1. Veri Merkezi Güvenlik Yazılımı

1.1. Teklif edilecek Veri Merkezi Güvenlik Yazılımını oluşturan tüm bileşenler aynı üreticiye ait tek bir ürün olacaktır. Aynı üreticiye dahi ait olsa farklı ürünlerin bir araya getirilmesinden oluşturulan bir çözüm olmayacaktır.

1.2. Teklif edilecek Veri Merkezi Güvenlik Yazılımı fiziksel, sanal ve bulut ortamdaki sunucu sistemlerin güvenlik politikalarını tek bir noktadan yönetebilecek özellikte olacaktır.

1.3. Teklif edilecek Veri Merkezi Güvenlik Yazılımı Merkezi Yönetim Sistemi ve İşletim sistemi ajan uygulamalarından oluşacaktır.

1.4. Teklif edilecek Veri Merkezi Güvenlik Yazılımı aşağıdaki işletim sistemi platformlarında çalışabilecektir:

- 1.4.1. Microsoft Windows
- 1.4.2. Red Hat Enterprise Linux
- 1.4.3. CentOS Linux
- 1.4.4. Rocky Linux
- 1.4.5. Oracle Linux
- 1.4.6. SUSE Linux
- 1.4.7. Ubuntu Linux
- 1.4.8. Debian Linux
- 1.4.9. CloudLinux
- 1.4.10. Amazon Linux
- 1.4.11. AlmaLinux
- 1.4.12. Solaris
- 1.4.13. AIX

1.5. Teklif edilecek Veri Merkezi Güvenlik Yazılımı yüksek erişilebilir mimaride çalışmayı desteklemelidir.

1.6. Teklif edilecek Veri Merkezi Güvenlik Yazılımı Merkezi Yönetim Sistemi Linux (Red Hat) ve Windows işletim sistemleri üzerinde çalışmayı destekleyecektir.

1.7. Teklif edilecek Veri Merkezi Güvenlik Yazılımı Merkezi Yönetim Sistemi veritabanı olarak Oracle ve Microsoft SQL Server ile çalışmayı destekleyecektir.

1.8. Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde saldırı tespit ve önleme, güvenlik duvarı, zararlı yazılım önleme, web sitesi güvenilirliği, bütünlük gözleme, kütük inceleme ve uygulama kontrolü bileşenleri bulunacak, bu işlevlerle ilgili tüm bileşenler teklif edilecektir.

1.9. Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak saldırı tespit ve önleme bileşeni gelen ve giden trafiği tarayabilecek ve derin paket inceleme (DPI) çalışabilecek mimaride olacaktır.

1.10. Teklif edilecek Veri Merkezi Güvenlik Yazılımı, sanal yama (host based IPS) özelliğini barındıracaktır. Sanal yama özelliği ile sunucular üzerinde bulunan ağ zaafiyetleri tespit edilebilecek, isteğe bağlı olarak manuel ve otomatik olarak kapatılabilecektir.

İbrahim İÇEN
İstanbul Üniversitesi-Cerrahpaşa
Hastaneler Genel Direktörlüğü
İSHOP
Analiz ve Uygulama Sorumlusu

1.11. Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak olan güvenlik duvarı, keşif taramalarını engelleme yeteneğine sahip olmalıdır. Bu güvenlik duvarı ile MAC,IP,Protokol,Port bazlı erişim kuralları uygulanabilecektir.

1.12. Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak bütünlük gözleme bileşeni kritik işletim sistemi dosyaları, dizinleri, kayıt defteri (registry) anahtar ve değerlerindeki değişiklikleri gerçek zamanlı izleyerek rapor edebilecek, alarm üretebilecektir.

1.13. Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak zararlı yazılım önleme bileşeni aynı üreticiye ait davranış tabanlı analiz motorunu kullanacaktır. Üçüncü taraf bir üreticiye ait motor kullanmayacaktır.

1.14. Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak kütük inceleme bileşeni çalıştığı işletim sistemi üzerindeki işletim sistemi ve uygulamalara ait günlük kayıtları ve kütükleri izleyerek şüpheli durumları rapor edebilecek, alarm üretebilecektir.

1.15. Teklif edilecek Veri Merkezi Güvenlik Yazılımı uygulama kontrolü özelliği ile işletim sistemi üzerinde çalışan uygulmalarada beyaz liste ve kara liste oluşturabilecektir. Bu modül mevcut envanteri çıkarıp ona izin verecek ve sonrasındaki yeni gelen veya değişen uygulamaları bloklayabilecektir.

1.16. Teklif edilecek Veri Merkezi Güvenlik Yazılımı sanal yama, kütük inceleme ve bütünlük gözleme bileşeni için sunucuda bir keşif taraması yaparak çalışan uygalama ve rollere göre otomatik olarak kurallar önerebilecektir. Böylece her sunucu için o sunucuya özgü bir kural setini otomatik olarak uygulayabilecektir.

1.17. Teklif edilecek Veri Merkezi Güvenlik Yazılımı VMware NSX ile entergre çalışabilecektir ve sunucularda ajansız koruma sağlayabilecektir.

1.18. Teklif edilecek Veri Merkezi Güvenlik Yazılımı üreticinin Global Tehdit İstihbarat hizmetine erişebilecek, bu hizmet sayesinde web sayfaları, elektronik posta kaynakları ve dosyalar için saygınlık sorguları yapabilecektir.

1.19. Teklif edilecek Veri Merkezi Güvenlik Yazılımı, aynı üreticinin Gelişmiş Saldırılar İçin Detaylı Analiz Sistemi ile entegrasyonu destekleyecektir. Bu entegrasyon ile şüpheli gördüğü dosyaları analize gönderebilecektir. Ayrıca analiz sonucu bulunan dosya ve URL leri bloklayabilecektir.

1.20. Teklif edilecek Veri Merkezi Güvenlik Yazılımı "docker" içeren bir işletim sistemi içinde çalışan konteynerlar için antivirüs, IPS ve firewall korumasını destkeleyecektir. Aynı işletim sistemi içindeki iki konteyner arasındaki trafiği inceleyebilecek ve atakları bloklayabilecektir.

1.21. Teklif edilecek Veri Merkezi Güvenlik Yazılımı ayrı bir lisans ile SAP sunucularıyla entegre olabilecek ve SAP ortamındaki dosyaları tarayabilecektir. Teklif edilecek Veri Merkezi Güvenlik Yazılımı, sanal masaüstü işletim sistemlerinin işlevselliğini değiştirmeden veya sınırlamadan çoklu oturum VDI Teklif edilecek Veri Merkezi Güvenlik Yazılımlerini desteklemelidir.

1.22. Teklif edilecek Veri Merkezi Güvenlik Yazılımı, kalıcı (persistent) ve kalıcı olmayan (non-persistent) VDI ortamlarında dağıtımı desteklemelidir.

İbrahim İÇEN
İstanbul Üniversitesi-Cerrahpaşa
Hastaneler Genel Direktörlüğü
BDP
Ağ ve Uygulama Sorumlusu

1.23. Teklif edilecek Veri Merkezi Güvenlik Yazılımı, imza tabanlı zararlı yazılım koruması, davranış analizi ve yapay zekâ/makine öğrenimi tabanlı analiz kombinasyonu sunmalıdır.

1.24. Teklif edilecek Veri Merkezi Güvenlik Yazılımının Makine öğrenimi, tehditleri tanımlayabilmek için hem dosya özelliklerini çıkaran ön-yürütme (pre-execution) zekâsına hem de dosya/süreç davranışının çalışma zamanı analizine (run-time) sahip olmalıdır.

1.25. Teklif edilecek Veri Merkezi Güvenlik Yazılımı, kötü amaçlı davranış sergileyen programlardan ek tehdit koruması sağlamak için, işletim sistemleri veya yüklü yazılımlarda olağandışı değişiklikleri sürekli izleyen bir davranış izleme modülüne sahip olmalıdır.

1.26. Teklif edilecek Veri Merkezi Güvenlik Yazılımı, exploit saldırılarıyla ilişkili anormal davranış sergileyen programları sonlandıracak anti-exploit işlevselliğine sahip olmalıdır. Teklif edilecek Veri Merkezi Güvenlik Yazılımı, Veri Yürütme Engellemesi (DEP), Yapılandırılmış Hata İşleme Taşması Koruması (SEHOP) ve heap spray önleme dahil olmak üzere çeşitli mekanizmalar kullanarak birden fazla exploit tekniğini tespit edebilmelidir.

1.27. Teklif edilecek Veri Merkezi Güvenlik Yazılımı, fidye yazılımlarına (ransomware) karşı bir koruma mekanizması sağlamalıdır. Bir makinenin ele geçirilmesi durumunda Teklif edilecek Veri Merkezi Güvenlik Yazılımı, belgeleri yetkisiz şifreleme veya değiştirmelere karşı korumalıdır.

1.28. Teklif edilecek Veri Merkezi Güvenlik Yazılımı, uç noktada fidye yazılımı tarafından şifrelenen dosyaların kopyalarını oluşturabilmeli ve etkilenen dosyaları orijinal durumuna geri yükleyebilmelidir.

1.29. Teklif edilecek Veri Merkezi Güvenlik Yazılımı, durum bilgisi olan denetim (stateful inspection) ile çalışan host tabanlı güvenlik duvarını desteklemeli; Kaynak/Hedef/Port/Protokol/Uygulama temelinde kurallar oluşturarak yüksek performanslı ağ virüs taraması ve durum bilgisi olan denetim sağlamalıdır.

1.30. Teklif edilecek Veri Merkezi Güvenlik Yazılımı, kurumsal uç noktalarda bilinmeyen ve istenmeyen uygulamaların çalışmasını engelleyerek kötü amaçlı yazılım ve hedefli saldırılara karşı savunmayı artırmak için entegre bir Uygulama Kontrol modülüne sahip olmalıdır. Bu, esnek ve dinamik politikaların, beyaz listeye alma (varsayılan reddetme) ve kilitleme yeteneklerinin birleşimiyle sağlanmalıdır.

1.31. Teklif edilecek Veri Merkezi Güvenlik Yazılımı, zararlı yazılımların yaptığı değişikliklerin (ağ ve dosya tabanlı kötü amaçlı uygulamalar, virüs ve solucan kalıntıları — Truva atları, kayıt defteri girdileri, virüslü dosyalar) otomatik temizliğini sağlayan hasar temizleme hizmetlerine sahip olmalıdır.

1.32. Teklif edilecek Veri Merkezi Güvenlik Yazılımı, ajanlardaki kayıt defteri değerleri, kayıt defteri anahtarları, servisler, süreçler, yüklü yazılımlar, portlar ve dosyalardaki beklenmedik değişiklikleri taramak için yerleşik bir Bütünlük İzleme modülüne sahip olmalıdır.

1.33. Teklif edilecek Veri Merkezi Güvenlik Yazılımı, işletim sistemi ve uygulama loglarında gizli kalabilecek önemli olayları tanımlamak için yerleşik bir Log

İbrahim İÇEN
İstanbul Üniversitesi Cerrahpaşa
Hastaneler Bilgi İşlem Direktörlüğü

Denetimi koruma modülüne sahip olmalıdır. Teklif edilecek Veri Merkezi Güvenlik Yazılımı bu olayları güvenlik bilgi ve olay yönetimi (SIEM) sistemine veya merkezi log sunucusuna korelasyon, raporlama ve arşivleme amacıyla gönderebilmelidir.

1.34. Teklif edilecek Veri Merkezi Güvenlik Yazılımı, container host'lar için host tabanlı koruma sağlamalı; kötü amaçlı dosyalara karşı gerçek zamanlı zararlı yazılım taraması ve çalışan container'ları yazılım açıklarının uzaktan istismarına karşı koruyacak saldırı önleme hizmetleri sunmalıdır.