LOG YÖNETİM YAZILIMI VE HOTSPOT SATIN ALIM İHALESİ

1. LOG YÖNETİM YAZILIMI TEKNİK ŞARTNAMESİ

1.1. Genel

1.1.1. Ürün Güvenlik Duvarı, UTM, Web Sunucu, Mail Sunucu, Uygulama Sunucu, Aktif Dizin, LDAP, Ağ Cihazları (Switch, Router, Kablosuz, Erişim Noktası), İçerik Filtreleme, Veri Tabanları, İşletim Sistemleri, IPS, IDS, DHCP, VPN Sunucuları, Depolama Ürünleri, Ağ Vekili, Trade Platform, CRM Sistemleri kapsamındaki farklı log kaynaklarından kayıtları toplama yeteneğine sahip olmalıdır.

1.1.2. Ürün, teklif edilen hotspot yazılımı üzerinde log toplayabilmelidir.

1.1.3. Log Toplama işlemi için aşağıdaki yöntemlerin hepsini desteklemelidir:

- Ajan
- SYSLOG (TCP ve UDP)
- SSH, SCP, SFTP, SMB
- WMI
- OPSEC
- NativeSQL, ODBC, JDBC, OLEDB
- CIFS, SMBFS, SAMBA (Paylaşım)
- FTP
- NFS
- TCP SOCKET
- Snmp, Snmp Trap
- Flow (Netflow, Sflow, Jflow)
- Kafka

1.2. Ajan

1.2.1. Ajanlı toplamada kayıtların sistemine gidip gitmediği otomatik kontrol edilmeli, kayıt toplama sistemine bilgi veremediği ve bilgi alınmadığı durumda ise kayıtları bekleterek sorun giderildiğinde aktarmalıdır.

1.2.2. Ajanlı yöntemde, loglar merkeze gönderilirken sıkıştırma, şifreleme (SSL) özelliği olmalıdır.

1.2.3. Ajanlar merkezi olarak yönetilmelidir. Ajanlar merkezi noktadan gerekli yetkide kullanıcı hesapları ile kurulabilmelidir ve kaldırılabilmelidir. Ajanlar üzerinde log kaynakları uzaktan merkezi olarak tanımlanabilmeli, düzenlenebilmeli ve silinebilmelidir. Ajanın kendine ait log kayıtları da uzaktan izlenebilmelidir.

1.2.4. Ajan yönetim ve log gönderim bağlantı noktaları ayrı olmalıdır ve hangi porttan iletişim kurulacağı özelleştirilebilmelidir.

1.2.5. Ajanlar merkezi noktadan güncelleştirilebilmelidir. Güncelleme işlemi sadece seçilen ajanlar için yapılabilmelidir.

1.2.6. Ajanlar WMI, Veri Tabanı toplama yöntemlerinde ara toplayıcı olarak çalıştırılabilmelidir. Uzak sunuculardan (sunucu üzerine kurulmadan) WMI ve Veri Tabanı yöntemlerinde okuma/toplama yetkisinde kullanıcı ile verileri toplayıp merkezi noktaya iletebilmelidir.

1.2.7. Ajan Windows olay kimlik numarası (eventid) bazında filtre yapabilmeli, sadece istenen kayıtları göndermeli veya istenmeyen kayıtları göndermemelidir.

1.2.8. Ajan gün içinde oluşan kayıtları günün belirlenen saatleri arasında topluca göndermeye imkân sağlamalıdır.

1.2.9. Ajan kayıtları Apache Kafka adreslerine gönderebilmelidir.

1.3. İnkâr Edilemezlik

1.3.1. Kayıt ve dosya bazında değişmezlik garantisi, bütünlük ve doğruluk değerleri ile sağlanmalıdır. İnkâr edilemezlik altyapısı sayesinde veri manipülasyonuna izin verilmemelidir.

1.3.2. Bilgisayar kayıtları (logları) dosya sistemi üzerinde zaman damgası ve hash bilgileriyle birlikte dijital sertifika ile imzalanarak saklanmalıdır. Dijital imzalama işlemi dosya sistemine log yazılması esnasında yapılmalıdır. Loglar, imzalanmadan dosya sistemine yazılmamalıdır.

1.3.3. Anlık olarak alınan hash ve imzalar, geçmişe yönelik sorgular sonucunda veriler dışarı aktarılırken kontrol edilebilmelidir. Aktarma sırasındaki veri özetleri ile veri toplanırken alınan özetler karşılaştırılabilmelidir.

1.3.4. Ürün, 5651 sayılı yasanın gereksinimlerini karşılamalıdır. Üretici, yasanın ya da ilgili mevzuatların düzenleme ve değişikliklerine uyma garantisi vermelidir. Üretici firma, yasal güncellemenin yürürlüğe girmesinden itibaren üç (3) ay içerisinde teknik uyumluluk taahhüdü vermelidir.

1.3.5. Sistem, dosya sisteminde yazdığı dosyaları isteğe bağlı olarak döndüğünde (rotate) TÜBİTAK zaman damgası ile imzalayarak kapatmalıdır. Gün sonunda tüm dosya hashleri TÜBİTAK zaman damgası ile damgalanabilmelidir.

1.3.6. Ürün, imzalanmış olan verinin ve harici zaman damgasının doğruluk ve bütünlüğünü kontrol etmek amacıyla, bir bütünlük kontrol aracına sahip olmalıdır.

1.3.7. İnkâr edilemezlik raporları periyodik olarak çalıştırılabilmelidir. Bu sayede toplanan veriler üzerinde değişiklik yapılıp yapılmadığı kontrolleri sağlanabilmelidir.

1.3.8. Ürün, kayıtları işleme sırasında dosya sistemine yazarken satır bazında şifreleme özelliği olmalıdır. Şifreleme seçeneği sadece istenen log kaynağı için aktif edilebilmelidir. Bu kayıtlar sadece arabirim üzerinden görüntülenebilmelidir.

1.3.9. Ürün dosya bütünlüğü izleme özelliğine sahip olmalıdır. Bir dizin altındaki dosyaların, dijital imzaları belirli periyotlar oluşturularak, dosya değişiklikleri kontrol edilebilmelidir. Dizin altındaki alt dizinler de bu kontrole dahil edilebilmelidir.

1.4. Log İşleme ve Ayrıştırma

1.4.1. Ürün toplanan logları ayrıştırarak tanıma özelliğine sahip olmalıdır. Ayrıştırma işlemini yapan eklentiler; Düzenli ifadeler (Regex - Regular Expressions), Ayraç (Delimiter), Statik, Code (C#, VB), SQL yapılarını desteklemelidir. Bu ayrıştırma yöntemlerinin geliştirebileceği bir ortam, araç ya da modül ürün içerisinde sunulmalıdır.

1.4.2. Ön tanımlı ve geliştirilen eklentiler, ayrıştırma işlemleri sırasında farklı sayıda ve tipte deyimlere izin vermelidir.

1.4.3. Eklentiler üzerinde normalizasyon alanları olmalı, loglar üzerinde işlenen alanlar istenilen değer ile değiştirilebilmeli ve normalize edilebilmelidir. Statik ve Dinamik Listeler ile ayrıştırılan alanlar zenginleştirilebilmelidir.

1.4.4. En az 500 farklı log tipi (eklenti) için log tanıma bileşeni olmalıdır.

1.4.5. Üretici, ürünün desteklediği sistemler arasında olmayan bir kaynak olması durumunda **1.1.3** numaralı maddede belirtilen yöntemlerden birini destekleyen log kaynakları için eklenti ve ayrıştırıcı geliştirmeyi taahhüt etmelidir. Ön tanımlı olarak algılayamadığı loglar için gerekli eklentiler yazılarak sisteme tanıtılabilmelidir.

1.4.6. Loglar Kafka üzerinden okunabilmelidir.

1.4.7. Loglar HDFS üzerine yazılabilmeli, arama ve rapor işlemleri HDFS üzerindeki kayıtlardan yapılabilmelidir.

1.4.8. Log kaynağı bazında okuma ve yazma aralıkları belirlenebilmelidir.

1.4.9. Ürün kayıtların ham halini saklayabilmelidir.

1.5. Veri Sınıflandırma

1.5.1. Toplanan verileri sınıflandırma ile benzer olayları bir grup/tür altında gösterebilmelidir. Olay tipleri hızlıca ortak değerlere göre sınıflandırılmalı ve tamamen farklı kaynaklardan gelen bilgilerle ilişkilendirme yapılabilmelidir. (Örn: Farklı üreticilerin saldırı tespit sistemlerinden ve güvenlik duvarlarından gelecek olan port taraması, tek bir port taraması olarak değerlendirilip, sınıflandırılacaktır.)

1.5.2. Sınıflandırılmayan kayıtlar için sınıflandırma şartları girilebilmelidir. Sınıflandırma ağacı özelleştirilebilmelidir.

1.5.3. Loglar sınıflandırma sisteminde Bilgi, Düşük, Orta, Yüksek, Kritik seviyelerinde derecelendirilmelidir.

1.6. Kullanıcı Hakları, Erişim Yönetimi ve Denetim Mekanizması

1.6.1. Sistem, çoklu kullanıcı ve yetkilendirme desteğine sahip olmalıdır. Log kaynağı grupları, Log kaynağı ve Eklentilere göre, görme ve değiştirme yetkisi/rolleri tanımlanabilmelidir.

1.6.2. Sistem yerel kullanıcı oluşturulmasına ve bu kullanıcılara rol atanmasına izin vermelidir.

1.6.3. Ürün üzerinde AD (Active Directory-Aktif Dizin), LDAP, RADIUS sistemler ile entegrasyon sağlayarak, harici doğrulama ve yetkilendirme yapılabilmelidir. Harici yetkilendirme sistemlerinden gelen kullanıcılara ön tanımlı rol atanabilmelidir ve bu roller süper kullanıcı tarafından düzenlenebilmelidir.

1.6.4. Ürün üzerinde tanımlanan kullanıcılara parola politikaları uygulanabilmelidir. Parola politikaları, içerdiği karakter sayısı, içerdiği karakter tipi (Büyük harf, küçük harf, rakam, özel karakterler), parola değiştirme periyodu, eski paroladan tekrar kullanılmaması özelinde özelleştirilebilmelidir. Parola denemelerine karşı Captcha ile koruma sağlayabilmelidir.

1.6.5. Sistem üzerinde yapılan aktivitelerin hepsi kayıt altına alınmalıdır. Yetkilendirme ve giriş işlemleri, Yapılandırma değişiklikleri, İşletim sistemi seviyesinde yapılan aktiviteler kayıt altına alınabilmelidir.

1.6.6. Ürün'e bağlantı yapacak bağlantı noktalarında IP bazlı erişim kısıtlaması yapılabilmelidir.

1.7. Sıkıştırma, Arşivleme, Yedekleme

1.7.1. Sıkıştırılmış kayıtlar üzerinden herhangi bir işlem yapmadan sorgulama yapılabilmelidir.

1.7.2. Otomatik arşiv özelliği olmalıdır. Örn: 6 aydan eski loglar otomatik olarak arşivlenmelidir. Arşivleme log grubu, türü ya da kaynak bazında özelleştirilebilmelidir. Arşivleme işleminde sıkıştırma yapılmalı ve konfigürasyonlar arşivlenmelidir.

1.7.3. Otomatik yedekleme özelliği olmalıdır. Örn: 6 aydan eski loglar otomatik olarak yedeklenmelidir. Yedekleme log grubu, türü ya da kaynak bazında özelleştirilebilmelidir. Yedekleme işleminde sıkıştırma yapılmalı ve konfigürasyonlar yedeklenmelidir. Ayrıca belirlenen periyotlarda ve sıklıkta yedekleme yapma özelliği olmalıdır (Aylık, haftalık, günlük vb.)

1.7.4. Ürün, disk doluluk oranının belirlenen eşik değerini geçmesi durumunda eski verileri silme özelliğini desteklemelidir.

1.8. Yönetim Arayüzü

1.8.1. Ürün hem web tabanlı arabirim hem de Windows masaüstü uygulama tarafından yönetilebilmelidir.

1.8.2. Yönetim arayüzleri, GUI (Graphical User Interface) şifreli trafik SSL (HTTPS) desteklemelidir.

1.8.3. Tüm analiz işlemleri GUI üzerinden yapılabilmelidir.

1.8.4. GUI bir gösterge paneline (dashboard) sahip olmalıdır. Log yönetim sunucusunun çalışma durumu, diskteki boş alan durumu, kaynak tüketim değerleri gibi sistemin çalışmasını etkileyebilecek parametrelerin takip edildiği bir bölüm, panel üzerinde bulunmalıdır.

1.8.5. Yönetim arayüzünde, toplanan kayıtların sayıları, log kaynağı ve tarih bazında gösterilebilmelidir.

1.8.6. Saniye başına işlenen kayıt sayısı göstergeler üzerinden izlenebilmelidir.

1.8.7. Genel olarak logların aylık, haftalık veya günlük olarak dağılımı grafiksel olarak izlenebilmeli, anlık kayıt izleme grafiği olmalıdır.

1.8.8. Yönetim arayüzünde istenildiği kadar özel göstergeler tanımlanabilmeli ve bu göstergeler arasında istenilen zaman aralığında otomatik olarak geçiş yapılabilmelidir.

1.8.9. Ürün log kaynağı bazında disk kullanımını gösterebilmelidir.

1.8.10. Arayüz üzerinden sınıflandırma istatistikleri görülebilmelidir.

1.8.11. Arayüz üzerinden indekslenen alanlar ve sınıflandırma verisi kullanılarak kolon bazlı analitik yapılabilmelidir.

1.9. Uyarı ve Alarmlar

1.9.1. Ürün bildirimleri e-posta veya SMS yolu ile uyarıları iletebilmelidir.

1.9.2. E-posta iletimi için SMTP ayarları özelleştirilebilmelidir. Harici e-posta sunucuları kullanılmalıdır.

1.9.3. Belirli bir log kaynağından özelleştirilebilen bir süre boyunca log gelmediği zaman uyarı gönderilebilmelidir.

1.9.4. Ürün log verilerinin ilişkilendirmeden bir kayıt içerisinde geçen değere göre uyarı gönderebilmelidir.

1.9.5. Ürün günlük olarak çalışma özet mailini gönderme yeteneğine sahip olmalıdır.

1.9.6. Sistem kendi çalışma mekanizması ile ilgili durum değişiklikleri, hataları kayıt altına alabilmeli ve bu durumları uyarı olarak gönderebilmelidir.

1.10. Sorgulama, Raporlama ve Analitik

1.10.1. Sistemde toplanan loglar belirli bir zaman aralığına ve parametrelere göre arayüz üzerinden sorgulanabilmelidir.

1.10.2. Analiz ve sorgulama modülü olmalıdır. Loglar üzerinde istenilen sorgular ayrıştırılan veya orijinal log satırı üzerinde yapılabilmelidir. İstenildiği kadar filtre verilebilmelidir. Filtrelerde şu operatörler olmalıdır:

- Eşit (=)
- Eşit değil (!=)
- Metin içinde ara
- Liste
- Listede olmayanlar
- Başlıyorsa
- Başlamıyorsa
- Bitiyorsa
- Bitmiyorsa
- Küçük (<)
- Büyük (>)
- Büyük eşit (>=)
- Küçük eşit (<=)
- RegEx
- Kod Tablosunda Varsa
- Kod Tablosunda Yoksa
- Kara listede varsa
- Kara listede yoksa
- Ağ modelinde varsa
- Ağ modelinde yoksa

1.10.3. Analiz modülü ile yapılan sorgular kaydedilebilmelidir ve daha sonraki sorgularda tekrar kullanılabilmelidir.

1.10.4. Arama sonuçları pdf, xls, csv, html, mht, xlsx, doc, docx, rtf formatında dışarı aktarılabilmelidir.

1.10.5. Yasal sorgulamalar için logları ve dijital imzalarını dışarı aktaracak bir arabirim olmalıdır.

1.10.6. İstatistiksel analizler yapmak için eklentiler üzerinde ayrıştırılan her alan için istatistik sayaçları tanımlanabilmelidir. Bu işlem log ayrıştırma sırasında yapılmalıdır.

1.10.7. Loglar üzerinde ayrıştırılan alanlar üzerinden istatistiki analizler yapılabilmelidir. Sistem anlık (ad-hoc) sorgu yapılabilecek bir arayüz sağlamalıdır. Örn: Verilen tarih aralığında güvenlik duvarında en çok engellenen kaynak IP adresleri

1.10.8. Anlık istatistikler ham veri ya da indekslenmiş veri üzerinden oluşturulabilmelidir.

1.10.9. Raporlar istenilen zamanlarda planlı olarak üretilebilecek (scheduled reports) ve istenilen kişilere e-posta ile gönderilebilecektir.

1.10.10. Rapor şablonu oluşturma esnasında sihirbaz ile özelleştirilebilmelidir. Rapor adları, grafik türleri, rapor kapağı, sayfa boyutu ve yönü düzenlenebilmelidir.

1.10.11. PCI/DSS, HIPAA, GPDR, SOX, FISMA/NIST, ISO/IEC gibi uyumluluk raporlarını hazır olarak sunmalıdır.

1.10.12. Raporlar dijital sertifika ile saklanabilmelidir.

1.10.13. Raporlamada statik ve dinamik listeler kullanılabilmelidir.

1.10.14. Kod yazarak (C# dili ile) rapor hazırlanabilmesine imkân sağlamalıdır.

1.11. İndeksleme

1.11.1. Sistem, toplanan logları indeksleyebilmelidir. Her bir log kaynağında ayrıştırılan alanlar üzerinde istenildiği kadar indeks tanımlanabilmelidir. (Örn: Güvenlik Duvarı kayıtlarında kaynak IP ve hedef IP'ye göre, Windows Güvenlik kayıtlarında kullanıcı adı, İş İstasyonu adı, Kaynak IP, Süreç (Process) Adı'na göre indekslenebilmelidir).

1.11.2. İndeksler log kaynağı bazında özelleştirilebilmelidir.

1.11.3. Sorgular ve istatistiksel raporlar alınırken indeksli alanlar varsa sistem sorguları indeks kullanarak getirmelidir.

1.11.4. Ürün indeksleme motoru olarak Lucene ve Elastic altyapılarını desteklemelidir. Kullanıcı kendi istediği indeks motorunu ürün arayüzünden seçebilmelidir.

1.11.5. Ürün, indekslerin günlük olarak oluşturulmasına izin verilecektir. Bu özellik arayüz üzerinden seçilebilmelidir.

1.11.6. Tam metin arama özelliği sayesinde tüm indekslenmiş kayıtlar içinden arama yapabilmelidir. Tam metin (fulltext) indeksleme, seçilebilir özellik olmalıdır.

1.12. Mimari

1.12.1. Ölçeklenebilirlik açısından ürünün log işleme, arama motoru, imzalama birimi, indeksleme, raporlama modülü ve yönetim sistemi bileşenleri ayrıştırılabilmelidir ve/veya farklı sunuculara kurulabilmelidir.

1.12.2. Ürün çapraz platform desteklemelidir. Hem Linux Sunucu hem Windows Sunucu işletim sistemleri üzerinde koşabilmelidir.

DİĞER HUSUSLAR

1.1. Genel

1.1.1. Ürünün lisanslama modeli EPS (Event Per Second) üzerine olmalıdır. Topladığı kayıtlar üzerinden işleme sırasında EPS lisans kontrolü yapılmalıdır. Çözüm 5000 EPS log toplamayı ve işlemeyi destekleyecek ve bu sayı üzerinden tekliflendirilecektir.

1.1.2. EPS aşılması durumunda log toplamaya devam edebilmelidir.

1.1.3. Ürün genişlemeye uygun mimaride olacaktır. Veri kaynakları çoğaldıkça veya EPS (Events Per Second) sayısı arttığı taktirde yedekli ve güç dengeleyici mimariyi desteklemelidir.

1.1.4. Log Yönetim sistemi hem Linux hem de Windows üzerinde çalışmayı destekleyecektir. Kurum istediği versiyonu seçebilecektir.

1.1.5. Sistem, yazılım olarak da teklif edilebilecektir.

1.1.6. Garanti süresi boyunca yeni log alınması istenen sistemler için pluginler ücretsiz geliştirilecektir.
1.1.7. Ürün, tutulan logları kanun gereği 2 (iki) seneden az olmamak üzere saklayabilmelidir.
1.1.8. Ürün lisansı sınırsız kaynaktan kayıt toplanmasını desteklemelidir.
1.1.9. Teklif edilecek olan çözüm, ayrı bir işletim sistemi ve veri tabanı lisansı gerektirmemelidir.
1.1.10. Teklif edilecek ürün, tüm erişimlerin kayıtlarını performans engeli olmadan tutabilecek kapasitede olacaktır.
1.1.11. Üretici firma destek paketi devam ettiği müddetçe limitsiz eklenti (parser/plugin) yazma desteği verecektir. Loglarının işlenmesi istenen yeni sistemler için hazırda eklenti yoksa üretici firmaya örnek loglar gönderilecek, üretici firma bu loglar için eklentilerini ücretsiz geliştirecektir.
1.2. Teklif veren firmanın, teklif edeceği ürün ile Ticaret Üniversitesi projesi ölçeğinde en az 3 (üç) Üniversite veya benzeri büyüklükte kuruluş ile iş deneyimine sahip olması gerekmektedir. Firmalar söz konusu projeler ile ilgili iş deneyim belgelerini teklif ile birlikte ibraz etmelidir.
1.3. Firma tarafından verilen teklif kurulum ve teslim dahil olmalıdır.
1.4. Teklife, sınırsız telefon-mail ve en az 3 uzaktan destek – 5X8 - ürün desteği dahil olmalıdır.
1.5. Firma tarafından, teklif edeceği program ile ilgili Ticaret Üniversitesi Bilgi teknolojileri birimi personellerinden seçilmiş olan 2 kişiye yetkin kişilerce eğitim vermelidir.
1.6. Ürünlerin teslim süresi, sipariş tarihinden itibaren en fazla 2 haftadır.

2. HOTSPOT UYGULAMASI TEKNİK ŞARTNAMESİ

2.1. İnternet çıkışında kablolu veya kablosuz ağın önünde çalışacak ve internet çıkışında kullanıcılardan "username password" ile giriş imkânı sağlamalıdır.
2.2. Uygulama "username", "password" bilgisinin talep edilmesini sağlayacak bir ara birime ve değiştirilebilir bir form yapısına sahip olmalıdır.
2.3. HotSpot uygulaması "username, password" bilgisini kendi üzerindeki, ağda veya uzak lokasyonda kurulu olan bir Radius ve veritabanı uygulamasından alabilmelidir.
2.4. HotSpot uygulaması DHCP sunucusu gibi davranabilmelidir.
2.5. MAC adreslerine göre yetkilendirme sağlanabilmelidir.
2.6. DHCP üzerinde verilen IP adresleri MAC adresi bazında sabitlenebilmelidir, havuz listelenebilmeli ve IP adresleri bıraktırılabilmelidir.
2.7. Uzak lokasyonlardan gelen "Layer-3" trafik için de IP bazlı oturumlar sağlanarak, merkezi noktada kullanıcı yetkilendirmeleri yapılabilmelidir.
2.8. KVKK ve ETK'ya uygun olarak elektronik ileti izni yönetimine ve altyapısına sahip olmalıdır.
2.9. Active Directory/Open LDAP entegrasyonu sağlanabilmelidir.
2.10. Active Directory ile giriş yapan kullanıcılar bulunduğu grup veya OU'ya göre farklı bant genişliğinde internete erişebilmelidir.
2.11. Kullanıcı girişinde gerek yalnız gerekse SMS gönderimiyle beraber, T.C. kimlik bilgileriyle doğrulama yapılabilmelidir.
2.12. "Username, password" gibi giriş bilgileri doğrudan cep telefonuna mesaj olarak alınabilmelidir.
2.13. Kullanıcılar ön tanımlı şablonlara göre oluşturulabilmelidir.
2.14. Kullanıcıların internet çıkışı zaman bazlı kısıtlanabilmelidir.
2.15. Kullanıcıların internet çıkışı bant genişliğine göre kısıtlanabilmelidir.
2.16. Kullanıcıların internet çıkışı kullanım miktarına (kotaya) göre kısıtlanabilmelidir.
2.17. Giriş yapan kullanıcılar için farklı ağlara erişimleriyle ilgili izinler ve kısıtlamalar yapılabilmelidir.
2.18. "Upstream HTTP Proxy" tanımlanabilmelidir.
2.19. Yönetim arayüzüne erişimler kısıtlanabilmeli, arayüz girişinde AD/LDAP/Radius gibi dış kaynaklar entegre edilebilmeli, rol tabanlı yönetici yetkilendirmesi sağlanarak, sadece HotSpot kullanıcı işlemlerini yapabilecek kullanıcılar gibi farklı yöneticiler tanımlanabilmelidir.
2.20. 5651 No.lu yasa kapsamında HotSpot uygulaması IP erişim bilgilerini ve URL kayıtlarını tutabilmelidir.
2.21. API desteği olan SMS sağlayıcıları ile entegrasyon, üretici firma tarafından garanti edilmelidir.
2.22. Paylaşımlı ortak şifre ile kullanıcı doğrulama imkânı verilmelidir.
2.23. Facebook, Twitter ve Google ile kullanıcı doğrulama imkânı verilmelidir, ayrıca desteği olan diğer sosyal ağlar ile entegrasyon talep edilmesi durumunda, üretici firma tarafından sağlanabilmelidir.
2.24. HTTP API'leri ile SMS gönderimlerinde, proxy tanımlanabilmelidir.
2.25. HotSpot Web arabirimi ve kullanıcı karşılama sayfası HTTPS üzerinden hizmet verebilmeli, ilgili kurum kendi domaini ve sertifikasını kullanabilmelidir.
2.26. 802.1Q VLAN desteği bulunmalıdır.

2.27. Kullanıcı şifre yazdırma penceresi bulunmalı ve özelleştirilebilir olmalıdır.

2.28. Karşılama sayfası İngilizce, Rusça, Arapça, Türkçe, Almanca, İtalyanca, İspanyolca, Fransızca dillerinde tarayıcının desteğini otomatik algılayarak açılabilmeli ve dil seçenekleri kullanıcıya da sunulabilmelidir.

2.29. HotSpot kullanıcı yönetimlerini (kullanıcı ekleme/silme, bağlantı sağlama/sonlandırma) üçüncü taraf uygulamaların sağlayabilmesi için API sunulmalıdır.

2.30. Karşılama arayüzünden kullanıcıların girdiği değerler beyaz ve kara listelerde belirlenerek engellenebilmelidir.

2.31. Kullanıcı hatırlama özelliği sunularak, daha önceden giriş yapmış ve tekrar gelen kullanıcının otomatik giriş yaptırılması sağlanabilmelidir.

2.32. Belirlenen kaynak IP/networkler için karşılama arayüzü getirmeden otomatik izin verdirilebilmelidir.

2.33. Bilet yetkilendirmesi ile giriş yapabilme imkânı verilmelidir. Üretilen bilet kodlarının kaç kere kullanılabileceği, farklı kullanıcılarla kullanılıp kullanılamayacağı seçilebilmelidir.

2.34. T.C. yabancı uyruklu kimlik numaraları ile doğrulama yapılabilmelidir.

2.35. Karşılama ekranında SMS gönderiminde kabul edilebilecek telefon numaralarını kısıtlamak için format belirlenebilmelidir. (Türkiye, yurt dışı numaraları gibi)

2.36. SMS gönderiminde numara desenlerine göre farklı SMS sağlayıcılarının kullanılması politikaları belirlenebilmelidir.

2.37. Kullanıcıların telefon numarası olsun veya olmasın onay mekanizması olmaksızın da kendi kaydolup aynı şifreyle giriş yapabilmeleri sağlanabilmelidir.

2.38. Sadece SMS alarak değil, maliyetsiz bir şekilde arama yaparak ve SMS göndererek de yetkilendirme seçenekleri sunulabilmelidir.

2.39. Tek karşılama ekranında istenilen sayıda giriş seçeneği bulunabilmeli herhangi bir kısıtlama olmamalıdır.

2.40. Karşılama ekranında kullanıcılara anket sunulabilmeli, anket sonuçları yönetici arayüzünde rapor ekranında gösterilebilmelidir.

2.41. Karşılama ekranında video veya imaj şeklinde reklam gösterilebilmelidir.

2.42. Kullanıcılara opsiyonel olarak veri paylaşım izni sözleşmesi gösterilebilmeli, izin veren kullanıcılar filtrelenerek gösterilebilmelidir.

2.43. URL filtreleme yapılabilmeli, kategorize edilmiş hazır adres listeleri kullanılabilmeli, özel listeler de tanımlanarak kurallar oluşturulabilmelidir.

2.44. İnternete erişen kullanıcılar arayüzden izlenebilmeli ve bağlantısı sonlandırılabilmelidir.

2.45. Sistem konfigürasyon ve veri yedekleri oluşturulabilmeli, şifreli olarak dışarı alınabilmeli ve geri yüklenebilmelidir.

2.46. Hotspot uygulaması aynı anda en az 250 kullanıcıyı destekleyecek şekilde donanım veya yazılım lisansı ile birlikte verilmelidir.

2.47. Bilgisayar kayıtları (logları) dosya sistemi üzerinde anlık zaman damgası ve hash ile birlikte imzalanarak tutulmalıdır.

2.48. Sistemde farklı kaynaklardan toplanan loglar belirli bir zaman aralığına ve parametrelere göre arayüz üzerinden sorgulanabilmelidir.

2.49. Ön tanımlı olarak algılayamadığı loglar için gerekli pluginler yazılarak siteme tanıtılabilmelidir.

2.50. Çoklu kullanıcı ve yetkilendirme desteği olmalıdır. Varlıklara veya topladığı log tipine göre erişim yetkisi tanımlanabilmelidir.

2.51. Uzaktan log toplayan bileşenlerin konfigürasyon dosyası değiştirilerek text formatındaki herhangi bir logunda log sunucusuna gönderilebilir olması gerekmektedir.

2.52. İmzalanmış olan verinin bütünlüğünü kontrol etmek amacıyla çözüm bir bütünlük kontrol aracına sahip olmalıdır.

2.53. Sistemde yer alan loglar ile ilgili istatistiki bilgi sistemden grafik olarak görülebilmelidir. İlgili tüm analiz işlemleri GUI üzerinden yapılabilmelidir.

2.54. GUI bir gösterge paneline (dashboard) sahip olmalıdır. Log yönetim sunucusunun çalışma durumu, diskteki boş alan durumu gibi sistemin çalışmasını etkileyebilecek parametrelerin takip edildiği bir bölüm panel üzerinde yer alabilmelidir. GUI arabirimi müşteri ihtiyacına göre özelleştirilebilmelidir.

2.55. Ürün üzerinde alınan raporlar PDF, XSL, WORD gibi formatlarda dışları aktarılabilmelidir.

2.56. Ürün 5651 No.lu yasa gereği trafik bilgisi olarak kaynak IP adresi, hedef IP adresi, bağlantı tarih-saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları), kaynak ve hedef bilgisayar için MAC adres bilgisi verebilmelidir.

2.57. Ürün, trafik bilgilerinin doğruluğunu, bütünlüğünü oluşan verilerin doğruluk değerlerini (hash) zaman damgasıyla birlikte muhafaza etmek ve bütünlüğünü temin etmeyi sağlamalıdır.

2.58. Ağ trafik bilgilerinde; kullanıcı adı, kaynak ve hedef IP adresi, portu veya kullanılan protokol, zaman gibi kriterlere göre sorgulama yapılabilmelidir.

2.59. Teklif veren firmanın, teklif edeceği ürün ile Ticaret Üniversitesi projesi ölçeğinde en az 3 (üç) Üniversite veya benzeri büyüklükte kuruluş ile iş deneyimine sahip olması gerekmektedir. Firmalar söz konusu projeler ile ilgili iş deneyim belgelerini teklif ile birlikte ibraz etmelidir.

2.60. Firma tarafından verilen teklif kurulum ve teslim dahil olmalıdır.

2.61. Teklife, sınırsız telefon-mail ve en az 3 uzaktan destek – 5X8 - ürün desteği dahil olmalıdır.

2.62. Firma tarafından, teklif edeceği program ile ilgili Ticaret Üniversitesi Bilgi teknolojileri birimi personellerinden seçilmiş olan 2 kişiye yetkin kişilerce eğitim vermelidir.

2.63. Ürünlerin teslim süresi, sipariş tarihinden itibaren en fazla 2 haftadır.