FENERBAHÇE ÜNİVERSİTESİ
Ataşehir Kampüsü
"Güvenlik Donanım ve Yazılım Yönetimi Alımı"
TEKNİK ŞARTNAME

VERİ SIZINTISI ÖNLEME (DLP)

- Teklif edilecek çözüm **210** kullanıcı lisansına sahip olacak ve bu lisans sözleşme tarihinden itibaren **1** yıl süreyle kuruma teslim edilecektir.
- Kurum, üretici firmaya ait lisans sözleşmesini kabül ederek, teklif edilen çözümün **1** yıl süresince tüm güncelleme ve yeni yayınlanacak versiyonlarını (minör ve majör versiyonlar) bedelsiz olarak kullanım hakkına sahip olacaktır.
- Teklif edilecek çözüm, kritik bilgilerin kurum dışına çıkmasını önlemek amacıyla, veri sızıntılarını ağ ve kullanıcı bilgisayarı seviyesinde (http, https, ftp, smtp, USB, CD/DVD, printer gibi risk kanalları) tespit edebilmelidir.
- Teklif edilecek çözüm kritik bilgilerin, ağ seviyesinde başka hangi sunucu ve kullanıcı bilgisayarlarında bulunduğunu tespit edebilecek, takip edebilecek keşif modülüne sahip olmalıdır.
- Tanımlı kritik bilgilerin tespitinde tam bir doğruluk olabilmesi için özel teknolojilere sahip olmalıdır.
- Kuruma özel politikalar tanımlayabilmek için; belirli anahtar kelimeler, regular expression'lar, belirli dokuman tipleri kullanılabilmelidir.
- Kritik bilgilerin sisteme öğretilebilmesi için, sistem kritik bilgilerin bulunduğu dosyaların parmak izini alabilmelidir.
- Parmak izi alınmış veriler, verinin bulunduğu dökümandan (adı, uzantısı) bağımsız olarak, ağ seviyesinde, veri sızıntısı politikaları ile tespit edilebilmelidir. Tespit sistemi orjinal dökümandan bağımsız işleyebilmelidir.
- Kritik verilerin tespiti için sıkıştırılmış dosyalar (ZIP, TAR, RAR) en az 16 alt seviyeye kadar açılabilmelidir.
- Parmak izi alınacak dosyalar için; dosya tipi, uzunluğu, lokasyonu, en son değiştirilme tarihi bazında filtreleme politikaları tanımlanabilmelidir.

- Parmak izi teknolojisi için erişilen dosyaların orjinal dosya erişim tarihi değiştirilmemelidir.
- Sistem şifreli sıkıştırılmış dosyaları otomatik algılayabilmeli ve içeriği analiz edilemeyen bu gibi dosyaları tespit edip bloklayabilecek hazır politikalara sahip olmalıdır.
- Farklı dil ve karakter setindeki dosyaların parmak izini alabilmelidir
- Sistem ODBC ile database'e bağlanarak, veri tabanındaki kritik bilgilerin de parmak izini alabilmelidir. Veri sızıntısı olmaması için, bu yöntem manual bir iş gerektirmemelidir. Veritabanına düzenli olarak ODBC ile bağlanarak, sadece değişen kayıtların parmak izini alabilmelidir.
- Sistem dosyalar ve veritabanları üzerinden topladığı parmak izine ait veritabanını kullanıcı bilgisayarlarındaki ajan üzerinde kullanabilmelidir. Kullanıcı bilgisayar ajanı kurum ağı içerisinde olmasa bile parmak izine ait politikaları icra edebilmelidir.
- Sistem LDAP, MS Active Directory ile entegre çalışabilmeli, veri sızıntısı politikaları tanımlanırken, LDAP veya AD kullanıcılarına göre politikalar tanımlanabilmelidir. Sistem, birbirinden bağımsız birden fazla Directory Servis tanımlamaya ve entegrasyona izin vermelidir.
- Parmak izi alma veya PC'de kritik bilgilerin kopyalarını arama işlemleri için sisteme tanımlanan tüm şifreler, DB içerisinde şifreli olarak tutulmalı ve tanımlamaların hiçbirisi için şifreler açık bir şekilde konfigürasyon dosyalarına yazılmamalıdır.
- Politikalar içerisinde Bloklama, İzin verme, Karantinaya alma, USB'ye şifreli kopyalama ve sadece izleme şeklinde aksiyonlar tanımlanabilmelidir.
- Taşınabilir USB disklere yapılan kopyalama işlemlerinde, dosya bloklanabilmeli veya USB Disk'e şifreli olarak kopyalayabilmelidir.
- USB Disk'e kopyalamada, şifreleme için kullanılacak anahtarları sistem yöneticisi oluşturabilmelidir. USB Disk'e kopyalamada; ek bir ajan, ürün veya lisanslama gerekmemelidir.
- Anında mesajlaşma, dosya paylaşım programları gibi, şifreli erişime sahip uygulamalar üzerinden gönderilmeye çalışılan kritik verilerin tespiti için, kullanıcı bilgisayarındaki ajanlar kullanılabilmelidir.
- Ajanlar en az Windows 7, XP SP3, Server 2003 SP2, Server 2008 SP2, Server 2008 R2 SP1, Server 2012 R2, Mac OS 10.7, 10.8, 10.9, 10.10) işletim sistemlerini desteklemelidir.
- Kullanıcı bilgisayarındaki ajan vasıtası ile,

    - Kritik bilgilerin USB depolama aygıtlarına kopyalanması engellenebilmeli veya şifreli kopyalanmalıdır
    - Sadece tanımlı marka/model USB depolama aygıtlarına izin verilebilmelidir
    - Ajan, PC'den çıkan HTTP ve HTTPS trafiğini izleyebilmeli ve gerekirse trafiği daha client'dan çıkmadan engelleyebilmelidir
    - Ajan, paylaşılan dizinlere yapılan dosya kopyalamalarında (File Share), veriyi analiz edebilmeli ve gerektiğinde bloklayabilmelidir.
    - Belirli uygulama veya uygulama grupları arasındaki cut, copy, paste, print screen gibi işlemler denetlenebilmeli, istenirse bloklanabilmelidir.
    - Kullanıcı bilgisayarı ağa bağlı değilken farklı politikaları, bağlı iken farklı politikaları icra edebilmelidir.
    - Sadece kritik verilerin bulunduğu dökümanların print edilmesi engellenebilmelidir
    - Bilgisayarlar içerisindeki kritik bilgi barındıran dosyalar, keşif yöntemi ile tespit edilebilmeli ve raporlanabilmelidir.
    - Keşif işlemi bilgisayar kullanılmıyorken, veya CPU farklı bir uygulama tarafından meşgul edilmediği sıralarda otomatik olarak yapılabilmelidir.
- Belirli bir kullanıcı bilgisayarındaki ajanı, geçici bir süre ile durdurabilmek ve bunu kayıt altına alabilmek mümkün olabilmelidir.
- Ajanlar ve yönetim sunucusu arasındaki iletişim şifreli olmalıdır.
- Ajanlar Group Policy Object veya SMS ile kullanıcı bilgisayarlarına dağıtılabilmelidir.
- Kullanıcıların ajanları stop etmeye çalışması, kapatmaya çalışması durumunda kendini koruyabilmeli ve otomatik olarak tekrar çalışabilmelidir.
- Kullanıcı bilgisayarlarında görünen mesajlar Türkçe olabilmelidir.
- Tespit edilen güvenlik ihlalleri için sistem içerisinde bir çağrı kaydı açılabilmeli ve belirli bir kişiye atanabilmelidir.
- Açılan her çağrı içerisinde, politika ihlaline neden olan olayın detayları (Source IP, Kullanıcı, Veri sızıntısı tipi, politikası, hedef adres, veri örneği) belirtilmelidir
- Açılan çağrıların içerisinde, adli soruşturmada kullanılabilecek şekilde, ihlala neden olan bilgi saklanabilmelidir.
- Sisteme rol tabanlı erişim sağlanabilmelidir.

- Sistem yöneticilerinin, oluşan çağrılar içerisindeki adli kayıtları görmesi engellenebilmeli, sadece bu çağrılara bakabilecek ve adli kayıtları görebilecek haklara sahip kullanıcılar tanımlanabilmelidir.
- Bilgi ihlali durumunda yönetici, bilginin sahibi, bilgiyi gönderene uyarı mesajı eposta ile gönderilebilmelidir.
- Ürün içerisinde hazır rapor şablonları olmalıdır. Bu raporların haricinde, kuruma özel raporlar da hazırlanabilmelidir.
- Teklif edilecek çözüm kritik bilgilerin mail yoluyla kurum dışındaki mobil cihazlara ulaşmasını engellemelidir. Böylece kuruma ait kiritk bilgiler mobil cihazlar üzerinde kurum dışarısında taşınamamalıdır. Bunun için sistem mobil cihazlar ile mail sunucular arasındaki ActiveSync trafiğini kontrol edebilmelidir.
- Belirli bir zaman diliminde, belirli bir sayıda kritik bilginin, zamana yayılarak kurum dışarısına gönderilmesi durumunda (örneğin 1 dakika içerisinde 10 farklı mail içerisinde 1'er adet TC kimlik numarasının ayrı mesajlar halinde gönderilmesi ve sonuçta 10 farklı TC kimlik numarasının gönderilmesi durumu) sistem bunu tespit edebilmelidir.
- Ürün içerisinde parmak izi mekanizması dışında kuruma ait kritik verilerin tanımlanması için öğrenme yoluyla çalışan akıllı bir mekanizma (machine learning) olmalıdır.
- Teklif edilecek çözüm kritik bilgilerin image dosyası olarak kurum dışarısına çıkmasını engellemelidir. , image dosyalarını OCR teknolojisi ile tarayabilecek ve veri sızıntısını tespit edebilecek bir çözüme sahip olmalıdır.
- Teklif edilecek çözüm, kritik bilgilerin tanımlanması için yapılan parmak izi veri tabanını export edebilmeli, gerektiğinde başka bir networkte bulunan sunucu üzerinde import edebilmelidir.
- Teklif edilecek çözüm güvenlik analiz yeteneklerine sahip olmalı oluşan olay kayıtları üzerinde analizler yaparak en riskli kullanıcıları gösterebilen bir dashboard ekranına sahip olmalıdır.

Ağ Güvenlik Duvarı Sistemi

Ağ Güvenlik Duvarı aşağıda belirtilen güvenlik fonksiyonlarını ve teknolojilerini sağlamalıdır.

- Teklif edilen sistem, yeni nesil güvenlik duvarı özellikleri olarak asgari;
    - Güvenlik Duvarı (Firewall)
    - IPSec VPN Sonlandırma Sistemi
    - SSL VPN Sonlandırma Sistemi
    - Saldırı Tespit ve Engelleme Sistemi (IPS)
    - Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
    - Virüs/Zararlı İçerik Kontrolü
    - URL Kategori Filtreleme
    - Bant genişliği yönetimi

Özelliklerine sahip olmalıdır.

- Bu özellikleri üreticiye ait donanımsal çözüm olarak tek bir cihaz ile sağlamalıdır. Fakat IPSec VPN ve SSL VPN özelliklerinin Transparan konumlandırıldığında desteklenememesi durumda; aynı sistem üzerinde sanal güvenlik duvarı özelliği ile veya aynı üreticiye ait ayrı bir donanımsal ürün ile sağlanabilir.

- Cihaz tek bir fiziksel güvenlik duvarı olarak çalışabileceği gibi, herhalukarda kurumun ihtiyaç duyması durumunda en az 10 adet sanal güvenlik duvarı çalıştıracak şekilde konfigüre edilebilmelidir.

- Teklif edilen Ağ Güvenlik Duvarı High-Availability için Aktif-Aktif ve Aktif-Pasif olarak çalışmayı desteklemelidir. Aktif-Aktif çalışırken yük paylaşımı yapabilmelidir. Cihazlardan birinin arızalanması durumunda, diğer cihaz tüm fonksiyonları üstlenerek çalışmaya devam edebilmelidir.

- Yedeklilik konfügrasyonunda her segment için güvenlik duvarı üzerinde set edilecek Ip sayısı 1 (bir) adet olmalıdır. Bu sayede modüller için ayrı, cluster IP si için ayrı IP adreslerinin kullanımına gerek kalmamalıdır.

- Sistemin SPI (Stateful Packet Inspection) Firewall özelliği olmalıdır.

- Sistem, spoof edilmiş paketleri tespit edip bloklayacaktır

- Sistemde bulunan ağ arayüzlerinin her biri; LAN, WAN, DMZ, veya kullanıcı tarafından isimlendirilebilen segmentler olarak tanımlanabilmelidir. Sistem IEEE 802.1Q VLAN desteklemeli ve tanımlanan VLAN'lar arayüz (interface) olarak kullanılabilmelidir.

- Sistem Sanal Güvenlik Duvarı özelliği ile kullanıldığı durumda; sistem üzerindeki fiziksel ve sanal ara yüzler Sanal Güvenlik Duvarları arasında paylaştırılabilmelidir. Sanal Güvenlik Duvarları kural ve yönlendirme açısından birbirinden bağımsız olarak yönetilebilmelidir.

- Sistem; Layer3 (routing mod) ve Layer2 (saydam mod) katmanlarında çalışabilmelidir. Sistem üzerinde sanal güvenlik duvarı sistemlerinden istenilenler Layer3 te çalışabilirken aynı anda istenilen sanal güvenlik duvarları Layer2 de transparant olarak çalışabilmelidir.

- Saydam (Transparent) modda aşağıdaki özellikleri sağlamalıdır;
    - SPI (stateful packet inspection),

    - Saldırı Tespit ve Engelleme Sistemi (IPS)
    - Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
    - Ağ Geçidinde Virüs/Zararlı İçerik Kontrolü
    - URL Kategori Filtreleme

- Routing modda aşağıdaki özellikleri sağlamalıdır;
    - SPI (stateful packet inspection),
    - IPSec VPN Sonlandırma,
    - SSL VPN Sonlandırma,
    - Saldırı Tespit ve Engelleme Sistemi (IPS)
    - Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
    - Virüs/Zararlı İçerik Kontrolü
    - URL Kategori Filtreleme
    - Bant genişliği kontrolü
    - Statik yönlendirme (static routing),
    - RIP, OSPF ve BGP yönlendirme protokollerini desteklemelidir. Bu yönlendirme protokollerini sağlamak için lisans veya fazladan yazılım gerekiyorsa sağlanmış olmalıdır.
    - Sunucu yük dengeleme

- Ağ Güvenlik Sisteminin, Birden fazla Geniş Alan Ağı (WAN) bağlantısını desteklemeli, birden fazla Internet bağlantısını yedekli ve/veya aynı anda kullanabilmelidir.

- Ağ Güvenlik Sistemi, Kural Tabanlı Yönlendirmeyi (Policy Based Routing) desteklemelidir.

- Sistemin DHCP Server ve DHCP Relay özelliği bulunmalıdır.

- Güvenlik duvarı politikaları, kullanıcı grupları bazında yazılabilmeldir. Kullanıcı bilgisi için AD entegrasyonu olmalıdır.

- Sistem Bant Genişliği Kontrolü amacıyla kural tabanlı trafik biçimlendirme ve trafik önceliklendirme yapabilmelidir. Sistem QoS ve Differentiated Services desteklemelidir.

    - Kaynak, hedef ve protokol (SMTP, FTP, DNS, H323 gibi) bazında yazılan kurallarda trafik biçimlendirme tanımı da yapılabilmelidir.
    - Maksimum ve/veya garanti edilecek bant genişliği değeri öncelik değeri (düşük, orta, yüksek gibi) ile tanımlanabilmelidir.
    - Aynı kural dahilinde izin verilen her kaynak için, tanımlanan bant genişliğinin ortak bir şekilde kullanılabilmesi sağlanabilmelidir.
    - Uygulama bazında bant genişliği kontrolü yapabilmelidir.

- Güvenlik Sistemi; kendi üzerinde tanımlanan kullanıcı veritabanı, RADIUS ve LDAP üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir.

- Sistemin uygulama kontrol özelliği bulunmalıdır. Sistem; Mesajlaşma (MSN, ICQ, Yahoo, AOL gibi), P2P (Kazaa, Skype, bitTorrent, eDonkey, Gnutella vb) ve Web Uygulamaları gibi tanımlı en az 3.000 (üçbin) adet uygulamaya ait trafiği kullanılan porttan bağımsız olarak tanıyabilmeli, kontrol edebilmeli ve engelleyebilmelidir. Uygulama kontrolü kapsamında tanınan uygulamalar internet üzerinden güncelleme servisi ile güncellenmelidir.
- Sistem VPN Gateway olarak IPSec VPN desteklemelidir. DES, 3DES, AES Kriptolama ile MD5 ve SHA-1 desteklemelidir. IKE ve PKI desteği olmalıdır.

- IPS sistemi Trafik ve Protokol anomalilerini tespit edip durdurabildiği gibi, imza tabanlı saldırıları da tanıyıp durdurabilmelidir. IPS imzaları otomatik olarak internet üzerinden güncelleme servisi ile güncellenebilmelidir. Güncelleme işlemi manuel olarak ta yapılabilmelidir.

- Teklif edilen Ağ güvenlik sistemi Botnet aktivitesini tespit edip engelleyebilmelidir.

- Ağ Güvenliği Sistemi üzerinde, Mobil Kullanıcıların Kurum kaynaklarına güvenli olarak erişimini sağlayabilmek için, SSL VPN Gateway özelliği bulunmalıdır. SSL

VPN istemcisi en az Windows, Mac OS, Linux işletim sistemlerini ve IOS, Android tabanlı mobil cihazları desteklemelidir.

- SSL VPN Gateway içerisinden TCP ve UDP tabanlı trafikler tünellenebilmelidir.

- SSL VPN özelliği eşzamanlı minimum 5000 kullanıcı lisansı ile teklif edilecektir.

- SSL VPN üzerinden erişen kullanıcılar, Sistem üzerinde tanımlı kullanıcı veritabanı, RADIUS, LDAP üzerinden kimlikleri doğrulanabilmeli, yetkilendirilebilmeli ve bu yetkilendirme ile erişilebilecek kurum içi ve dışı kaynaklar tanımlanabilmelidir.

- SSL VPN ile erişim sağlayan kullanıcı veya sistemleri için; SPI (stateful packet inspection), Saldırı Tespit ve Engelleme Sistemi (IPS), Uygulama Tanıma ve Kontrolü (Application Control) Sistemi, Virüs/Zararlı İçerik Kontrolü ve URL Kategori Filtreleme, Bant Genişliği yönetimi (QoS) özellikleri uygulanabilir olmalıdır.

- Ağ Güvenlik Duvarı Sistemi üzerinde zararlı yazılım (Malware) tespit ve engelleme özelliği bulunmalıdır. Sistem; HTTP, SMTP, FTP ve POP3 trafiğini tarayarak zararlı yazılımları engelleyebilmelidir. Sistem, anılan protokoller içinde tarama yaparak; Worm, Trojan, Keylogger, Spy, Dialer türünden tehditleri tanıyıp durdurabilmelidir. Virüs Kontrolü, Ağ Güvenlik Duvarı Sistemi üzerinde bulunan bütün network segment'leri arasında yapılabilmelidir. AntiVirus sistemi Internet üzerinden virüs imzalarını otomatik olarak güncelleyebilmelidir

- Ağ Güvenliği Sistemi üzerinde URL Filtreleme özelliği bulunmalıdır. Bu sayede Kategori bazlı URL Filtreleme yapabilmelidir. Farklı kullanıcı ve kullanıcı gruplarına farklı kategorilerde URL filtreleme uygulanabilmelidir.

- Sistem üzerinde en az 60 adet URL kategorisi bulunmalıdır.

- Sistemin URL Filtreleme fonksiyonu için kullanıcı sınırı olmamalı ve sınırsız kullanıcı lisansı ile teklif edilmelidir.

- URL filtreleme kategorileri dışında, wildcard, regex veya tam URL olarak istenilen adreslerin farklı profiller altında tanımları yapılabilmelidir (Örneğin *.gov.tr* gibi). Tanımı yapılan bu adreslere erişim engellenebilmeli veya izin verilebilmelidir.

- İstenildiğinde categorilerden bağımsız olarak, sisteme eklenebilecek tam URL bilgisi (Örneğin: www.abc.com/deneme/sayfa1.php) bazında engelleme yapabilmelidir.

- URL filtreleme uyarı ekranları özelleştirilebilecektir.

- Teklif edilen tüm sistemlerin IPv6 desteği bulunmalıdır ve IPv4 ile IPv6 protokollerinin aynı anda kullanımına izin veren dual-stack özelliği desteklenmelidir. IPv6 kapsamında en az; IPv6 adresleme, IPv6 statik yönlendirme, IPv6 DNS, IPv6 güvenlik kuralları, IPv6 kayıt ve raporlama ve Ping6 desteklenmelidir.

- Sistem yapılandırması en az aşağıdaki yöntemler ile yapılabilmelidir:
    - Seri bağlantı ile konsol port üzerinden,
    - Http ve Https bağlantı ile web ara yüz üzerinden veya üreticinin kendisine ait Linux veya Windows tabanlı yönetim uygulaması üzerinden
    - SSH bağlantı ile komut satırı (commandline) üzerinden

- Ağ Güvenlik Duvarı Sistemin SNMP desteği olmalı ve SNMPv3 desteklemelidir

- Ağ Güvenlik Duvarı Sistemi işletim sistemi ve yazılım güncellemelerini Web ara yüzü, TFTP veya FTP üzerinden yapılabilmelidir.

- Önerilecek güvenlik duvarı sistemi üreticisinin, bir veya birden fazla ürünü, “NSS Labs Network IPS” ve “NSS Labs Next Generation Firewall” testlerine girmiş olması gereklidir.

- Teklif edilen Ağ Güvenlik Duvarı Sistemi üreticisi, güncel “Enterprise Firewall” için “Gartner Magic Quadrant” tablosunda yer almalıdır.

- Güvenlik Duvarı Sisteminin coğrafi veri tabanı bulunmalıdır. Ülke bazında kural yazılarak belirtilen ülke veya ülkelerden gelen trafiği kesebilmelidir.

- ***Güvenlik Duvarı Performans Değerleri***

- Teklif edilen Ağ Güvenlik Duvarı ile birlikte şartnamede belirtilmiş tüm güvenlik servis lisansları (IPS, URLFilter, App Control, VPN) teklife dahil edilecektir.

- Teklif edilen güvenlik sistemi, teklif edilen konfigürasyonda, en az 36 Gbps Firewall performansı değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

- Ağ Güvenlik Duvarı Tehdit Koruma (Firewall + IPS + Uygulama Denetimi + Antimalware) özellikleri aktifken en az **7 Gbps** kapasiteye sahip olmalıdır. Bu kapasite kullanıcı/istemci arasındaki istek-cevap trafiğinin toplamına (**çift yönlü analiz ile**) bu güvenlik özelliklerinin uygulandığı konfigürasyonda belirlenmiş olmalıdır. Belirtilen bu değer ürün kataloglarında yer almalıdır. Ürün kataloglarında Tehdit Koruma için farklı terminoloji kullanılmış ise bu koşulda ürün kataloğunda NGFW (Firewall + IPS + Uygulama Denetimi) kapasitesi gerçek ortam değeri baz alınarak en az **9.5 Gbps** olmalıdır.

- Sistem aynı anda en az 8 milyon oturumu desteklemeli ve saniyede en az 450.000 yeni oturum açabilme performansına sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

- Güvenlik Duvarı Sistemi en az 20 Gbps IPSec VPN throughput değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

- Güvenlik Duvarı Sistemi en az 5.0 Gbps SSL VPN throughput değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

- Sistem Site-to-Site için en az 2.000 adet, Client to site için 10.000 adet IPSec VPN tünel desteklemelidir. Cihaz, anılan VPN protokollerini destekleyen standartlarla uyumlu VPN Gateway cihazları ile uyumlu çalışabilmelidir

- Sistem 5 Gbps IPS throughput performans değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

- Sistem üzerinde;
    - En az 10 adet 1GE RJ45 ara yüz bulunmalıdır.
    - En az 8 adet 1GE SFP ara yüz bulunmalıdır.
    - En az 2 adet 10GE SFP+ ara yüz bulunmalıdır.

- Güvenlik Sistemi üzerinde en az 450 Gbyte kapasitede depolama alanı bulunmalıdır. Sistem Syslog Sunuculara, Sistem ile birlikte teklif edilecek Kayıt/Raporlama Sistemine kayıt gönderebilmeli ve sistem üzerindeki Depolama Biriminde de kayıt Tutabilmelidir.

- Sistemin; Firewall, VPN, IPS fonksiyonlarının hiç biri için kullanıcı sınırı olmamalıdır ve sınırsız kullanıcı lisansı ile teklif edilmelidir. Ağ Güvenlik Sisteminin 1 yıl süre ile Yazılım/işletim sistemi güncellemelerini ve en az 1 yıl süre için IPS, Uygulama Tanıma ve Kontrolü, AntiVirus, URL Kategori Filtreleme servis ve güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.

Ağ Güvenlik Loglama Sistemi

- Önerilen Sistem teklif edilen Ağ güvenlik Duvarına ait logların kayıt altına alınması ve izlenmesini sağlamalıdır.

- Önerilen sistem, günde 5 GB kayıt alabilmelidir.

- Log kayıt alanı olarak en az 3 TB depolama alanını desteklemelidir.

- Önerilen sistem Vmware veya HyperV üzerinde çalışabilmelidir ve gerekli lisanslar teklife dahil edilmelidir.

- Herhangi bir anda kurulmuş olan bağlantıları gerçek zamanlı olarak izleyebilme olanağı olacaktır.

- Cihaz üzerinden geçen tüm trafiğin günlüklerde tutulması, istenen kıstaslara göre (En az IP, IP aralığı, ağ, protokol, zaman) filtrelenebilmesi ve aktif bağlantıların gerçek zamanlı izlenebilmesi sağlanacaktır.

- Gün, saat veya haftalık periyodlarda yapılandırılabilen otomatik kayıt arşivleme özelliği olacaktır.

- Güvenlik duvarları ile kayıt sunucusu arasında iletişimin sağlanamaması durumunda oluşturulan kayıtlar, bağlantı sağlanana kadar güvenlik duvarının kendi üzerinde tutulabilmelidir.

- Yönetilen ağ güvenlik duvarlarına ait performans ve güvenlik duvarları üzerinden geçen trafik ile ilgili bilgileri geçmişe yönelik olarak gösterebilme özelliği desteklenecektir.

- Önerilen kayıt yönetim sistemi geçmişe yönelik olarak raporlama yapabilme özelliğine sahip olacaktır. Örneğin bant genişliği kullanımı, uygulama denetimi, URL filtreleme ile ilgili istenen tarih aralıklarında raporlar üretebilecektir.

- Tutulan kayıt alanları baz alınarak özelleştirilmiş sorgular yazılabilmeli ve bu sorguların çıktıları, tablo, pie-chart şeklinde raporlar içerisine konulabilmelidir.

- Pdf formatında rapor üretebilmeli ve üretilen raporları belirtilen e-mail adreslerine otomatik veya elle gönderebilmeli, ftp veya web sitelerine otomatik olarak yükleyebilmelidir.

- Kayıtları ftp veya benzer bir protokolle harici bir Sunucu veya Depolama alanı üzerinde yedekleme yapıp arşivleyerek kayıtların yedekliliği sağlayabilmelidir.

- Teklif edilen sistemlerin en az 1 yıl 7/24 garantisi bulunmalıdır. 1 yıl süre ile Yazılım/Firmware güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.

Log Yönetim Sistemi (SIEM)

Performans Özellikleri

- Sistem 50 Adet network cihazından(router, switch, firewall, IPS gibi) log alabilmelidir.
- Sistem 1500 EPS değerini destekleyecek şekilde lisanslanmalıdır.
- Sistem donanım olarak veya Vmware, Hyper-V, KVM gibi Sanal ortamlar üzerinde çalıştırılabilmelidir.
- Sistem SIEM özellikleri kısmında belirtilen tüm özellikleri içeren lisanslar ile tekliflendirilmelidir.
- Sistem 1 senelik destek lisansı ile tekliflendirilemelidir.

SIEM (Güvenlik ve Olay bilgisi yönetimi) özelikleri

- Önerilecek SIEM çözümü ölçeklenebilir olabilmeli ve aşağıdaki seçenekler dahilinde kurulumu yapılabilmelidir:
    - Gerektiğinde harici toplayıcılar (collector) ile log toplamak mümkün olabilmelidir.
    - Harici toplayıcılar (collector) topladığı logları korelasyon bileşenine HTTPS protokolü üzerinden gönderebilmelidir.

    - Harici toplayıcılar (collector) logları merkezi birime gönderemediği durumda ise logları kendi üzerinde tutabilmelidir.
    - Harici toplayıcılar (collector) topladığı logları gönderim öncesinde sıkıştırabilmelidir.
    - 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.
    - Harici toplayıcılar (collector) Netflow bilgisi alabilmelidir.
    - Harici toplayıcılara (collector) gelen kayıtlara (EPS) ve ip adresi sınırı konulabilmelidir.
- Önerilen SIEM 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.
- Önerilen SIEM ürünü log kayıtların toplandığı tüm sistemleri ilişkilendirilmiş bir CMDB (yapılandırma yönetim veri tabanı) sisteminde toplayabilmelidir.
- 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.
- Keşfedilen sistemlere ip/subnet seviyesinde yer(lokasyon) bilgisi girilebilmelidir. Bu bilgiler CSV dosyası olarak da import edilebilmelidir.
- Keşif esnasında SIEM sistemine girilen local SNMP community ve Windows AD kullanıcı bilgilerinin yanısıra harici kullanıcı bilgisi sağlayan sistemler (örneğin CyberArk) ile entegrasyon sağlayabilmelidir.
- SIEM sistemi Amazon AWS ve Microsoft Azure sistemlerini de uzaktan keşfedebilmelidir.
- Keşfedilen sistemlerde önemli interface, process ve port'lar seçilerek sadece kritik interface, process ve portlara ilişkin oluşacak yoğunluklar olay (incident) verisi oluşturabilmelidir.
- Keşfedilen sistemlerde istenilen disk'lerin doluluk durumu olay (incident) verisi oluşturmada hariç tutulabilmelidir.
- Gerçek zamanlı, memory üzerinde korelasyon yapabilmelidir.

- Event bilgisi sıkıştırılmış bir halde tutulmalıdır.
- İlişkisel bir veri tabanı (Oracle, MSSql gibi) üzerinde event kaydı tutmamalıdır, ilişkisel veri tabanı sadece konfigürasyon veya vaka (incident) kayıtlarının depolanması amacıyla kullanılmalıdır.
- Veri toplamak veya cihazlarla haberleşebilmek amacıyla aşağıdaki protokolleri desteklemelidir:
    - SNMP
    - WMI
    - VM SDK
    - OPSEC
    - JDBC
    - Telnet
    - SSH
    - JMX
- 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.
- SIEM 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)
- SIEM sistemi kendine kayıt gönderen sistemlerin dahil olduğu gruplanmış bir envanter sistemine sahip olmalıdır (CMDB)
- SIEM 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)
- CMDB sistemi üzerinden XML formatında raporlar export edilebilmelidir.
- SIEM sistemi güncel malware ip, malware URL, malware process bilgilerini düzenli aralıklarla merkezi sistemden güncelleyebilmelidir.
- SIEM sistemi malware hash bilgilerini merkezi sistem üzerinden veya TAXII protokolü üzerinden harici sistemlerden güncelleyebilmelidir. Ayrıca belli hash bilgilerini de whitelist olarak sınıflandırabilmelidir.

- SIEM sistemi anonymity (open proxies, tor vb.) network bilgilerini merkezi sistemden düzenli olarak yenileyebilmelidir.
- SIEM sistemi User Agent blacklist bilgilerini merkezi sistemden düzenli olarak yenileyebilmelidir ve belli User Agent'leri whitelist olarak kaydedebilmeldir.
- SIEM sistemi custom bloklu ip ve domain'leri CVS formatında import edebilmelidir.
- SIEM 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.
- Önerilen SIEM sistemi yeni cihaz ve log parser (log ayrıştırıcı) tanımlarını merkezi sistem üzerinden alarak onaylanması durumunda sisteme dahil edebilmelidir.
- Önerilen SIEM sisteminde olmayan cihazlar için log ayrıştırıcı (log parser) yöntemi bilinen bir yazım sistemi (örneğin XML) ile yazılarak sisteme dahil edilebilmelidir.
- Önerilen SIEM 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.
- Önerilen SIEM sistemi belirli dosya, konfigrasyon veya dizinlerdeki değişikliklere karşı değişiklik takibi (integrity-check) yapabilmelidir. Oluşan değişiklikler monitör edilerek alarm oluşturulabilmelidir.
- Önerilen SIEM 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.
- SIEM sistemi belirli cihazlardan gelen log kayıtlarını başka cihazlara yönlendirebilmelidir. (örneğin netflow veya snmp traps)
- SIEM sistemi bir syslog paketindeki çok satırlı syslog kayıtlarını ayrıştırabilmelidir.
- 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.
- Aşağıdaki uyumluluk süreçleri için hazır raporlar oluşturabilmelidir:
    - PCI-DSS
    - HIPAA
    - SOX
    - NERC

    - FISMA
    - ISO
    - GLBA
    - GPG13
    - SANS Critical Controls
- Takip amaçlı dashboard ekranlarına sahip olmalı slideshow görünümünde olabilmelidir
- 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
- Vaka oluşması durumunda script çalıştırma özelliği bulunmalıdır.
- API bazlı entegrasyon ile CMDB ve olay bilgileri harci ticketing sistemleri ile entegre olabilmelidir. (serviceNow, ConnectWise vb.)
- Dahili ticketing sistemi barındırmalıdır.
- Anahtar kelime bazlı arama tüm log alanlarında veya istenilen bir alan dahilinde yapılabilmelidir.
- Geçmişe yönelik arama yapılabilmesi desteklenmelidir.
- Arama yapılırken boolean filtreler, gruplamalar, zaman bazlı filtreler, regex kullanımı desteklenmelidir.
- İstatiksel profiller desteklenmelidir. Örneğin sistem network kullanımında olağan dışı bir artış olduğunu bu sayede anlayabilmeli ve alarm üretebilmelidir.
- Zamanlanmış raporların oluşturulması desteklenmelidir. Bu raporlar CSV veya PDF formatında export edilip mail ile gönderilebilmelidir.

Yönetim Özellikleri

- SIEM ürünü Web üzerinden GUI/https üzerinden yönetilebilmelidir.
- Çözüm cihazlardan toplanan envanter, performans verisi, güvenlik ile log verisinin aynı ekrandan analiz edilmesini sağlayabilmelidir.
- Multi-teanent (çok organizasyonlu) desteği olmalıdır. Bu sayede birbirinden bağımsız organizasyon konfigürasyonları ve bunlara erişen kullanıcı yetkilendirmeleri yapılabilmelidir.
- Multi-teanent (çok organizasyonlu) yapılanmada belirli sistemler ip seviyesinde ilgili organizasyona atanabilmelidir.
- Multi-teanent (çok organizasyonlu) yapılanmada
- Rol temelli yönetim desteği olmalıdır, yönetici, standart kullanıcı, sadece görüntüleme özelliklerinin yanı sıra aşağıdaki şekilde roller oluşturulabilmelidir.
    - Sadece Network sistemlerinin kayıtlarını yönetebilme
    - Sadece Windows sistemlerinin kayıtlarını yönetebilme
    - Sadece Unix sistemlerinin kayıtlarını yönetebilme
    - Sadece Güvenlik sistemlerinin kayıtlarını yönetebilme
- Kullanıcı kimlik doğrulaması local veya harici LDAP/Radius sisteminden yapılabilmelidir.
- SIEM ürünü zamanı belirlenebilen düzenli rapor bilgileri mail veya scp ile gönderebilmelidir,
- SIEM sistemi olay (incident) bilgilerini kendi üzerinde gösterebildiği gibi SNMP Trap (v1, v2c), XML https üzerinden harici sistemlere gönderebilmelidir.
- SIEM sistemi olay (incident) bilgilerini otomatik çağrı açabilen sistemlere WSDL üzerinden göndererek acil müdahale edilmesini sağlayabilmelidir.
- SIEM sistemi kendine dahil olan tünelleme uygun sistemlere gerektiğinde uzaktan tünel kurarak sisteme müdahale edebilmelidir. (ssh, wmi vb.)
- SIEM sistemi raporlarında firma logosunun konulmasına izin vermelidir.

- SIEM sistem kaynak kullanımları (memory, CPU, disk vb.) toplam ve process olarak da ayrıntılı şekilde gösterilmelidir. Aşırı artışlarda alarm oluşturulabilmelidir.
- SIEM sistemi belli zaman aralıklarında kayıtları arşivleyebilmeli ve arşivlenmiş verileri görüntülenmek üzere geri yükleyebilmelidir.
- SIEM sistemi herhangi bir tarihte oluşan herbir event'i bir checksum algoritması (örneğin sha256) üzerinden doğrulayabilmelidir

- **AĞ ERİŞİM KONTROL CİHAZI**

- Ağ erişim kontrol sisteminin lisanslama modelinin bir defalık olması (perpetual) tercih sebebidir.
- Eğer Ağ erişim kontrol sistemi abonelik lisanslama modeli ile sunuluyorsa 1 (bir) yıl süreyle ve anlık en az "300" (üçyüz) uç cihazı destekleyecek şekilde teklif edilecektir.
- Eğer Ağ erişim kontrol sistemi bir defalık lisanslama modeli ile sunuluyorsa 1 (bir) yıl bakım bedeli ve anlık en az "300" (üçyüz) uç cihazı destekleyecek şekilde teklif edilecektir.
- Ağ erişim kontrol sistemi merkezi mimaride çalışabilmeli, trafiği dinlemeden gerekli kontrol ve erişim yetkilendirmelerini yapabilmelidir.
- Ağ erişim kontrol sistemi bağlanan kullanıcı ve bağlanılan cihaz özelliklerine bağlı olarak rol bazlı erişim yetkilendirme yapabilmelidir.
- Ağ erişim kontrol sisteminde yöneticiler tarafından yapılan bütün değişimler kayıt altında tutulmalı ve raporlanabilir durumda olmalıdır.
- Ağ erişim kontrol sisteminde yöneticilerin yetkilendirmesi için yerel kullanıcı, Radius, Active Directory ve LDAP metotları desteklenmelidir.
- Ağ erişim kontrol sistemi kullanıcıları dinamik olarak farklı vlan'lara atabilmelidir. Bu hedefe ulaşmak için 802.1x protokolü desteklenmelidir. Ayrıca 802.1x desteği olmayan yönetilebilir anahtarlarda da dinamik vlan desteği bulunmalıdır.

- Ağ erişim kontrol sistemi şu güvenlik protokollerini desteklemelidir: MS-CHAP v2,PAP,EAP-MD5,EAP-PEAP,EAP-TLS
- Ağ erişim kontrol sistemi yedekli mimaride çalışmayı desteklemelidir. Aktif ve yedek bileşenler aynı ağ içerisinde bulunup ortak bir sanal IP adresini kullanabilmelidir. Ek olarak Aktif ve yedek bileşenler farklı veri merkezlerinde ve farklı ip aralıkları kullanarak da yedeklilik sağlayabilmelidirler.
- Ağ Erişim kontrol sisteminin birden fazla sistemi yönetebilecek merkezi yönetim çözümü olmalıdır. Bu sayede çözüm yatay olarak büyüyebilmelidir.
- Ağ Erişim kontrol sistemi kontrol ve uygulama işlevlerini farklı cihazlara bölerek de çalışma prensibini desteklemelidir.
- Ağ erişim kontrol sistemi istenirse donanım istenirse sanal ortamda çalışacak şekilde teklif edilebilir. Vmware ESXi ve Hyper-V sanallaştırma platformları desteklenmelidir.
- Ağ Erişim kontrol sistemi ağ'a yeni katılan ve ağda bulunan cihazları aşağıdaki metotları kullanarak profilleyebilmelidir. Bu Sayede IoT cihazlarıda otomatik olarak algılanabilecektir.
    - DHCP isteklerini inceleyerek
    - http/HTTPS isteklerine verilen cevapları inceleyerek
    - IP aralığına göre
    - Bulunduğu yere göre
    - Ajan yüklü olup olmamasına göre
    - SNMP isteklerine verdiği cevaplara göre
    - SSH/Telnet isteklerine verdiği cevaplara göre
    - TCP/UDP portlarının açık olup olmamasına göre
    - Vendor OUI bilgisine göre
- Ağ Erişim kontrol sistemi misafir ve çalışan yetkilendirmesi için misafir karşılama (captive portal) destekleyecektir. Bu captive portal ile misafirler bir sponsor izni ile sisteme dahil olabilirlerken kendi cihazlarını ofis ağına bağlamak isteyen şirket çalışanları ise Radius, ldap ve Active Directory yetkilendirmesi ile sisteme kendi cihazlarını kaydedebilmelidirler.
- Ağ Erişim kontrol sistemindeki misafir karşılama ekranları özelleştirilebilmelidir.

- Ağ Erişim kontrol sisteminin Mac adresini olduğundan farklı gösteren sistemleri algılayabiliyor olması gerekir. Bu algılama için kullanılan metotlar ve alınabilecek önlemler ayrıntılı olarak belirtilmelidir.
- Ağ erişim kontrol sistemi periyodik olarak yapılan kontrollerde başarısız olan cihazları ağdan izole edebilmelidir ve eksiklerini gideren cihazlarıda otomatik olarak geri alabilmelidir.
- Güvenlik tehdidi nedeniyle ağdan izole edilen cihazların o ana kadar kullandıkları bütün bağlantı adaptörlerinden izole edilmeleri gerekmektedir.
- Ağ Erişim Kontrol sistemi Windows uç cihazlarda ajan aracılığı ile aşağıdaki kontrolleri yapabilmelidir.
    - Windows işletim sistemi versiyon ve kritik güncelleme kontrolleri
    - Windows işletim sistemi üzerinden bağlantı paylaşımının aktif olup olmaması
    - Windows işletim sisteminde bağlantı köprülemenin aktif olup olmaması
    - Windows işletim sistemi üzerinde belirlenen programların aktif olup olmaması
    - Sertifika ve domain kontrolleri
    - Kütük versiyon ve anahtar kontrolleri
    - Windows Servislerinin çalışma durum kontrolleri
- Ağ Erişim Kontrol sistemi Linux ve MacOs-X uç cihazlarda ajan aracılığı ile aşağıdaki kontrolleri yapabilmelidir.
    - Linux ve MacOs-X işletim sistemi üzerinde belirlenen programların aktif olup olmaması
    - Linux ve MacOs-X İşletim Sistemi üzerinde dosya kontrolleri
    - Linux ve MacOs-X işletim sistemi üzerinde yazılım paketi kontrolleri
- Ağ Erişim kontrol çözümü mobil cihazların etkin kontrolü için MobileIron, Airwatch ve Zenmobile MDM çözümleri ile entegrasyonu bulunmalıdır.
- Ağ erişim kontrol sistemi oluşan alarmlarda yöneticileri e-posta ve sms aracılığı ile uyarabilmelidir.

Uç cihaz güvenliği

- Önerilen çözüm bu şartname içerisinde alınacak olan güvenlik duvarı ve loglama sistemi ile entegre olabilecektir. Bu bağlamda güvenlik duvarına gerçek zamanlı kullanıcı bilgisini ve loglama sistemine log gönderebilecektir.

- Çözüm 4000 kullanıcı için lisanslanmış olmalıdır.
- Uç cihazların gerçek zamanlı durumunu gözleyebilmelidir.
- Uç cihazların güvenlik zaafiyetleri konusunda bilgi veren ekranları bulunmalıdır.
- Uç cihaz güvenlik yazılımı aşağıdaki işletim sistemlerini desteklemelidir.
    - Windows 7 ve üzeri
    - Microsoft Windows Server 2008 R2 ve üzeri
    - Macos 10.12 ve üzeri
    - Android
    - IOS
    - Linux

- Windows ve Mac işletim sistemleri için aşağıdaki özellikler desteklenmelidir.
        - Güvenlik zaafiyetine sebebiyet olabilecek yazılım versiyonları hakkında bilgi verme
        - Antivirüs kontrolü
        - Web filtreleme
        - Uygulama kontrolü

- IOS,Android,Windows ve Macbook platformaları için ssl vpn ve ipsec vpn istemcisi olarak çalışabilmeldir.
- Uç cihazlar sıfırıncı gün ataklarına karşı kullanılan sandbox sistemleri ile entegre olabilmelidir. Sandbox sistemlerine dosya gönderebilmeli Sandbox sistemlerinden gelen gerçek zamanlı imzaları değerlendirebilmelidir.
- Teklif edilen sistemlerin en az 1 yıl yazılım garantisi bulunmalıdır. 1 yıl süre ile Yazılım/Firmware güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.

Veritabanı Güvenlik Duvarı

- Veritabanına yapılabilecek gerçek zamanlı saldırıları algılama.
- Siber saldırılarla ilgili kötü amaçlı faaliyetlerin bildirilmesi ve uyarılması için sürekli, gerçek zamanlı izleme ve veritabanı etkinliğinin analizi, uyarılması ve raporlanması.
- Ayrıcalıklı kullanıcı ile uyumlu olmayan erişim hareketlerinin sürekli takip edilerek Kim, Ne, Ne Zaman, Nerede ve Nasıl sorularının cevaplanması.
- Birçok dahili rapor ve analiz tesisi.
- Konsol, e-posta veya diğer sistemlere yönelik uyarıları yapılandırma.
- SYSLOG, SNMP ve Veritabanı bağlantıları sayesinde uyarıları kaydetme ve başka sistemlere aktarma.
- Bağlantı engelleme ve yüksek profil uyarısı dahil, olayların özelleştirilebilir şekilde ele alınması.
- Politika ihlallerine ve şüpheli davranışlara otomatik tepkiler oluşturma.
- Kullanıcı oturumunu kapatma, hesap kilitleme veya özelleştirilmiş aksiyon yazma desteği.
- Veritabanı güvenlik olaylarına ve hareketlere göre detaylı raporlama.