T.C.
ANADOLU ÜNİVERSİTESİ
AÇIKÖĞRETİM FAKÜLTESİ
Piyasa Fiyat Araştırma Mektubu

Sayı: 97653057/68
Konu: Piyasa Fiyat Araştırma

Tarih: 16/05/2025

Sayın : .....

Kurumumuzun ihtiyacı olan aşağıda cins ve miktarı yazılı 1 kalem malzemeye ve/veya hizmete ilişkin fiyatınızı en geç 20/05/2025 tarih ve saat 12:00'e kadar teslim müddeti ile mal kalitesi açıklanmak suretiyle silinti, kazıntı ve karalama yapılmadan hazırlanarak adresimize elden teslim etmenizi, E-posta veya faks göndermenizi rica ederim.

Sertaç BETGÜ
Şef

SIRA NO	MALZEME CİNSİ	MİKTAR	BİRİM	B.FİYAT	TUTAR	MLZ. TESLİM TARİHİ
1	Antivirüs Yazılımı Lisans Yenilenmesi 3 Yıl 100 (Yüz) Kullanıcı	1	Adet			
	TEKNİK ŞARTNAMELERİ EKTEDİR.(TEKNİK ŞARTNAMENİN KAŞELENİP İMZALANARAK GERİ GÖNDERİLMESİ GEREKMEKTEDİR)					

MALZEME İSTEK BİRİMİ:	AÇIKÖĞRETİM FAKÜLTESİ DEKANLIĞI
MALZEME TESLİM YERİ:	A.Ü. Taşınır İşlemleri Şube Müdürlüğü Yunusemre Kampüsü ESKİŞEHİR - 0222 335 05 80 / 1780

Yukarıda cins ve miktarı yazılı malzemeleri ve/veya hizmeti hizalarında belirtilen fiyatlarla vermeyi beyan ediyorum.

AÇIKLAMA

Firma Adı/ Kaşe/ İmza

1- Fiyatlar KDV hariç TL (Türk Lirası olarak belirtilecektir. (Örn:0,00))
2- Alternatif Fiyat Mektubu Değerlendirmeye Alınmayacaktır.
3- Malzeme Teslim Tarihi Önemle Belirtilecektir.
4- Malzemelerin Nakliye Bedeli Firmanıza Aittir.
5- Kargo ile mal gönderilmemesi esastır. Gönderilmesi halinde sorumluluk firmaya aittir.
6- Firmalar malı göndermeden önce Malzeme Muayene Kabul ve Teslim Alma Merkezine bildirimde bulunması ve kabulde firma yetkilisinin bulunması yasa gereğidir.
7- Teklif edilen ürünlere ait varsa TSE marka ve ISO kalite güvence belgeleri teklif ile birlikte sunulmalıdır.
8- Bilgi için telefon numarası: 0 222 335 05 80 / 1084-85 Faks:0 222 330 46 26
9- Adres: A.Ü. AÇIKÖĞRETİM FAKÜLTESİ YUNUSEMRE KAMPÜSÜ 26470 TEPEBAŞI ESKİŞEHİR
10- E-Posta: donersatinalma@anadolu.edu.tr Web: anadolu.edu.tr
Yazılı olan mail adresine cevap veriniz. Bu mail adresi dışındaki adreslere gönderilen teklifleriniz dikkate alınmayacaktır.
11- Üniversitemiz ile ilgili satınalma duyurularımıza [https://www.anadolu.edu.tr/satin-alma-duyurular] adresinden ulaşabilirsiniz.

TEKNİK ŞARTNAME

Anadolu Üniversitesi Açıköğretim Fakültesi Öğrenme Teknolojileri ARGE Birimi içerisinde, Anadolu Üniversitesi personeli ve Açıköğretim Fakültesi öğrencisi odaklı üretilen dijital malzemelerin paylaşımında ve depolanmasında kullanılan Microsoft Windows ve Mac OSx işletim sistemine sahip bilgisayarlarda ve sunucu bilgisayarlarında kullanılan antivirüs yazılımının lisans yenilemesine ihtiyaç duyulmaktadır.

1. **Antivirüs Merkezi Yönetim Yazılımı**
2. **Kullanıcılarda ve Sunucularda Çalışacak Koruma Modülü**

1. Antivirüs Merkezi Yönetim Yazılımı

1.1. Lisans yenilemesi yapılacak antivirüs yazılımı; bilgisayarları, sunucuları ve mobil cihazları uzaktan yönetebilecek merkezi yönetim konsoluna sahip olmalıdır.

1.2. Merkezi yönetim yazılımı, aşağıda detayları belirtilen tüm özellikleri Türkçe dil desteği bulunan tek bir Web ara yüzü üzerinden yapabilmelidir.

1.3. Merkezi yönetim konsolu ve modülleri Windows ve Linux işletim sistemlerine veya Bulut sistemi desteği ile yönetilebilir olmalıdır.

1.4. Merkezi yönetim yazılımı Microsoft Azure Marketplace üzerinde ürün olarak bulunmalıdır.

1.5. Merkezi Yönetim Yazılımı aşağıdaki işletim sistemlerine kurulabilmelidir.

1.5.1. Windows Server 2003 SP2 ve R2
1.5.2. Windows Server 2008 SP2, R2 SP1 ve Core
1.5.3. Windows Server 2012, R2 ve 2016 ve üzeri
1.5.4. Windows 7 SP1, Windows 8 ve 8.1, Windows 10 ve üzeri
1.5.5. Ubuntu 12.04, 14.04, 16.04
1.5.6. RHEL ve CENTOS 5, 6, 7
1.5.7. SLED ve SLES 11, 12
1.5.8. OpenSuse 13
1.5.9. Debian 7, 8
1.5.10. Fedora 19, 20, 23

1.6. Merkezi yönetim konsolu, veritabanı sunucusu olarak Microsoft SQL Server ve MySQL desteklemelidir.

1.7. Active Directory ile entegre olup domain içerisindeki bilgisayarlar otomatik olarak yönetim konsolunda listelenmeli ve bu bilgisayar ve sunuculara uzaktan agent ve antivirüs kurulumu yapabilmelidir.

1.8. Yönetim konsolu üzerinden, Agent yüklü makinelerin aşağıdaki özellikleri görüntülenmelidir ve bu bilgiler istenildiği zaman PDF, CSV ve PostScript formatında raporlanabilmelidir.

1.8.1. Üretici

1.8.2. Model

1.8.3. Ağ Adaptörü IP Adresi

1.8.4. İşletim Sistemi Adı

1.8.5. İşletim Sistemi Versiyon Numarası

1.8.6. İşletim Sistemi Dili

1.8.7. İşletim Sistemi Saat Dilimi

1.8.8. Oturum Açmış Kullanıcı Adı

1.9. Bilgisayarlar, sunucular ve mobil cihazlardan toplanan tehdit günlükleri merkezi yönetim yazılımı veritabanında barındırılmalı ve veritabanında ne kadar süre saklanacağı seçilebilmelidir.

1.10. Yönetim yazılımı üzerinden tehditler, bilgisayar koruma durumları, antivirüs yüklü olmayan makineler gibi detaylı raporlar .PDF, CSV, PS formatında çıktı alınabilmeli ve bu raporlar düzenli olarak yerel diske kaydedilebilmeli veya bir eposta adresine gönderilebilmelidir.

1.11. Yönetim konsolu üzerinden Agent yüklenmiş makinelere aşağıda açıklanan komutlar uzaktan gönderilebilmelidir.

1.11.1. **Bilgisayar Tarama Komutu**: Yönetim konsoluna bağlı bilgisayarlarda istenilen zamanda virüs taraması başlatabilmelidir.

1.11.2. **Yazılım Yükleme Komutu**: Yönetim konsoluna bağlı Windows, Linux ve Mac OS işletim sistemlerine antivirüs yazılımını kurabilmelidir. Windows bilgisayarlara MSI tabanlı 3. parti uygulamaları HTTP ve Dosya Paylaşımı (SMB) üzerinden uzaktan kurabilmelidir.

1.11.3. **Yazılım Kaldırma:** Bilgisayarda yüklü MSI tabanlı uygulamaları uzaktan kaldırabilmelidir.

1.11.4. **Mesaj Gönderme Komutu:** Windows bilgisayarlar ve Android / iOS işletim sistemine sahip mobil cihazların ekranında belirtilen metin mesajını görüntülemelidir.

1.11.5. **Windows ve Linux Shell Komutu**: Windows ve Linux bilgisayarlara istenen Shell (komut satırı) komutlarını gönderip çalıştırabilmelidir. Örn: Ipconfig /flushdns

1.11.6. **Bilgisayarları Kapatma ve Yeniden Başlatma**: Konsola bağlı bilgisayarlarda uzaktan kapatma ve yeniden başlatma yapabilmelidir.

1.12. Yönetim yazılımının Agent'ını bilgisayarlara kurmak için aşağıdaki kurulum yöntemlerini desteklenmelidir.

1.12.1. **Uzaktan Kurulum**: Yönetim konsolu, Active Directory üzerinden bulduğu makinelere uzaktan kendi Agent yazılımını kurabilmelidir.

1.12.2. **GPO ve SSCM** :Uzaktan Yönetim konsolu, Active Directory GPO ve SSCM üzerinden Agent kurulumu yapmaya olanak sağlayan konfigürasyon dosyasını oluşturabilmelidir.

1.12.3. **Script Dosyası:** Windows, Linux ve Mac OS işletim sistemlerine Agent kurabilen script dosyası konsol üzerinden çıkartılabilmelidir.

1.12.4. **.EXE Dosyası**: İçerisinde agent ve antivirüs kurulum dosyalarını bulunduran bir .exe paketi çıkartılabilmelidir. Bu paket oluşturulurken içerisine lisans ve konfigürasyonlar gömülebilmelidir.

1.13. Yönetim yazılımı üzerinden istemciler üzerinde yüklü olan yazılım bilgileri görülebilmelidir. Aşağıda bulunan bilgiler yönetim yazılımı tarafından listelenebilmelidir.

1.13.1. Üretici

1.13.2. Yüklü yazılımın sürüm bilgisi

1.13.3. Boyut bilgisi

1.13.4. Uzaktan kaldırmayı destekleyip desteklemediği bilgisi

1.14. Yönetim yazılımı üzerinden istemcilerin aşağıda belirtilen donanım bilgileri görülebilmelidir.

1.14.1. CPU

1.14.2. RAM

1.14.3. Depolama alanı

1.14.4. Bağlı çevre birimleri

1.14.5. Tanımlı yazıcılar

1.14.6. Ağ bağdaştırıcıları

1.15. Merkezi Yönetim Konsolu Android ve iOS işletim sistemleri için Mobile Device Management (MDM) özelliği içermelidir.

1.16. Android mobil cihazlarda aşağıda açıklaması yapılan işlemleri yapabilmelidir:

1.16.1. **Antivirüs**: Kötü amaçlı Android uygulamalarını tespit edip ve temizler.

1.16.2. **Anti-Theft**: Çalınmaya karşı koruma özelliği ile uzaktan cihaz kilitleme, GPS üzerinden konum bulma, siren çaldırma, güvenilir sim kart belirleme özelliklerini sağlama.

1.16.3. **Anti-phishing**: Mobil tarayıcılarda girilen web sitelerini tarayarak oltalama saldırılarını önler.

1.16.4. **Uygulama Kontrolü**: Telefonlara yüklenen uygulamaları kısıtlar. Kısıtlama; uygulama ismine, kategorisine ve uygulama izinlerine göre belirlenebilir.

1.16.5. **Yüklü Uygulamalar**: Android cihazda yüklü uygulamaların listesi yönetim konsoluna gönderilir ve yönetim konsolunda görüntülenebilir.

1.17. iOS mobil cihazlarda aşağıda tanımları yapılan özellikler bulunmalıdır:

1.17.1. **Anti-Theft**: Çalınmaya karşı koruma özelliği ile iOS cihaz uzaktan kilitlenip kilidi açılabilmeli ve cihaz içindeki tüm kişisel verileri silen bir komut gönderilebilmelidir.

1.17.2. **Uygulama Kontrolü**: Uygulama kontrolü özelliği ile uygulama beyaz listesi ve kara listesi oluşturulabilmelidir.

1.17.3. **iCloud Denetimi**: Kullanıcının iCloud hesabı ile yapabileceği işlemleri kısıtlayan bir özellik bulunmalıdır.

1.17.4. **Cihaz Yönetimi**: iOS cihazlara uzaktan WIFI, VPN, HTTP Proxy, Mail Hesapları, Kişiler, Takvim, Google hesabı bilgileri gönderilebilmelidir.

1.18. Yönetim yazılımı oluşturduğu günlükleri depolamak için Syslog server ve native IBM Qradar desteği bulunmalıdır.

1.19. Windows bilgisayarlarda yüklü olan antivirüs programlarını otomatik olarak tespit ederek kaldırabilen bir özellik içermelidir.

1.20. Sunucu işletim sistemleri için her tipte kötü amaçlı yazılım türüne karşı etkili ve güvenilir koruma sağlamalı. Ağ Saldırısı Koruması ile ağ içinden veya dışardan sunuculara gelen atakları engellemeli Otomatik Dışlamalar özelliği ile kurulum yapılan sunucunun tipine göre tarama dışında bırakılması gereken dosya ve klasörler, ekstra bir işlem yapmanıza gerek kalmadan tarama dışında bırakılabilir olmalı.

2. Kullanıcılarda ve Sunucularda Çalışacak Koruma Modülü

2.1. Lisans yenilemesi yapılacak antivirüs yazılımı aşağıda belirtilen işletim sistemlerine kurulabilmelidir.

2.1.1. Windows XP, Vista, 7, 8, 8.1, 10

2.1.2. Mac OS X 10.6, 10.7, 10.8, 10.9 , 10.10 10.11, 10.12, 10.13

2.1.3. Debian, Fedora, Mandriva, Red Hat, SuSE

2.1.4. RHEL ve CENTOS 5, 6, 7

2.1.5. SLED ve SLES 11, 12

2.1.6. OpenSuse 13

2.1.7. Debian 7, 8

2.1.8. Fedora 19, 20, 23

2.2. Lisans yenilemesi yapılacak antivirüs yazılımı bilgisayardaki yerel diskler, taşınabilir cihazlar, ağ paylaşımları, İnternet trafiği, e-posta trafiğini ve ağ trafiğini gerçek zamanlı tarayarak virüs, solucan, truva atı, rootkit, adware, spyware, malware ve fidye yazılımı türevlerine karşı bilgisayarları ve sunucuları koruyacaktır.

2.3. Virüs taraması yapan antivirüs motoru üzerinde taranacak yerler, taranacak dosya boyutu ve uzantısı sınırlamaları, kullanılacak tarama teknolojileri gibi özelleştirmeler yapılabilmelidir.

2.4. İstenilen dosya ve klasörler antivirüs taraması dışında bırakılabilmelidir.

2.5. Antivirüs yazılımı, yayılan yeni virüsleri tanımasını sağlayan virüs veritabanı güncellemesini yerel ağdaki merkezi yönetim sunucusundan, internet üzerinden otomatik olarak indirebilmeli veya bilgisayara takılan bir USB bellek üzerinden yükleyebilmelidir.

2.6. Virüs imza güncellemesi isteğe bağlı olarak önceki bir tarihe çekilebilmeyi desteklemelidir.

2.7. Virüs imza güncellemeleri isteğe bağlı olarak normal, önceden dağıtım ve gecikmeli dağıtım olarak yüklenebilmelidir.

2.8. Antivirüs yazılımı isteğe göre virüs tespit ettiğinde kullanıcıya sormadan silecek şekilde ayarlanabilmelidir. Ayrıca antivirüs yazılımı grafik ara yüzü, kullanıcı masaüstü ortamında görünmeden sessiz modda çalışabilmelidir.

2.9. Belirlenecek bir parola antivirüs yazılımının bilgisayardan kaldırılması veya pasif hale getirilmesi engellenebilmelidir.

2.10. Antivirüs tarafından silinen tüm dosyalar yerel karantinaya taşınmalı ve istendiği zaman karantinadan dışarı çıkartılabilmelidir.

2.11. USB portları üzerinden çalışan depolama aygıtları, taşınabilir cihazlar, yazıcılar, tarayıcılar, akıllı kart okuyucular ve bluetooth cihazların bilgisayara takılmasını engelleyen bir aygıt kontrolü modülü bulunmalıdır. Bu modül sayesinde USB'den çalışan depolama cihazları için aşağıdaki şekilde kısıtlamalar yapılabilecektir.

2.11.1. **Engelleme**: Bilgisayara takılan cihaz engellenir ve kullanılamaz.

2.11.2. **Salt-Okunur**: Bilgisayara takılan depolama aygıtından dosya okunabilir, depolama aygıtına dosya aktarılamaz.

2.11.3. **Uyarı**: Bilgisayara USB takıldığında kullanıcıyı uyaran bir ekran çıkmalı, kullanıcı bu ekrana onay vererek USB depolama cihazını kullanmaya devam edebilir.

2.12. Bilgisayara takılan USB depolama cihazlarında otomatik olarak tarama başlatılabilmelidir.

2.13. Bilgisayardaki HTTP/HTTPS trafiği taranmalı ve denetlenen URL'ler üzerinde anahtar kelime bazlı ve alan adı bazlı engelleme yapılabilmelidir.

2.14. Bilgisayarda istenilen zamanda ve aralıklarda otomatik virüs taraması başlatılabilmelidir ve virüs taraması zamanlayıcısı aşağıdaki fonksiyonları desteklemelidir.

2.14.1. Taramadan sonra bilgisayarda otomatik olarak Kapatma, Yeniden Başlatma, Uyku Modu ve Hazırda Bekleme işlevlerini yapabilmelidir ve kullanıcının bu işlevleri engelleyip engelleyememesi ayarlanabilmelidir.

2.14.2. Kullanıcının, zamanlanan taramayı belirtilecek dakika kadar duraklatabilmesini desteklemelidir.

2.14.3. Dizüstü bilgisayarlar bataryada çalışıyorsa taramayı atlamayı desteklemelidir.

2.14.4. Tarama belirli bir zaman aralığında rastgele başlamayı desteklemelidir.

2.15. Aşağıda listelenen özelliklere sahip bir HIPS(Host Bazlı Saldırı Önleme) modülü bulunmalıdır.

2.15.1. Bilgisayarda çalışan uygulamaların davranış analizini yaparak Cryptolocker gibi fidye yazılımlarını engelleyebilmelidir.

2.15.2. Windows kayıt defterini denetlemeli ve belirli kayıt defteri anahtarlarında yapılacak değişiklikler oluşturulacak kural ile engellenmeli ve girişimler kayıt altına alınmalıdır.

2.15.3. Yolu belirtilen .exe dosyasının çalıştırılması bir kural ile engellenebilmelidir.

2.15.4. Bilgisayara yeni bir sürücü yükleme bir kural ile engellenebilmelidir.

2.15.5. Windows başlangıcında çalışacak olan uygulamalarda bir değişiklik meydana geldiğinde bildirim çıkartabilmelidir.

2.16. POP3/POP3s ve IMAP/IMAPS eposta protokollerini gerçek zamanlı olarak tarayarak gelen ve giden epostalarda virüs taraması yapabilmelidir.

2.17. Bilgisayardaki gelen/giden ağ trafiğini tarayan, isteğe göre gelen/giden bağlantı kuralları oluşturulabilecek bir güvenlik duvarı modülü bulunmalıdır.

2.18. Bilgisayarın kurduğu botnet trafiğini ağ seviyesinde tespit edip engelleyebilen ayrı bir botnet engelleyici modül bulunmalıdır.

2.19. Bilgisayara gelen/giden ağ paketlerini tarayarak aşağıda belirtilen saldırılara karşı koruma sağlayacak bir IDS (Intrusion Detection Systems) modülü bulunmalıdır.

2.19.1. DNS ve ARP poisoning attack

2.19.2. Port Scanning Attack

2.19.3. Eternalblue Exploit Attack

2.20. Windows istemcilerine kurulacak antivirüs Microsoft Outlook, Thundebird gibi eposta istemcileri için istenmeyen e-posta(spam) engelleyici bulundurmalıdır. Modül tarafından tespit edilen istenmeyen e-postalar İstenmeyen Eposta klasörüne otomatik taşınmalıdır.

2.21. İstenmeyen e-posta engelleyici modül üzerinde Genel Kara Liste, Genel Beyaz Liste, Kullanıcı Kara Listesi ve Kullanıcı Beyaz Listesi tanımlanabilmelidir. Kullanıcılar Outlook üzerindeki e-postalara tıklayıp istenmeyen e-posta olarak işaretleyebilmelidir.

2.22. Microsoft Outlook ve Windows Live Mail için otomatik olarak kurulan bir eklentisi bulunmalı. Bu eklenti sayesinde kullanıcı istediği epostayı tekrar antivirüs taramasından geçirebilmelidir.

2.23. Bulut tabanlı bir itibar veritabanı özelliğine sahip olmalı ve istenen dosyanın ilk görülme tarihi ve kullanım sıklığı görüntülenebilmelidir.

2.24. Web tarayıcılar, Microsoft Office bileşenleri, PDF okuyucuları ve eposta istemcilerinin açıklarından faydalanan exploit ve 0day saldırılarını engelleyebilecek bir Exploit engelleme modülü bulunmalıdır.

2.25. Bilgisayar kilit moduna girdiğinde, ekran koruyucu devreye girdiğinde veya kullanıcı oturumu kapatıldığında otomatik olarak bilgisayar taraması yapabilmelidir. Dizüstü bilgisayarlar bataryada çalışıyorsa taramayı atlayabilmelidir.

2.26. Bilgisayarlarda virüs taraması yapabilmek için ön yüklenebilir bir kurtarma ortamının ISO dosyası üreticinin web sitesinden hazır olarak indirilebilmelidir. CD veya USB belleğe yazdırılan ISO dosyası ile bilgisayardaki işletim sistemi taranabilecektir.

2.27. Lisans yenilemesi yapılacak antivirüs yazılımı aşağıda belirtilen işletim sistemlerine işletim sistemi seviyesinde, sanallaştırma platformlarına ise host seviyesinde kurulabilmelidir.

2.27.1. Microsoft Windows Server
2003 / 2003R2 / 2008 / 2008R2 / 2012 /2012R2 / 2016

2.27.2. Microsoft Windows Storage Server 2008 R2 Essentials SP1/2012/2012 R2

2.27.3. Microsoft Windows Small Business Server 2003 (x86) / 2003 R2(x86) / 2008 (x64) / 2011 (x64)

2.27.4. Microsoft Windows Server 2012 Essentials / 2012 R2 Essentials

2.27.5. Microsoft MultiPoint Server 2010 / 2011

2.27.6. Windows MultiPoint Server 2012

2.27.7. Debian, Fedora, Mandriva, Red Hat, SuSE

2.27.8. VMware vSphere 5.5, 6.0 ve 6.5

2.27.9. Windows Server 2008 R2 Hyper-V, Windows Server 2012 Hyper-V, Windows Server 2012 R2 Hyper-V, Windows Server 2016 Hyper-V

2.28. Windows sunuculara kurulacak antivirüs yazılımı Microsoft Azure Marketplace üzerinde ürün olarak bulunmalıdır.

2.29. Lisans yenilemesi yapılacak antivirüs yazılımı fiziksel ve sanal sunuculardaki yerel diskler, taşınabilir cihazlar, ağ paylaşımları, Internet trafiği ve e-posta trafiğini gerçek zamanlı olarak tarayarak virüs, solucan, truva atı, rootkit, adware, spyware, malware ve fidye yazılımı türevlerine karşı koruyacaktır.

2.30. Virüs taraması yapan antivirüs motoru üzerinde taranacak yerler, taranacak dosya boyutu ve uzantısı sınırlamaları, kullanılacak tarama teknolojileri gibi özelleştirmeler yapılabilmelidir.

2.31. Kurulacak antivirüs yazılımı Windows Server üzerindeki IIS, SQL Server, Exchange Server, Sharepoint, Hyper-V, Kerio Connect ve Kerio Control uygulamalarını tespit edip, bu uygulamaların hassas dosyalarını ve veritabanı dosyalarını otomatik olarak antivirüs taraması dışında tutan bir özellik bulundurmalıdır.

2.32. İstenilen dosya ve klasörler antivirüs taraması dışında bırakılabilmelidir.

2.33. Windows sunuculara kurulacak antivirüs yazılımı dosyaları tarama dışında bırakabilmenin yanında istenilen windows işlemini (process) tarama dışında bırakabilmeye imkan tanımalıdır.

2.34. Windows Hyper-V ana makinesine kurulacak antivirüs yazılımı, bu ana makine üzerinde çalışan sanal sunuculara herhangi bir program kurmaya gerek kalmadan antivirüs taraması yapabilmelidir.

2.35. Windows Terminal Sunucularda, oturum açan her kullanıcı için antivirüs grafik arayüzünün çalışmasını engelleyen bir terminal modu bulunmalıdır.

2.36. Vmware vShield ve NSX ürünlerine entegre olarak sanal makineleri bir agent kurulmadan tarayabilmelidir.

2.37. Sunucularda virüs taraması yapabilmek için ön yüklenebilir bir kurtarma ortamının ISO dosyası üreticinin web sitesinden hazır olarak indirilebilmelidir. CD veya USB belleğe yazdırılan ISO dosyası ile bilgisayardaki işletim sistemi taranabilecektir.

2.38. Web tarayıcılar, Microsoft Office bileşenleri, PDF okuyucuları ve eposta istemcilerinin açıklarından faydalanan exploit ve 0day saldırılarını engelleyebilecek bir Exploit engelleme modülü bulunmalıdır.

2.39. Belirlenecek bir parola antivirüs yazılımının bilgisayardan kaldırılması veya pasif hale getirilmesi engellenebilecektir.

2.40. Daha önce hiç görülmemiş tehdit türlerini tespit etmek için bulut tabanlı sandbox teknolojisini kullanarak sıfır gün tehditlerine karşı proaktif koruma sağlamayı amaçlayan birden fazla bulut bileşeninden oluşan bir sisteme sahip olmalıdır. Kum havuzu, kod statik analizi, makine öğrenimi, bellek içi içgözlem ve davranış tabanlı algılama kullanarak örneklerin derin incelemesini gerçekleştiren çok sayıda sensörden oluşmalıdır.

2.41. Bilgisayara gelen/giden ağ paketlerini tarayarak aşağıda belirtilen saldırılara karşı koruma sağlayacak bir IDS (Intrusion Detection Systems) modülü bulunmalıdır.

2.41.1. DNS ve ARP poisoning attack

2.41.2. Port Scanning Attack

2.41.3. Eternalblue Exploit Attack

Uzm. Gör.
Melda BEYAZ KORKUT

Dr. Uzm. Üyesi
Emel GÜLER