmetleri İdare'nin belirleyeceği yerde ve ölçütler doğrultusunda kurmakla, hizmet işlemi verecek duruma getirmekle mükelleftir.

3.19. Yüklenici, işbu Şartname kapsamındaki yükümlülüklerini yerine getirmek amacıyla gerekli tüm lisans, muvafakat ve yetkileri haiz olduğunu taahhüt eder.

3.20. Yüklenici, tüm donanım ve yazılımları "teklif edilen ürün ailesinin sertifikasyonuna sahip" personelleri tarafından kurulacak, konfigüre edilecek ve çalışır halde teslim edecektir.

3.21. İstekli, teklif edeceği tüm ürünleri satmaya yetkili olduklarına dair yetki belgelerini teklifine ekleyecektir. İlgili yetki belgeleri, üretici firmanın Türkiye ofisinden veya üretici firmanın yetkili distribütöründen alınacaktır.

3.22. Yüklenici, kullanacağı tüm cihaz ve parçalar için İdare'nin onayını alarak işe başlayacaktır.

3.23. Yüklenici, işin süresi içerisinde bu kısımda talep edilen tüm cihaz ve yazılımları İdare'nin onaylayacağı şekilde anahtar teslimi çalışır şekilde kurup çalıştıracaktır.

3.24. İstekli, teklif dosyasındaki tüm belgeleri hem kâğıt ortamında hem de dijital CD ortamında (.doc, .docx, .pdf, .xls, .dwg formatlarından biri) teklif esnasında İdare'ye teslim edecektir.

4. YENİ NESİL GÜVENLİK DUVARI LİSANS YENİLEME

4.1. Mevcut iki adet yeni nesil güvenlik duvarının lisansları 3 yıl süre ile yenilenecektir.

4.2. Lisanslar aşağıdaki özellikte olacaktır:

4.2.1. Tümleşik Tehdit Koruma (UTP – Unified Threat Prevention)

4.2.2. 7x24 Üretici Global Teknik Desteği

4.2.3. Mevcut lisanslara ek olarak güvenlik bilgi ve olay yönetim lisansı ücretsiz olarak ilave edilecektir. Lisans aşağıdaki özellikleri sağlayacaktır.

4.2.3.1. Mevcut güvenlik duvarı olay günlük analiz sistemi ile aynı üretici tarafından üretilmiş olacaktır.

4.2.3.2. En az 90 adet ağ cihazından, en az 60 adet sunucu ve kullanıcı bilgisayarı dışındaki diğer muhtelif sistemlerden olay günlüğü alabilecektir.

4.2.3.3. En az 75 gelişmiş ajanı destekleyecektir.

4.2.3.4. Saniyede en az 2500 sayıda olay günlüğünü destekleyecektir.

4.2.3.5. Olay günlükleri arasında gerçek zamanlı ilişki kurmayı, alarm üretmeyi destekleyecektir.

4.2.3.6. Olay bilgisini sıkıştırılmış bir halde tutacaktır.

4.2.3.7. Toplanan olay günlükleri yapılandırma yönetim veritabanında tutulacaktır.

4.2.3.8. Gerektiğinde harici toplayıcılar (collector) ile log toplamak mümkün olabilmelidir.

4.2.3.9. Harici toplayıcılar (collector) topladığı logları korelasyon bileşenine HTTPS protokolü üzerinden gönderebilmelidir.

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

4.2.3.11. Harici toplayıcılar (collector) topladığı logları gönderim öncesinde sıkıştırabilmelidir.

4.2.3.12. 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.

4.2.3.13. Harici toplayıcılar (collector) Netflow bilgisi alabilmelidir.

4.2.3.14. Harici toplayıcılara (collector) gelen kayıtlara (EPS) ve ip adresi sınırı konulabilmelidir.

4.2.3.15. Güvenlik bilgi ve olay yönetim lisansı ürünü verilen ip/subnet içerisindeki sistemleri ajan olmaksızın otomatik olarak WMI, VM SDK(VM Ware vCenter), snmp, ping gibi yöntemler ile

düzenli aralıklarda keşfedebilmelidir. Keşfedilen sistemler bir CMDB veri tabanında yönetilebilmelidir.

4.2.3.16. Güvenlik bilgi ve olay yönetim lisansı ürünü log kayıtların toplandığı tüm sistemleri ilişkilendirilmiş bir CMDB (yapılandırma yönetim veri tabanı) sisteminde toplayabilmelidir.

4.2.3.17. Keşfedilen sistemlere uygulama, ip subnet, VIP ip, proxy ip ve sadece onaylanmış sistemlerin olay kaydı atabilmesi gibi ön filtreler tanımlanarak CMDB ve olay veri tabanı sadeceleştirmesi yapılabilmelidir.

4.2.3.18. Keşfedilen sistemlere ip/subnet seviyesinde yer(lokasyon) bilgisi girilebilmelidir. Bu bilgiler CSV dosyası olarak da import edilebilmelidir.

4.2.3.19. Keşif esnasında Güvenlik bilgi ve olay yönetim lisansı sistemine girilen local SNMP community ve Windows AD kullanıcı bilgilerinin yanısıra harici kullanıcı bilgisi sağlayan sistemler (örneğin CyberArk) ile entegrasyon sağlayabilmelidir.

4.2.3.20. Güvenlik bilgi ve olay yönetim lisansı sistemi Amazon AWS ve Microsoft Azure sistemlerini de uzaktan keşfedebilmelidir.

4.2.3.21. Keşfedilen sistemlerde önemli interface, process ve port'lar seçilerek sadece kritik interface, process ve portlara ilişkin oluşacak yoğunluklar olay (incident) verisi oluşturabilmelidir.

4.2.3.22. Keşfedilen sistemlerde istenilen disk'lerin doluluk durumu olay (incident) verisi oluşturmada hariç tutulabilmelidir.

4.2.3.23. Gerçek zamanlı, memory üzerinde korelasyon yapabilmelidir.

4.2.3.24. Event bilgisi sıkıştırılmış bir halde tutulmalıdır.

4.2.3.25. İlişkisel bir veri tabanı (Oracle, MSSql gibi) üzerinde event kaydı tutmamalıdır, ilişkisel veri tabanı sadece konfigürasyon veya vaka (incident) kayıtlarının depolanması amacıyla kullanılmalıdır.

4.2.3.26. Veri toplamak veya cihazlarla haberleşebilmek amacıyla aşağıdaki protokolleri desteklemelidir:

- SNMP
- WMI
- VM SDK
- OPSEC
- JDBC
- Telnet
- SSHJMX

4.2.3.27. Eklenen cihazların SNMP/WMI protokolü ile CPU, Memory, session sayısı, disk kullanımları, ağ arayüz bilgileri gibi performans verileri ve sistem üzerinde çalışan uygulama durumu her bir sistem için tanımlanabilen aralıklarda monitör edilebilmelidir.

4.2.3.28. Güvenlik bilgi ve olay yönetim lisansı sistemi ping/traceroute, tcp/udp, http/https, smtp, pop3,imap, dns, ssh, ldap, jdbc, ftp vb. gibi uygulama seviyesini de içeren servis kontrolü yapabilmelidir. Synthetic Transaction Monitoring (STM)

4.2.3.29. Güvenlik bilgi ve olay yönetim lisansı sistemi kendine kayıt gönderen sistemlerin dahil olduğu gruplanmış bir envanter sistemine sahip olmalıdır (CMDB)

4.2.3.30. Güvenlik bilgi ve olay yönetim lisansı sistemi belirli sistemler, kullanıcılar için watch list (gözlem listesi) oluşturarak belirli bir sürede oluşabilecek önceden belirli herhangi bir durumda alarm üretebilmelidir. (örneğin belli kullanıcının hesabının kilitlenmesi veya önemli bir process'in down olması gibi)

4.2.3.31. CMDB sistemi üzerinden XML formatında raporlar export edilebilmelidir.

4.2.3.32. Güvenlik bilgi ve olay yönetim lisansı sistemi güncel malware ip, malware URL, malware process bilgilerini düzenli aralıklarla merkezi sistemden güncelleyebilmelidir.

4.2.3.33. Güvenlik bilgi ve olay yönetim lisansı sistemi malware hash bilgilerini merkezi sistem üzerinden veya TAXII protokolü üzerinden harici sistemlerden güncelleyebilmelidir. Ayrıca belli hash bilgilerini de whitelist olarak sınıflandırabilmelidir.

4.2.3.34. Güvenlik bilgi ve olay yönetim lisansı sistemi anonymity (open proxies, tor vb.) network bilgilerini merkezi sistemden düzenli olarak yenileyebilmelidir.

4.2.3.35. Güvenlik bilgi ve olay yönetim lisansı sistemi User Agent blacklist bilgilerini merkezi sistemden düzenli olarak yenileyebilmelidir ve belli User Agent'leri whitelist olarak kaydedebilmeldir.

4.2.3.36. Güvenlik bilgi ve olay yönetim lisansı sistemi custom bloklu ip ve domain'leri CVS formatında import edebilmelidir.

4.2.3.37. Güvenlik bilgi ve olay yönetim lisansı sistemi istenilen network, sistem, storage, servis vb. elemanlarının dahil olduğu birçok servis grubu oluşturabilmeli ve grup olarak tüm elemanlarının performans, availability, event, CMDB vb. bilgilerini gösterebilmelidir.

4.2.3.38. Önerilen Güvenlik bilgi ve olay yönetim lisansı sistemi yeni cihaz ve log parser (log ayrıştırıcı) tanımlarını merkezi sistem üzerinden alarak onaylanması durumunda sisteme dahil edebilmelidir.

4.2.3.39. Önerilen Güvenlik bilgi ve olay yönetim lisansı sisteminde olmayan cihazlar için log ayrıştırıcı (log parser) yöntemi bilinen bir yazım sistemi (örneğin XML) ile yazılarak sisteme dahil edilebilmelidir.

4.2.3.40. Güvenlik bilgi ve olay yönetim lisansı sistemi el ile script aracılığı ile dahil edilen sistemler üzerinden belli komut çıktılarını da log ayrıştırıcı (log parser) gibi sistem log kayıtlarına dahile ederek belli durumlarda monitör edilebilmelidir.

4.2.3.41. Güvenlik bilgi ve olay yönetim lisansı sistemi belirli dosya, konfigrasyon veya dizinlerdeki değişikliklere karşı değişiklik takibi (integrity-check) yapabilmelidir. Oluşan değişiklikler monitör edilerek alarm oluşturulabilmelidir.

4.2.3.42. Güvenlik bilgi ve olay yönetim lisansı sistemi belli log kayıtlarını giriş esnasında hariç tutularak istenirse sadece kaydedilerek herhangi bir işleme tabi tutulmamalı veya giriş esnasında direk silinebilmeli. Bu silinen log kayıtları lisans EPS'den hariç tutulabilmelidir.

4.2.3.43. Güvenlik bilgi ve olay yönetim lisansı sistemi belirli cihazlardan gelen log kayıtlarını başka cihazlara yönlendirebilmelidir. (örneğin netflow veya snmp traps

4.2.3.44. Güvenlik bilgi ve olay yönetim sistemi bir syslog paketindeki çok satırlı syslog kayıtlarını ayrıştırabilmelidir.

4.2.3.45. 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.

4.2.3.46. Aşağıdaki uyumluluk süreçleri için hazır raporlar oluşturabilmelidir:

- PCI-DSS
- HIPAA
- SOX
- NERC
- FISMA
- ISO
- GLBA

- GPG13
- SANS Critical Controls

4.2.3.47. Takip amaçlı dashboard ekranlarına sahip olmalı slideshow görünümünde olabilmelidir

4.2.3.48. Dashboard görüntülemesi sırasında aşağıdaki tiplerde verinin görüntülenmesi desteklenmelidir.:

- Bar
- Pie
- Line
- Table
- Combination (line ve table view)
- Treemap
- Scatter graph
- Single values
- Gauges
- Geographical Map

4.2.3.49. Vaka oluşması durumunda script çalıştırma özelliği bulunmalıdır.

4.2.3.50. API bazlı entegrasyon ile CMDB ve olay bilgileri harci ticketing sistemleri ile entegre olabilmelidir. (serviceNow, ConnectWise vb.)

4.2.3.51. Dahili ticketing sistemi barındırmalıdır.

4.2.3.52. Anahtar kelime bazlı arama tüm log alanlarında veya istenilen bir alan dahilinde yapılabilmelidir.

4.2.3.53. Geçmişe yönelik arama yapılabilmesi desteklenmelidir.

4.2.3.54. Arama yapılırken boolean filtreler, gruplamalar, zaman bazlı filtreler, regex kullanımı desteklenmelidir.

4.2.3.55. İstatiksel profiller desteklenmelidir. Örneğin sistem network kullanımında olağan dışı bir artış olduğunu bu sayede anlayabilmeli ve alarm üretebilmelidir.

4.2.3.56. Zamanlanmış raporların oluşturulması desteklenmelidir. Bu raporlar CSV veya PDF formatında export edilip mail ile gönderilebilmelidir.

4.2.3.57. SIEM ürünü Web üzerinden GUI/https üzerinden yönetilebilmelidir.

4.2.3.58. Çözüm cihazlardan toplanan envanter, performans verisi, güvenlik ile log verisinin aynı ekrandan analiz edilmesini sağlayabilmelidir.

4.2.3.59. Multi-teanent (çok organizasyonlu) desteği olmalıdır. Bu sayede birbirinden bağımsız organizasyon konfigürasyonları ve bunlara erişen kullanıcı yetkilendirmeleri yapılabilmelidir.

4.2.3.60. Multi-teanent (çok organizasyonlu) yapılanmada belirli sistemler ip seviyesinde ilgili organizasyona atanabilmelidir.

4.2.3.61. Multi-teanent (çok organizasyonlu) yapılanmada

4.2.3.62. Rol temelli yönetim desteği olmalıdır, yönetici, standart kullanıcı, sadece görüntüleme özelliklerinin yanı sıra aşağıdaki şekilde roller oluşturulabilmelidir.

4.2.3.62.1. Sadece Network sistemlerinin kayıtlarını yönetebilme

4.2.3.62.2. Sadece Windows sistemlerinin kayıtlarını yönetebilme

4.2.3.62.3. Sadece Unix sistemlerinin kayıtlarını yönetebilme

4.2.3.62.4. Sadece Güvenlik sistemlerinin kayıtlarını yönetebilme

4.2.3.63. Kullanıcı kimlik doğrulaması local veya harici LDAP/Radius sisteminden yapılabilmelidir.

4.2.3.64. Güvenlik bilgi ve olay yönetim sistemi zamanı belirlenebilen düzenli rapor bilgileri mail veya scp ile gönderebilmelidir,

4.2.3.65. SI Güvenlik bilgi ve olay yönetim sistemi olay (incident) bilgilerini kendi üzerinde gösterebildiği gibi SNMP Trap (v1, v2c), XML https üzerinden harici sistemlere gönderebilmelidir.

4.2.3.66. Güvenlik bilgi ve olay yönetim sistemi olay (incident) bilgilerini otomatik çağrı açabilen sistemlere WSDL üzerinden göndererek acil müdahale edilmesini sağlayabilmelidir.

4.2.3.67. Güvenlik bilgi ve olay yönetim sistemi sistemi kendine dahil olan tünelleme uygun sistemlere gerektiğinde uzaktan tünel kurarak sisteme müdahale edebilmelidir. (ssh, wmi vb.)

4.2.3.68. Güvenlik bilgi ve olay yönetim sistemi sistemi raporlarında firma logosunun konulmasına izin vermelidir.

4.2.3.69. Güvenlik bilgi ve olay yönetim sistemi sistem kaynak kullanımları (memory, CPU, disk vb.) toplam ve process olarak da ayrıntılı şekilde gösterilmelidir. Aşırı artışlarda alarm oluşturulabilmelidir.

4.2.3.70. Güvenlik bilgi ve olay yönetim sistemi sistemi belli zaman aralıklarında kayıtları arşivleyebilmeli ve arşivlenmiş verileri görüntülenmek üzere geri yükleyebilmelidir.

4.2.3.71. Güvenlik bilgi ve olay yönetim sistemi sistemi herhangi bir tarihte oluşan herbir event'i bir checksum algoritması (örneğin sha256) üzerinden doğrulayabilmelidir.

5. GÜVENLİK DUVARI OLAY GÜNLÜĞÜ ANALİZ SİSTEMİ LİSANS YENİLEME

5.1. Mevcut bulunan güvenlik duvarı olay günlüğü analiz sistemi lisansı günlük 100 GB olay günlüğü toplamayı ve analiz etmeyi sağlayacak şekilde 3 yıl süre ile yenilenecektir.

5.2. Hotspot servisi sunabilen ve 5651 sayılı kanun ile uyumlu olarak olay günlüklerine kamu zaman damgası basabilen olay günlüğü toplama ve raporlama lisansı ücretsiz olarak ilave edilecektir. Söz konusu lisans aşağıdaki özellikleri sağlayacaktır.

5.2.1. Olay günlüğü toplama ve raporlama lisansı, MS Windows İşletim Sistemleri üzerinde çalışmalıdır. Desteklenen MS Windows İşletim Sistemleri belirtilmelidir. Olay günlüğü toplama ve raporlama lisansı Sanal sistemler (Vmware, Hyper-V, Xen) üzerinde çalıştırılmak isteniyorsa MS Windows İşletim Sistemi Sanal Sistem üzerinde kurulu olmalıdır.

5.2.2. Olay günlüğü toplama ve raporlama lisansının Log ve Disk kapasite sınırı olmamalıdır.

5.2.3. Olay günlüğü toplama ve raporlama lisansı, kurumda mevcut güvenlik duvarı tarafından gönderilen Log Kayıtları üzerinden istenen kriterlere göre filtreleme yapabilmeli ve kurumda mevcut güvenlik duvarı için en az 40 adet önceden tanımlanmış rapor üretebilmelidir.

5.2.4. Olay günlüğü toplama ve raporlama lisansı ile birden fazla kurumda mevcut güvenlik duvarına ait log'ları merkezi olarak tutabilmeli ve raporlama yapabilmelidir.

5.2.5. Olay günlüğü toplama ve raporlama lisansı; Trafik, Web, Uygulama, Email, Saldırı ve Olay gibi en az 6 farklı kategoride Rapor üretebilmelidir. Olay günlüğü toplama ve raporlama lisansı, pdf formatında rapor üretebilmelidir.

5.2.6. Olay günlüğü toplama ve raporlama lisansı, Log kayıtlarını ftp veya benzer bir protokolle harici bir Sunucu veya Depolama alanı üzerinde yedekleme yapıp arşivleyerek log yedekliliği sağlayabilmelidir. Olay günlüğü toplama ve raporlama lisansı, Hata ve olay durumlarında belirtilen e-posta adresine bilgi verebilmelidir.

5.2.7. Olay günlüğü toplama ve raporlama lisansı, 5651 sayılı kanunun uygulanmasına yönelik 'Internet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik' kapsamında, Log kayıtlarının

doğruluğunu ve bütünlüğünü kendi üzerinde sağlamalıdır. Log/Raporlama Sistemi, 5651 sayılı kanun kapsamında Logların yedeklenmesi ve imzalanması, toplanan logların filtrelenmesi ve raporlanması işlevlerini yerine getirmelidir.

5.2.8. Olay günlüğü toplama ve raporlama lisansı, 5651 sayılı kanunun uygulanmasına yönelik zaman damgası ve İmzalama için Kamu SM Entegrasyonu (Tübitak Kamu Sertifikasyon Merkezi) desteği sağlamalıdır. Kamu SM Zaman Damgası ve İmzalama hizmeti yazılımın içine gömülü olmalı bunun için ilave ücret ödenmemelidir. Olay günlüğü toplama ve raporlama lisansı , Log kayıtlarına herhangi bir Zaman sunucudan alınan Zaman bilgisi ile Zaman damgası vurma ve Self-Signed Sertifika ile imzalama imkanını da sağlamalıdır.

5.2.9. Olay günlüğü toplama ve raporlama lisansı , kurumda mevcut güvenlik duvarına belirli sıklıkta SSH (Secure Shell) üzerinden bağlanarak IP/MAC adresi eşleştirme tablosunu alıp bu bilginin geçmişe yönelik kayıtlarını tutabilmelidir.

5.2.10. Lisanslama modeli, log gönderecek belirli Seri No'lu Güvenlik sistemleri için lisanslama şeklinde olmalıdır. Kurumda mevcut güvenlik duvarının lisanslandığı süre boyunca Log/Raporlama sistemi bu sistemden log kabul edebilmelidir. Lisanslanan sürenin sona ermesinden sonra, eski döneme ait log kayıtları üzerinde filtreleme ve raporlama imkanı devam etmelidir.

5.2.11. Olay günlüğü toplama ve raporlama lisansı , Lisanslanan kurumda mevcut güvenlik duvarının konfigürasyon yedeklemesini istenen zamanlamaya göre SCP (Secure Copy Protocol) ile yapabilmeli ve bu konfigürasyon dosyaları şifreli bir veritabanı üzerinde tutulmalıdır.

5.2.12. Olay günlüğü toplama ve raporlama lisansı, Güvenlik cihazına API (Application Programming Interface) üzerinden bağlanarak Güvenlik cihazının sağlamış olduğu altyapı ile anlık Network/Oturum vs. bilgileri takibi yapabilmelidir.

5.2.13. Olay günlüğü toplama ve raporlama lisansı, Üzerinde tanımlı IP Kullanıcı Rehberi ile IP ve Kullanıcı adlarını eşleştirerek IP-Kullanıcı adı çözümlemesi yapabilmelidir. Olay günlüğü toplama ve raporlama lisansı, kurumda mevcut güvenlik duvarı üzerinden alınan Makina ismi veya LDAP protokolü ile sağlanan Kullanıcı adları ile IP-Kullanıcı adresi çözümlemesi yapabilmelidir.

5.2.14. Olay günlüğü toplama ve raporlama lisansı na Log gönderebilecek Seri No ile tanımlı Güvenlik Sistemleri, 3 yıl süre ile Log gönderebilecek şekilde lisanslanmalıdır.

5.2.15. Olay günlüğü toplama ve raporlama lisansı; Güvenlik cihazının firmware versiyonundan bağımsız şekilde ve log formatında yapılan değişikliklerden etkilenmeyerek Log kaydı yapabilmelidir.

5.2.16. Olay günlüğü toplama ve raporlama lisansı, kurumda mevcut güvenlik duvarı ve aynı marka ve yönetilebilir wireless AP ile tam entegre olarak çalışacak Hot Spot yazılım özelliklerini desteklemelidir.

5.2.17. Hot Spot yazılımı, WiFi kullanıcı erişiminde SMS Doğrulama, TCKN Doğrulama, SMS+TCKN Doğrulama , Captive Portal özelliklerini desteklemelidir. Ek olarak mekanda bulunmayı doğrulayan gizli kelime (2FA) özelliğini desteklemelidir.

5.2.18. SMS Doğrulamada, SMS sağlayıcı olarak NetGSM, Vatan SMS ve Posta Güvercini sistemlerinden en az birini desteklemelidir.

5.2.19. Hotspot kullanıcıların anlık durumu (trafik, süre, bağlılık durumu vb.) Hotspot ekranından takip edilebilmeli ve gerektiğinde kullanıcının kimlik denetimi iptal edilebilmelidir.

5.2.20. Beyaz ve Kara Liste desteklenmeli ve gerektiğinde canlı ortam üzerinde tek tıklamayla herhangi bir kimlik kara listeye eklenebilmelidir.

5.2.21. Hotspot çerçevesinde kullanıcıların trafikleri ilgili kimlikleriyle loglara yansıtılmalıdır.
5.2.22. Geriye dönük tarihlere gidilerek hotspot bağlanan kullanıcı listesine erişilebilmelidir.
5.2.23. Hotspot karşılama ekranında çıkacak mesajlar özelleştirilebilmelidir.
5.2.24. Hot Spot dökümantasyonuna yazılıma ait Portal' dan erişilebilmelidir.
5.2.25. Hotspot özelliği, kullanılan Entegre Log/Raporlama yazılım lisansına dahil olmalıdır. Ek bir lisans gerektirmemelidir.

6. İŞİN SÜRESİ VE HİZMET DETAYLARI

6.1. Yüklenici, teknik şartnamede tanımlanan tüm işleri ve hizmetleri 60 takvim günü içerisinde tamamlayacaktır. (Cihaz kurulumu ve çalışır halde teslimini kapsayacaktır.) Yüklenici iş planı hazırlayacak, idarenin onayına istinaden iş planına uygun olarak kurulumlar yapılacaktır.

6.2. Hizmet süresi boyunca İdare'nin ihtiyaç duyduğu ve talep ettiği her türlü kurulum ve yapılandırma, düşey ve dikey taşıma Yüklenici tarafından ücretsiz yapılacaktır. Tüm kurulumlar idare tarafından talep edilecek konfigürasyon özelliklerine göre kurulumlar yapılacak, kurulumların tamamlanmasına istinaden kontrolleri yapılacaktır.

6.3. Temin edilecek tüm ürünler, lisanslar "Kurum Adına" kaydedilecek ve lisanslanacaktır.

6.4. Üreticinin verdiği garanti süresi Teknik Şartnamede talep edilen garanti süresinden daha uzun olması durumunda üretici firma garanti süresi geçerli olacak ve Yüklenici bu garantiyi vermeyi taahhüt etmiş sayılacaktır. Garanti süresince, çağrı açma, parçalı bakım ve onarım hizmetleri işçilik dâhil olmak üzere, yerinde ve ücretsiz yapılacak ve destek hizmetleri Yüklenici tarafından bedelsiz olarak sağlanacaktır.

6.5. İdare tarafından aksi belirtilmedikçe, arızalara Madde-7 de belirtilen arıza kademeleri uyarınca müdahale edilecektir. Arızaya müdahale, İdare ve/veya Kurum tarafından Yüklenicinin talep ettiği sözlü veya yazılı (telefon, faks, e-mail, resmi yazı vb. gibi) iletişim kanallarından gerçekleştirilecektir. Yüklenici, ön incelemenin yapılması, çözüm yönteminin belirlenmesi ve sorun giderme zamanı ile ilgili bilgileri müdahale süresi içinde idareye bildirmelidir.

6.6. Arıza bildirim zamanı, İdare'nin Yükleniciye veya temsilcisine yazılı, sözlü (telefon vb.) veya mail bildirimde bulunduğu zamandır. Cihazların arızalarının çözümlenmesi, İdare ve Yüklenici arasında e-posta veya yazılı olarak arızaların giderildiğinin kayıt altına alınması ile tamamlanmış kabul edilecektir.

6.7. Hizmet süresince ortaya çıkabilecek tüm bakım ve onarım Yüklenici tarafından, belirtilen hizmet seviyeleri süreleri içerisinde yerine getirilecektir. Yüklenici, hizmet süresinde İdare tarafından hizmet kapsamında olmak üzere talep edilen hiçbir mal ve hizmet için her ne koşulda olursa olsun İdare'den ayrıca ücret talep etmeyecektir.

6.8. Hizmet süresi içinde doğabilecek her türlü arıza ve hasarlardan (kullanım hataları hariç) Yüklenici sorumlu olacaktır.

6.9. Arızanın çözüm süresi Yüklenicinin İdare'ye yazılı veya e-posta ile işin tamamlandığını bildirmesi veya İdare'ye isim-imza karşılığı teslim edeceği servis formunda belirtilen saat ile tespit edilir.

7. GARANTİ, BAKIM VE CEZAİ KOŞULLAR

7.1. Yüklenici garanti süresince çağrı açılacak tüm iletişim bilgilerini (Firma, İlgili Kişi, Telefon, e-Mail vb.) İdare' ye kabul dokümanlarında teslim edecektir.

7.2. Yeni Nesil Güvenlik Duvarı Lisansı, Güvenlik Duvarı Olay Günlüğü Analiz Sistemi Lisansı ve ücretsiz verilecek diğer lisanslar 3 (üç) yıl boyunca üretici garantisine sahip olacaktır.

7.3. İdare/Kurum tarafından bildirilen arızalar yüklenici tarafından kayıt altına alınmalı, istenildiğinde raporlanabilmelidir.

7.4. Yüklenici hizmet süresince yukarıda tanımlanan hizmetleri İdare'ye sağlayacak ve aşağıdaki tablolarda belirtilen müdahale ve çözüm sürelerine riayet edecektir.

Tablo 1 : Müdahale ve Çözüm Süreleri

GRUP	HİZMET PENCERESİ	MÜDAHALE SÜRESİ	ÇÖZÜM SÜRESİ
A	7x24	Azami 2 saat	Azami 8 saat
B	7x24	Azami 4 saat	Azami 48 saat
C	7x24	Azami 48 saat	Azami 240 saat
D	5x8	İdare ve Yüklenici tarafından ortaklaşa belirlenir	

Tablo 2 : Arıza ve Kesinti Grup Tanımları

GRUP	TANIM
A	**Ciddi Kesintiler** **Örnek:** • Söz konusu sistemin tamamen işlemez duruma gelmesi ya da bir uygulamanın tamamen durması. • Söz konusu sistemin önemli bir fonksiyonunun doğru çalışmaması. • Sistemin bazı fonksiyonlarının doğru çalışmaması ya da gereğinden fazla yavaşlaması.
B	**Majör İş Kesintileri- Kısmi Hizmet Kaybı** **Örnek:** • Tepki süresi ve yavaşlık problemleri • Sistem yönetim konsolundan sisteme ulaşılamaması • Sistemin çalışmasını etkileyen fakat sistemi durdurma noktasına getirmeyen arızalar.
C	**Minör İş Kesintileri- Bir grup kullanıcının etkilendiği durumlar** **Örnek:** • Sistemin çalışmasını etkilemeyen veya bakım sırasında ortaya çıkmış düzenleyici ve arıza önleyici tedbirler.
D	**İdare Tarafından Talep Edilen Teknik destek ve Ek İstekler**

8. GİZLİLİK VE SORUMLULUK

8.1. Hizmetin ifası sebebiyle bu işe ait ve işin yürütülmesi esnasında İdareye tanzim olunan her türlü belge, rapor, istatistik verisi, bilgisayar kayıtları ve sair materyalin, yazılım kodlarının ve verinin mülkiyeti ve bunlar üzerindeki yayma, çoğaltma, işleme ve umuma iletim şeklindeki her türlü fikri mülkiyet hakkı İdare'ye aittir. Yüklenici, bu bilgileri, istemesi halinde İdare'ye teslim edecek ve kendi kopyasını bir daha ulaşılamayacak şekilde imha edecektir. 3. Şahıslar/Firmalar ile paylaşamayacaktır.

8.2. Bu gizlilik yükümlülükleri, bu Yüklenici ile yapılacak sözleşmenin sona ermesi veya feshinden sonra da devam edecek ve geçerli olacaktır.

9. ÜRÜN LİSTESİ

S.N.	ÜRÜN AÇIKLAMASI	ADET
1	Yeni Nesil Güvenlik Duvarı Lisansı	2
2	Güvenlik Duvarı Olay Günlüğü Analiz Sistemi Lisansı	1

ERÜ SAĞLIK UYGULAMA VE ARAŞTIRMA MERKEZİ
Oktay KARASU
Sicil No: 40516

ERÜ SAĞLIK UYGULAMA VE ARAŞTIRMA MERKEZİ
Şerife ÜNAL OK
Donanım Birimi Sorumlusu
Sicil No: 41607

ERÜ SAĞLIK UYGULAMA VE ARAŞTIRMA MERKEZİ
Süleyman ÇERİ
Bilgi İşlem Koordinatörü
Sicil No: 41910