**Yeni Nesil İstemci ve Sunucu Güvenlik Yazılımı**

**Alımı Teknik Şartnamesi**

**İşin çeşidi :** Lisans Alımı

**İşin niteliği :** PaloAlto Cortex XDR Yeni Nesil İstemci ve Sunucu Güvenlik Yazılımı Lisans Alımı, Kurulumu ve Güncellenmesi Hizmeti

**Alınması Planlanan Hizmetle İlgili Ürünler:**

## PaloAlto Cortex XDR-Yeni Nesil İstemci ve Sunucu Güvenlik Yazılımı

**Şartnamede;**

İstanbul Bilgi Üniversitesi – KURUM, BİLGİ

İstanbul Bilgi Üniversitesi-Santral Kampüsü-Bilişim Teknolojileri Departmanı – BT Dept.

Teklif veren kuruluş, FİRMA / YÜKLENİCİ,

Satın alınacak Donanım / Yazılım / Hizmet olarak anılacaktır.

**ÖN KOŞULLAR**

* İşbu şartname, BİLGİ'nin kendi lokasyonunda konuşlandırdığı yukarıda belirtilen yazılımla ilgili lisans alımı, kurulumu bakımı konusunda bilgi birikimine sahip olan FİRMA dan alımın yapılmasını kapsamaktadır.
* Yazılım lisansının teslimat adresi, BİLGİ’ nin Santral Kampusu – BT Departmanıdır.
* BİLGİ adına hazırlanmış lisans bilgileri, sözleşme başlangıç tarihinden itibaren en geç 1 hafta içinde BİLGİ BT Dept. na teslim edilecek veya ilgili sunucu üzerinde güncel lisans aktivasyonu sağlanacaktır.
* Satın alınacak her bir mal ve hizmete ait orijinal belge ve doküman (İngilizce ve/veya Türkçe) tam olarak kullanıcıya teslim edilecektir. FİRMA, ürünlerle ilgili tüm sertifikasyonları ıslak imzalı teklifle birlikte teslim edecektir.
* HİZMET’i oluşturan lisanslar BİLGİ adına kayıtlı ve son sürüm olmalı veya son sürüm FİRMA tarafından teslimattan sonraki ilk ay içinde BT Dept. onayıyla yüklenmelidir.

**GENEL İSTEK VE ÖZELLİKLER**

* Yayımlanan versiyon güncellemeleri ve yamalar sözleşme tarih aralığında FİRMA desteğiyle bedelsiz olarak uygulanacaktır.
* FİRMA, Uygulama hatalarından kaynaklanan servis kayıtlarına limitsiz olarak destek verecek, üretici firma ile iletişimi sağlayacaktır.
* FİRMA, konusunda uzmanlaşmış mühendisini/teknik personelini yazılım kurulumu, lisans güncelleme, lisans bakımı ile ilgili konularda, tüm işleri takip etmekten sorumlu olarak atayacak ve bu atamayı BİLGİ’ ye bildirecektir.
* FİRMA, güncelleme ile ilgili çağrı bildirimini takiben en geç 1 hafta içinde BİLGİ’nin onayını alarak gerekli güncellemeyi yapacaktır.
* FİRMA, lisansla ilgili problemlere en kısa sürede müdahale ve çözüm sağlayabilmek amacıyla kendi içindeki kaynakları harekete geçirirken gerekli hallerde ÜRETİCİ’ ye çağrı açacaktır. Doğrudan RMA kaydı açma konusunda üretici tarafından yetkilendirilmiş partner statüsünde olmalıdır.

**BİLGİ GÜVENLİĞİ, YETKİNLİK ve YETERLİLİK**

FİRMA’ nın aşağıdaki güvenlik ve kalite sertifikalarına sahip olması tercih sebebi olup, belgeler teklif dosyasına eklenecektir.

* ISO 27001 Bilgi Güvenliği Yönetim Sistemleri
* ISO 9001:2008 veya eşdeğer kalite uygunluk belgesi
* PaloAlto Cortex XDR Yönetim/Uzmanlık Sertifikası
* FİRMA hizmet kapsamındaki ürünle ilgili 1000 kullanıcı üzerinde lisanlamaya sahip en az 3 referansı belgeleyecektir.

**ÜRÜN ÖZELLİKLERİ**

* Teklif edilecek İstemci ve Sunucu Güvenlik Yazılımı tek ajan yazılımı olarak çalışacak ayrı ayrı çalışan ajan yazılımları olarak teklif edilmeyecektir.
* İstemci ve Sunucu Güvenlik Yazılımının yönetim arabirimi bulut ( cloud ) mimarisinde olacaktır. İstemciler, bulut ( cloud ) tabanlı web arayüzünden yönetilebilir olacaktır.
* İstemci ve Sunucu Güvenlik Yazılımı sıfırıncı gün zafiyetlerini istismar eden kodları (exploit prevention) ve zararlı yazılımları (malware prevention) teknik tabanlı engelleme özelliklerine sahip olacaktır.
* İstemci ve Sunucu Güvenlik Yazılımı exploit engeleme ve malware engelleme özelliği imza tabanlı olmayacaktır.
* Teklif edilecek İstemci ve Sunucu Güvenlik Yazılımı, zararlı yazılımlara karşı istemci ya da sunucu üzerinde statik analiz yapabilecektir. Böylece çalıştırılabilir dosyaları zararlı kod içerebilme potansiyeline karşı çalıştırmadan, dosyanın karakteristik yapısını ve niteliğini kontrol edebilecektir.
* Statik analiz için kullanılan model dosyası otomatik olarak indirilip ajanlara yüklenebilecektir.
* İstemci ve Sunucu Güvenlik Yazılımı ajanı işletim sistemi ya da uygulama zafiyetlerinden faydalanan atakları sisteme bulaşmadan önce tespit ederek engelleyebilecektir.
* Ajan kurulduğu sistemlerde zararlı kodun faydalanmaya çalıştığı zafiyet ile ilgili güvenlik yaması yüklenmemiş olsa bile koruma sağlayacaktır.
* İstemci ve Sunucu Güvenlik Yazılımı ajanı, istismar etme (exploitation) ana teknikleri ya da zararlı kod çalıştırılmasına olanak sağlayan zararlı yazılım (malware) tekniklerini ilgili process’in sonlandırılması ya da durdurulması ile engelleyebilecek ve bu şekilde atağı engelleyebilecektir.
* Zararlı bulunan çalıştırılabilir dosyaları karantinaya alabilecektir. Güvenlik yöneticisi isterse karantinaya alınan dosyayı geri döndürebilecektir.
* İstemci ve Sunucu Güvenlik Yazılımı ajanı dijital olarak imzalanmamış güvenilir kaynaktan gelmeyen dosyaların çalıştırılmasını kurulu olduğu sistemler üzerinde anlık olarak engelleyebilecektir.
* İstemci ve Sunucu Güvenlik Yazılımı kurulu olduğu sistem üzerinde belli klasörlerden dosya çalıştırılmasına izin vermeyecek şekilde yapılandırılma yeteneğine sahip olacaktır.
* İstemci ve Sunucu Güvenlik Yazılımı, hazır konfigürasyonunda en az 80 (seksen) process’i (İşletim sistemi processleri, MS Office, Adobe Reader, Internet tarayıcıları, vb) koruyabilecektir. Hangi process için hangi koruma modüllerinin açık ya da kapalı olacağına yönetim arayüzü üzerinden sistem yöneticisi karar verebilecektir.
* İstemci ve Sunucu Güvenlik Yazılımı, hazır konfigürasyonunun haricinde farklı processler ya da kurum içi geliştirilmiş özel uygulamalarında konfigürasyona eklenmesini ve korunmasını sağlayacaktır.
* İstemci ve Sunucu Güvenlik Yazılımı Microsoft Ofis Makro ve Betik (Script) temelli çalışan zararlı yazılımlara karşı koruma yapacaktır.
* Teklif edilecek İstemci ve Sunucu Güvenlik Yazılımı, Anti-Ransomware Koruma özelliği ile, fidye yazılımına karşı ek koruma sağlamalıdır. Herhangi bir veri kaybı oluşmadan önce fidye yazılımı ile ilişkili şifreleme tabanlı etkinliği ve fidye yazılımı etkinliğini analiz edebilmeli ve durdurabilmelidir.
* Teklif edilecek İstemci ve Sunucu Güvenlik Yazılımı oluşan şüpheli, zararlı kod içeren olay kayıtlarını Yönetim Sunucusu ara yüzünden detaylı olarak raporlayabilecektir.
* İstemci ve Sunucu Güvenlik Yazılımı konfigürasyona bağlı olarak önce zararlı olduğu tespit edilmiş olan dosyaları güvenlik duvarı üreticisinin bulut servisine hash sorgusu yaparak anlık olarak bloklama kabiliyetine sahip olacaktır.
* Teklif edilen yazılım, üretici firmanın bulut tabanlı analiz servisi olarak çalışabilen kum havuzu mimarisi (sandbox) ile entegre olabilecektir. Konfigürasyona bağlı olarak istenilmesi durumunda şüpheli dosyaların üretici firmanın bulut tabanlı analiz servislerine gönderilerek ek davranış analizlerinin yapılmasına ve sonucun zararlı olması durumunda buna göre engelleme ya da karantinaya alınmasını sağlamalıdır.
* Analiz için gönderilen dosyaların detaylı analiz raporları teklif edilen yazılımın yönetim arayüzünden indirilebilecektir.
* Teklif edilen yazılım yönetim cloud’u ile bağlantısı kesilse dahi Exploit ve Malware koruması yapabilecektir. Böylece kurulu olan son kullanıcı cihazları için kurum içerisinde veya dışında koruma sağlanacaktır.
* İstemci ve Sunucu Güvenlik Yazılımı yönetim sunucusu üzerinde, engellenen ataklarla ilgili registry kayıtları, dosya lokasyonu, bilgisayar ismi, tespit zamanı, kullanıcı bilgisi, işletim sistemi bilgisi, AD lokasyonu gibi bilgileri raporlayabilecektir.
* İstemci ve Sunucu Güvenlik Yazılımı, gelişmiş delillendirme (forensic) raporlar alınmasına olanarak sağlayacak, xml formatında, adım adım davranışları ve sonlandırılmış process’e ait kapsamlı hafıza (memory) çalışma bilgisinin (dump) alınmasını sağlayacaktır.
* İstemci ve Sunucu Güvenlik Yazılımı Java tabanlı ataklara karşı koruma sağlayacaktır.
* İstemci ve Sunucu Güvenlik Yazılımı sıfırıncı gün Exploit koruması ve Malware koruması için aşağıdaki atak türlerini engelleyebilecektir.

|  |  |
| --- | --- |
| * CPL Protection | * Kernel Privilege Escalation Protection |
| * DEP | * Library Preallocation |
| * DLL Security | * Memory Limit Heap Spray Check |
| * DLL-Hijacking Protection | * Null Dereference Protection |
| * Exception Heap Spray Check | * ROP Mitigation |
| * Exploit Kit Fingerprinting Protection | * SEH Protection |
| * Font Protection | * Shellcode Preallocation |
| * Hot Patch Protection | * ShellLink Protection |
| * JIT Mitigation | * SysExit |
| * Kernel APC Protection | * UASLR |

* İstemci ve Sunucu Güvenlik Yazılımı, bilinmeyen çalıştırılabilir dosyaların çalıştırılmaması, kara listeye (blacklist) alınmış klasörlerden dosya çalıştırılmaması, beyaz listeye (whitelist) alınmamış ağ (network) klasörlerinden dosya çalıştırılmaması, yavru (child) process çalıştırılmasının engellenmesi ve dijital olarak imzalanmamış dosyaların çalıştırılmaması yeteneklerine sahip olacaktır.
* İstemci ve Sunucu Güvenlik Yazılımı, istenirse yüklü olduğu sistem üzerinde harici disk ve optik sürücüler üzerinde dosya çalıştırılmasını engelleyebilecektir.
* İstemci ve Sunucu Güvenlik Yazılımı Internet tarayıcıları (browser) üzerinden çalıştırılabilen java processlerine karşı koruma sağlayabilecektir.
* İstemci ve Sunucu Güvenlik Yazılımı, davranış veya teknik tabanlı koruma sağladığı sistemlerde tespit ettiği zararlı yazılım ve prosesler için son kullanıcıya özeleştirilebilir bir uyarı ekranı (pop-up) çıkarabilecektir.
* Engelleme yapıldığında çıkan pop-up ekranında hangi process’i neden engellediği bilgisini verecektir.
* İstemci ve Sunucu Güvenlik Yazılımı, davranış veya teknik tabanlı koruma sağladığı sistemlerde tespit ettiği zararlı yazılım ve prosesler için sistem yöneticisine mail ile uyarı bildirimi yapabilmelidir.
* İstemci ve Sunucu Güvenlik Yazılımı, davranış tabanlı koruma sağladığı sistemlerde tespit ettiği zararlı yazılım ve prosesler için oluşan iz kayıtlarını harici loglama veya SIEM ürünlerine syslog ile gönderebilmelidir.
* İstemci ve Sunucu Güvenlik Yazılımının yüklü olduğu sistemlerde kullanıcı, (admin haklarına sahip olsa bile) yazılım ajanına ait bir servisi durdurmak istediği veya yazılım ajanını sistemden kaldırmak istediği durumda parola koruması ile karşılaşmalı ve yazılım ajan servislerinin durdurulması ya da kaldırılması engellenebilmelidir.
* İstemci ve Sunucu Güvenlik Yazılımı, davranış tabanlı koruma sağlarken oluşabilecek istisnai (false positive) durumlar için ayrıcalık tanımlanabilmesine olanak sağlayacaktır. Bu ayrıcalık tüm yazılım ajanları için tanımlanabildiği gibi belirli ajan grupları ya da ajanlar için de tanımlanabilecektir.
* Teklif edilen İstemci ve Sunucu Güvenlik Yazılımı, kara listeye (blacklist) alınmış dosyaların çalıştırılmasını engellemelidir.
* İstemci ve Sunucu Güvenlik Yazılımı ajanı aşağıdaki sistemlere yüklenebilmelidir;
* Windows XP (32-bit, SP3 ya da sonrası),
* Windows Vista (32-bit, 64-bit, ve SP1 ya da sonrası; FIPS mode),
* Windows 7 (32-bit, 64-bit, RTM ve SP1; FIPS mode; Home edition hariç bütün sürümler),
* Windows 8.1 (32-bit, 64-bit; FIPS mode),
* Windows Embedded 8.1 Pro,
* Windows 10 RTM (32-bit ve 64-bit),
* Windows 10 Pro (CB ve CBB) , Enterprise (CB, CBB ve LTSB),
* Windows 10 FCU (Fall Creators Update),
* Windows Server 2003 (32-bit, SP2 ya da sonrası),
* Windows Server 2003 R2 (32-bit, SP2 ya da sonrası),
* Windows Server 2008 (32-bit, 64-bit; FIPS mode),
* Windows Server 2008 R2 (32-bit, 64-bit; FIPS mode),
* Windows Server 2012 (bütün sürümler; FIPS mode),
* Windows Server 2012 R2 (bütün sürümler; FIPS mode),
* Windows Server 2016
* Windows Server 2019
* macOS 10.12
* macOS 10.13
* macOS 10.14
* macOS 10.15
* macOS 11.0
* CentOS 6-7-8
* Debian 8-9-10
* Ubuntu 14-16-18
* İstemci ve Sunucu Güvenlik Yazılımı Citrix (XenDesktop RDS ve VDI), Microsoft (Server 2008, 2012, 2016 RDS) ve Vmware (Horizon View RDS ve VDI) VDI ortamlarında çalışmayı destekleyecektir.
* Teklif edilecek İstemci ve Sunucu Güvenlik Yazılımı OS X ve MacOS için aşağıdaki exploit ve malware korumalarına sahip olacaktır.
* JIT
* ROP
* Dylib-Hijacking koruması
* Kernel Privilige escalation
* Gatekeeper Enhancement
* İstemci ve Sunucu Güvenlik Yazılımı, istemcilerde yüklü olan ajanların yeni bir versiyonu çıktığında yönetim konsolu üzerinden yeni versiyona güncelleme yapılmasını destekleyecektir.
* İstemci ve Sunucu Güvenlik Yazılımı, istemcilerde yüklü olan ajanları uzaktan kaldırabilmelidir.
* İstendiğinde son kullanıcı makinalarında yazılım ajanının işletim sistemi durum çubuğunda simge olarak çıkması engellenebilmelidir.
* İstemci ve Sunucu Güvenlik Yazılımı yönetim ekranında, her bir yazılım ajanının online ve offline durumları görülebilmelidir.
* İstemci ve Sunucu Güvenlik Yazılımı yönetim ekranından oluşturulan ajan kurulum dosyası, Microsoft SCCM ile uzaktan kurulabilmeli ve kaldırılabilmelidir.
* Teklif edilen yazılım aktif dizin ile entegre çalışabilmeli ve kullanıcı/kullanıcı grubu bazlı kurallar oluşturulabilmelidir.
* Teklif edilen çözümün PCI-DSS ve HIPAA uyumluluk raporu alınmasına olanak sağlamalıdır.
* Teklif edilen çözüm Gartner “Endpoint protection platformu” raporunda ve Forrester, AV-test ve AV-Comparatives test ve raporlarına katılmış olmalıdır.
* Kurulum teklif dahilinde olup, lisans ve destek paketleri 1 ve 3 yıllık olarak 300 ve 1600 adet olarak teklif edilecektir.

**BİLGİ** **FİRMA**