

**ÜSKÜDAR ÜNİVERSİTESİ**

**YILLIK LİSANS ve EK ALIM PROJE ŞARTNAMESİ**

**2022**

**İÇİNDEKİLER**

1. **SERVER STORAGE TEKNİK ŞARTNAMESİ**
   1. VMWARE LİSANS YENİLEMELERİ
   2. VERITAS LİSANS YENİLEMELERİ
   3. SUNUCU VE DEPOLAMA BİRİMİ BAKIM DESTEK GEREKSİNİMLERİ
   4. BÜTÜNLEŞİK ALTYAPI TEKNİK ÖZELLİKLERİ - EŞLENİK İKİ LOKASYON - (Toplam 8 Node)
   5. BÜTÜNLEŞİK ALTYAPI İÇİN ANAHTAR MODÜLLERİ - EŞLENİK 2 LOKASYON (Toplam 4 Adet)
   6. YEDEKLEME ÇÖZÜMÜ TEKNİK ÖZELLİKLERİ
   7. YEDEKLEME ÇÖZÜMÜ YAZILIM TEKNİK ÖZELLİKLERİ

1. **NETWORK TEKNİK ŞARTNAMESİ**
   1. OMURGA ANAHTAR CİHAZI (4 ADET)
   2. KENAR ANAHTAR CİHAZI (2 ADET)
   3. AĞ ÜRÜNLERİ EK ALIM VE LİSANS YENİLEME
2. **BİLGİ GÜVENLİĞİ TEKNİK ŞARTNAMESİ**
   1. BİLGİ GÜVENLİĞİ ÜRÜNLER YENİ ALIM YAPILACAK ÇÖZÜMLER
   2. TRELLİX LOG YÖNETİM YAZILIMI YENİLEME
   3. SUNUCU ve UÇ NOKTA GÜVENLİĞİ ÇÖZÜMÜ
   4. AĞ TABANLI ATAK ÖNLEME SİSTEMİ
   5. ATAK TESPİT ve KORUMA TEKNİKLERİ
   6. YÖNETİMSEL VE RAPORLAMA ÖZELLİKLERİ
   7. VERİ SIZINTISI ENGELLEME YAZILIMI
   8. TRELLİX LOG YÖNETİM YAZILIMI LİSANS ALIMI
   9. VERİ TABANI GÜVENLİĞİ ÇÖZÜMÜ YENİ ALIMI
   10. CRYPTTECH HOTSPOT YAZILIMI LİSANS YENİLEMELERİ
   11. F5 YÜK DENGELEME YAZILIMI LİSANS YENİLEME
   12. AĞ GÜVENLİK CİHAZLARI YENİLEME
   13. ALDATMA PLATFORMU ( DECEPTION) YAZILIMI YENİ ALIMI
   14. ÇOK FAKTÖRLÜ KİMLİK DOĞRULAMA YAZILIMI
   15. UÇ NOKTA TEHDİT ALGILAMA VE YANIT YAZILIMI
   16. BİLGİ GÜVENLİĞİ ÜRÜNLERİ TEKNİK OPERASYON SÜREÇ KAPSAMI
   17. BİLGİ GÜVENİĞİ, YÜKLENİCİNİN PERSONEL YETKİNLİKLERİ KAPSAMI
3. **MICROSOFT VE ADOBE LİSANSLARI TEKNİK ŞARTNAMESİ**
   1. MICROSOFT LİSANS YENİLEMELERİ VE YENİ LİSANS ALIMLARI
   2. ADOBE LİSANS YENİLEMELERİ
4. **SOLIDWORKS LİSANS YENİLEMELERİ**
5. **DEEPFREEZE LİSANS YENİLEMELERİ**
6. **EXCLAIMER LİSANS YENİLEMELERİ**
7. **XMEDIUS FAX SERVER BAKIM YENİLEMELER**
8. **TEKNİK VE YÖNETİLEN HİZMETLER TEKNİK ŞARTNAMESİ**
   1. YÖNETİLEN HİZMETLER
   2. BAKIM ANLAŞMASI
9. **DİĞER KONULAR**
   1. TANIMLAR
   2. PROJE ESNASINDAKİ SLA SEVİYELERİ VE DİĞER HİZMET PARAMETRELERİ
   3. YEMEK VE ULAŞIM
   4. TEKLİF PARA BİRİMİ
10. **FİNANSAL BİLGİLER**
    1. TEKLİF, ZAMAN TABLOLARI VE KABUL ŞARTLARI

# **Giriş ve Amaç**

Üsküdar Üniversitesi, Türkiye’nin yeniliğe açık, eğitim sektöründe markalaşmayı önem veren bir “Kurum” dur. Bu kurum, verdiği eğitimin kalitesi ile diğer tüm kurumlardan ayrışmakta ve yetiştirdiği insanlar ile ülkemizin iyi bir yere gelmesinde önemli bir rol oynamaktadır.

Bu önemli misyonu gereği kurumun verdiği eğitim, eğitimin ve bilginin sunumu, bilgiye erişim ve bilginin korunması gibi normal kurumlardan farklı davranması gereken bazı konular bulunmaktadır.

Üsküdar Üniversitesi bilgiyi hem öğrencilerine sunmakta hem de kurum içinde hizmet kalitesi ve iç işleyişinin devamlılığı için kurum bünyesinde kullanmaktadır.

Üsküdar Üniversitesi bilgiyi sakladığı sunduğu sistemleri yenileme, iyileştirme ve bu altyapı ile ilgili ek ve bütünleyici hizmet ve ürün satın almaya dönük olarak bu şartnameyi oluşturmuştur.

# **Projenin Açıklaması ve Ön Kabuller**

Proje; kurumun altyapısındaki yazılım, sistem, sunucu, ağ yapısı gibi birçok noktaya hizmet veren servislerde yenileme, iyileştirme, kurulum, göç (migration) çalışmalarını içermektedir. Bu projede aşağıda teknik detayları verilen hizmetin alınması planlanmaktadır. Bununla birlikte şartnamenin genelinde belirtilen teknik detaylardan bağımsız olarak aşağıdaki şartların sağlanması olmazsa olmazdır.

* + Kurum, istediği şartlarda ve teknik özelliklerde değişiklik yapma hakkına veya bu projeyi komple iptal etme hakkına sahiptir. Bu değişikliği İstekli’lere bildirmek Kurum’un kendi insiyatifindedir.
  + Kurum, gelen tekliflerdeki tüm kalemlerde hizmet almak yerine parçalı satın almayı da tercih edebilir. İstekli bunu peşinen kabul etmiş sayılır.
  + Çözüm için önerilecek hizmet detayları, uluslararası ve yerel tüm standartlara üretici en iyi pratiklerine, sektör en iyi pratiklerine, gerek güvenlik, gerek performans tüm açılardan uyumlu olmalıdır. Standart dışı hiç bir yaklaşım, çözümlerde kullanılmamalıdır.
  + İstekli, teklif vermeden önce çalışma yapılacak yeri ve sistemleri görebilir. Görmeden vereceği tekliflerin tamamında doğacak herhangi bir zarar ve ortaya çıkan bir eksikten İstekli ve eğer teklifi kabul olmuş ise “Yüklenici” sorumlu olacaktır.
  + Çözümlerin bileşenlerinde hiçbir tek-hata-noktası (single-point-of-failure) olmamalıdır. Yani sistemdeki herhangi bir bileşende yaşanacak herhangi bir sorun, mutlak suretle sistemin kendi içindeki bileşenler ile telafi edilmeli ve sistem çalışır halde olabilmelidir. Aksi mümkün değilse İstekli, sunacağı teklif içeriğinde bunu net olarak belirtmelidir.
  + Sistemin çalışabilmesi için gerekli olan tüm lisanslar, çözüm ile birlikte verilmelidir.
  + Sistemin çalışabilmesi için gerekli olan tüm bağlantı kabloları, kartlar, ek modüller vb. çözüm ile birlikte eksiksiz bir şekilde verilmelidir.
  + Aşağıda teknik detayları verilmiş bileşenlerin, birbirlerinden fiziksel olarak ayrı veya tek bir bütünsel yapıda olması, hedeflenen performans ve kapasite değerleri yakalandığı sürece Kurum tarafından aynı değerlendirilecektir. Hem geleneksel hem de bütünleşik çözümleri içerecek şekilde üretilmiştir.
  + Üsküdar Üniversitesinin belirttiği şekilde ürünlerin kurulum ve montajları eksiksiz olarak Yüklenici tarafından yapılacaktır.

# **Genel Koşullar**

Bu ihale kapsamındaki işlerde Yüklenici ile Kurum arasında “GİZLİLİK” anlaşması yapılacaktır. Kapsam Kurum tarafından belirlenecektir.

Yüklenici, proje kapsamında Kurum tarafından belirlenen standart prosedürlere ve yönergelere uyumlu olacak şekilde hizmet verecek ve kayıtları Kurum’un göstereceği elektronik ortamda saklayacak, istendiğinde Kurum’a sunacaktır.

Yüklenici, kurumun talep ettiği ISO27001, ISO9001:2015 ve ISO20000-1:2011 sertifikasyonlara sahip olan firmalar tercih sebebidir.

Yüklenici, bu “Şartname” ve eklerinde belirtilsin veya belirtilmesin alacağı ve uygulayacağı kararlarda Kurum’un onayını alacaktır. Kurum, yazılı olmak kaydı ile yapılacak işlemler için süreçleri Yüklenici’ye devredebilir.

Yüklenici, çalışmalar sırasında sistemin kesintiye uğramaması için gerekli önlemleri alacak ve müdahaleye başlamadan önce Kurum’u bilgilendirecektir.

İstekli, teklif edeceği ürünlerle ilgili (Donanım, yazılım, lisans, Microsoft, Vmware, Veeam) üreticisinden veya yetkili distribütöründen bu ihale için alınmış şartname kapsamında teklif edilen ürünleri satmaya, kurmaya ve teknik desteğini vermeye yetkili olduklarını gösterir İstekli adına düzenlenmiş yetki belgelerini teklif ile birlikte Kurum’a sunacaktır.

Belirtilen ürün ve hizmetlerin bir bütün olarak çalışması için gerekli her türlü ek/yardımcı donanım ve hizmet Yüklenici tarafından sağlanacaktır. Sadece geçiş ve kurulum için gerekli olan ve geçiş sonrasında Kurum’un ihtiyacı olmayacak bir bileşen var ise onu da Yüklenici karşılayacaktır.

Tüm ürünler (donanım, yazılım, lisans vb.) yeni, kullanılmamış, hasarsız ve eksiksiz olarak, orijinal paketinde işin yapılacağı yere getirilecektir.

Projede kullanılacak olan tüm ürünlerin birbirleriyle uyumluluğu gözetilecektir. Projede öngörülen uygulamalarda ürünlerin herhangi bir nedenle (sürüm, standart uyuşmazlığı vb.) ortaya çıkan uyum sorunlarının giderilmesi yükümlülüğü Yüklenici’ye aittir.

Her türlü malzeme temini, işçilik ve uyumu Yüklenici sağlayacaktır. Bu şartnamede tarif edilmeyen ama sistemin çalışması için zorunlu olan tüm tamamlayıcı parçalar Yüklenici tarafından ücretsiz bir şekilde temin edilecek ve monte edilip çalışır hale getirilecektir.

Temin ve teslim edilecek her türlü malzemenin nakliye, taşıma, sigorta, geçici depolama sorumluluğu ve bunlara bağlı her türlü masraf, Yüklenici tarafından karşılanacaktır. Teslim ve kurulum yeri Kurum lokasyonudur.

Kurum, gerekli görmesi durumunda, kullanılacak ürünlerden numune isteyebilir veya Yüklenici’nin benzer ürünleri sattığı, hizmetleri sunduğu bir veya birkaç yerde yerinde inceleme yapmak isteyebilir. Yüklenici, talep edilmesi halinde bu istekleri yerine getirecektir.

İstekli teklifinde kullanacağı tüm cihazlar, malzemeler ve donanımlara ait marka ve modellerini liste halinde ve yoruma mahal bırakmayacak detayda (isim, ürün kodu, marka, model, alt model, bileşen detayı vb.) sunacağı teklif dökümanında yer verecektir.

Belirtilen tüm ürünler, kurulumu yapıldıktan sonra anahtar teslimi çalışır vaziyette teslim edilecektir.

İstekli, “Şartname”deki tüm maddeleri ayrı ayrı cevaplayacaktır. Hiçbir madde boş bırakılmayacak, cevaplar açık, anlaşılır, yeterli teknik düzeyde olacaktır. Sadece “**okunmuş, anlaşılmış ve kabul edilmiştir**” şeklinde verilen cevaplar kabul edilmeyecektir. Cevapların olması gereken yerde olmayışının ve/veya bulunamayışının ve bu nedenle değerlendirme yapılamamasının sorumluluğu teklif verene aittir.

Yüklenici, projelerde risk yönetimi uygulayacaktır. Proje boyunca yaşatacağı ve güncelleyeceği risk dokümanı ile olası risk, kesinti ve aksaklıklar için proaktif tedbir alınmasını sağlayacaktır. Risk yönetimi yaklaşımını Kurum, Yüklenici’ye iletecek ve gerekli doküman/şablon vb. Yüklenici ile paylaşacaktır.

Yüklenici, bu ihale kapsamındaki tüm çalışmalarında gerekiyor ise mesai saatleri dışında da (akşam, hafta sonu gibi) çalışacaktır.

Yüklenici, projenin her aşamasından sorumlu, bir proje yöneticisi belirleyecektir. Bu kişiye tatil günleri dâhil 7/24 ulaşılabilecektir.

Tüm çalışmalar için taslak proje planı ve süre, teklif ile birlikte kuruma sunulmalıdır.

Tüm çalışmalar aşağıdaki fazlardan geçerek uygulanacaktır. Aşağıdaki maddeler, bütünsel projenin her bir alt projesi için ayrı ayrı uygulanacaktır.

* + Kapsam ve Vizyon
  + Planlama
  + Geliştirme
  + Kararlı Hale Getirme
  + Yaygınlaştırma
  + On-the-job training

Tüm çalışmalarda (her bir proje/danışmanlık için ayrı ayrı olacak şekilde) aşağıdaki dokümanlar üretilmeli ve teslim edilmelidir.

* + Kapsam ve Vizyon dokümanı
  + Proje planı (Sürekli güncellenecek – mpp ve xlsx formatlarında)
  + Risk dokümanı (Sürekli güncellenecek)
  + Analiz dokümanı
  + Planlama ve tasarım dokümanı
  + Geçiş esnasında gerekecek prosedürler ve kontrol listeleri
  + Haftalık ilerleme durum raporu

Tüm çalışmalarda aşağıdaki durumlarda toplantı yapılması gerekecektir.

* + Alt proje başlangıçlarında
  + Kriz anında
  + Tasarım ve geçişlerde gerektiği zaman
  + Kurum talep ettiği zaman

# **İhtiyaç**

Yüklenici, Kurum’a aşağıdaki ihtiyaçlar doğrultusunda çözüm önerecek ve kabulü ardından bunun uygulamasını yapacaktır.

# **SERVER STORAGE TEKNİK ŞARTNAMESİ**

* 1. **VMWARE LİSANS YENİLEMELERİ**

### Üsküdar Üniversitesi bünyesinde kullanılmakta olan vmware lisanslarının yenilemeleri yapılacaktır.

### Lisans yenilemeleri 1 yıl olarak yapılacaktır

### Yenileme yapılacak kontratlar aşağıdaki şekilde olmalıdır.

### Kontrat No: 494075402

### Kontrat No: 439408110

### Kontrat No: 41762141

### Kontrat No: 41762190

### Kontrat No: 41874973

### Kontrat No: 4126142663

### Kontrat No: 4105483375

* 1. **VERITAS LİSANS YENİLEMELERİ**

### Üsküdar Üniversitesi’nde kullanılmakta olan aşağıdaki lisansların yenilemeleri yapılacaktır:

### 10 adet ENTERPRISE VAULT EMAIL MGMT

### 600 adet ENTERPRISE VAULT ARCHIVE DISCOVERY

### Yenileme 1 yıl Essential (7x24) seviyesinde olmalıdır.

|  |  |
| --- | --- |
| ESSENTIAL 12 MONTHS RENEWAL FOR ENTERPRISE VAULT ARCHIVE DISCOVERY 1 USER ONPREMISE STANDARD PERPETUAL LICENSE ACD | 600 |
| ESSENTIAL 12 MONTHS RENEWAL FOR ENTERPRISE VAULT EMAIL MGMT 1 USER ONPREMISE STANDARD PERPETUAL LICENSE ACD. | 10 |

* 1. **SUNUCU VE DEPOLAMA BİRİMİ BAKIM DESTEK GEREKSİNİMLERİ,**

### DELL Donanım Support Yenilemeleri

### Aşağıda aktif kullanılan cihazların 1 yıl donanım dahil support yenilemeleri yapılacaktır.

|  |  |  |
| --- | --- | --- |
| VNX5400 | 1 | VNX 5400 Bakımı |
| VNX5400 | 1 | USKUDAR UNIVERSITESI VNX 5400 Bakımı |
| VNX5200 | 1 | USKUDAR UNIVERSITESI VNX 5200 Bakımı |
| VNX5300 | 1 | USKUDAR UNIVERSITESI VNX 5300 Bakımı |
| DD2500-36TB-B | 1 | DD2500 Bakımı |
| C-ES30-30S-B | 1 | DD2500 Shelf Bakımı |
| DD2500-36TB-B | 1 | USKUDAR UNIVERSITESI DD2500 Bakımı |
| C-ES30-45S-B | 1 | USKUDAR UNIVERSITESI DD2500 Shelf Bakımı |
| L-MC-BASE | 1 | DD Base lisans supportu |
| L-MC-BASE | 1 | USKUDAR UNIVERSITESI DD Base lisans supportu |
| DS-300B 8/24P 8G BASE SWITCH | 1 | San switch supportu |
| DS-300B 8/24P 8G BASE SWITCH | 1 | San switch supportu |
| VNX5300 DPE; 15X3.5 DRV FD IN 8X600 15K | 1 | USKUDAR UNIVERSITESI VNX 5300 Bakımı |
| SC5020F | 1 | SC COMPELLENT STORAGE SUPPORTU |
| SC5020 | 1 | Üsküdar Üniversitesi SC Compellent storage supportları |
| SC420 | 1 | Üsküdar Üniversitesi SC Compellent storage supportları |

### HPE Donanım Support Yenilemeleri

### Aşağıda aktif kullanılan cihazların 1 yıl support yenilemeleri yapılacaktır.

|  |  |  |
| --- | --- | --- |
| **1 YIL - HPE TechCare Essentials SVC** |  |  |
| HP BL460c Gen9 10Gb/20Gb FLB CTO Blade | 6 | Üsküdar Üniversitesi HPE Blade serverların support yenilemeleri |
| HP BLc7000 CTO 3 IN LCD Plat Enclosure | 1 | Uskudar Universitesi Blade Şase supportu |
| HP DL380p Gen8 8-SFF CTO Server | 1 | Güney DC Sunucusu supportu |
| HP DL580R07 (E7) CTO Server | 2 | ESX Sunucu supportu |
| HP DL360e Gen8 8SFF CTO Server. Etiler - Feneryolu | 2 | Feneryolu DC supportu |
| HP DL160 G6 8 SFF Hot Plug CTO Server | 1 | DNS Sunucusu supportu |
| HP DL160 G6 8 SFF Hot Plug CTO Server | 1 | DC Sunucusu supportu |
| HP DL180 G6 CTO Server | 1 | Backup Sunucu supportu |
| **HPE Techcare Critical SVC** |  |  |
| HP DL560 Gen8 CTO Server | 1 | Server bakımları |
| HP DL560 Gen8 CTO Server | 1 | Server bakımları |
| HP DL560 Gen8 CTO Server | 1 | Server bakımları |
| HP DL560 Gen8 CTO Server | 1 | Server bakımları |
| **HPE Techcare Basic SVC** |  |  |
| HPE DL380 Gen9 8SFF CTO Server | 1 | Server bakımları |
| HPE DL380 Gen9 8SFF CTO Server | 1 | Server bakımları |
| HPE DL380 Gen10 8SFF CTO Server | 1 | Server bakımları |
| HPE DL380 Gen10 8SFF CTO Server | 1 | Server bakımları |

* 1. **BÜTÜNLEŞİK ALTYAPI TEKNİK ÖZELLİKLERİ - EŞLENİK İKİ LOKASYON - (Toplam 8 Node)**

### Teklif edilen ürün ve ürüne ilişkin bileşenler yenilenmiş, tamir görmüş olmayacaktır. Ürün ve ürüne ait bileşenler yeni ve kullanılmamış olacaktır.

### Bütünleşik Sistem her bir lokasyon için en az 4 uçtan (Node) oluşmalıdır.

### Bütünleşik Sistem veri işleme ve depolama görevlerini tek bir altyapıda birleştirecek ve tek bir noktadan yönetilebilecek donanım ve yazılımdan oluşan bir bütün olacaktır.

### Teklif edilecek bütünleşik altyapı fiziksel sunucular üzerine atanmış diskleri sanallaştırarak küme yapısı üzerinde bunları ortak bir veri depolama kaynağı olarak gösterecektir. Veri depolama sanallaştırması sunucu sanallaştırma yazılımının bir süreci (process) olarak çalışacak, ve bu sayede bütünleşik altyapı olarak çalışmak için herhangi bir sanal makina kurulmasına ve bu makinelere kaynak atanmasına gerek duymayacaktır.

### Sistem en az teklif edilen sunucu, işlemci, bellek, veri depolama disk ve toplam alanı kapasite için gerekli olan tüm lisanslar ile birlikte teklif edilecektir.

### Teklif edilecek bütünleşik altyapı çözümü, yönetim yazılımı, sunucu ve veri depolama donanımı ile birlikte bütünleşik altyapı üreticisi tarafından bir ürün olarak desteklenecektir. Virtual SAN Ready Node veya benzeri yöntemlerle bir araya getirilmiş çözümler kabul edilmeyecektir.

### Teklif edilecek bütünleşik altyapı çözümde, tüm uçlar sanallaştırma ve veri depolama işlemleri için kullanılacaktır. Sadece sanallaştırma yapan veya sadece veri depolama işlemleri için kullanılan uç modelleri kabul edilmeyecektir.

### Teklif edilecek bütünleşik sistemlerde, en az 1600W gücünde, Titanium sertifikalı 1+1 yedekli güç ünitesi bulunacaktır.

### Teklif edilen bütünleşik altyapı, herhangi bir markaya ait ağ bağlantı cihazına (network switch) bağımlı ve/veya bağımsız olmadan çalışmalıdır.

### Teklif edilen bütünleşik altyapının gelecekte genişlemek için eklenebilecek uç noktalar sistemi kesintiye uğratmadan eklenebilmeli ve sistem büyütülebilmelidir.

### Teklif edilecek yönetim yazılımı, bütünleşik altyapı üreticisi tarafından teklif edilecek çözüm mimarisi için geliştirilmiş olacaktır.

### Teklif edilecek yönetim yazılımı, sanallaştırma ortamının kurulumu için gerekli tanımlamaların yapılacağı ekranlara sahip olup, sanallaştırma altyapısının kurulumu, sisteme yeni sunucu eklenmesi, mevcut disk ve ağ donanımların yenilenmesi, ağ ve veri depolama katmanları ile ilgili yönetimi otomatize edilmiş tanımlamalara sahip olacaktır.

### Teklif edilecek yönetim yazılımı, sanallaştırma yönetim yazılım ile entegre çalışacaktır.

### Teklif edilecek yönetim yazılımı, yönetimi altındaki tüm sistemlerin, şasileri ve makinelerin sağlık durumları ile ilgili bilgi ekranlarına sahip olacaktır. Bunlarla ilgili veri depolama, işlemci ve bellek kullanımları ile ilgili bilgi ekranlarına sahip olacaktır. Sunucu makinelerin diskleri ve ağ portları ile ilgili sağlık durumu bilgileri verebilmelidir.

### Teklif edilecek uçlar üzerinde en az 2 adet işlemci yuvası bulunacaktır.

### Teklif edilecek her uç üzerinde, en az 2 (iki) adet Intel Xeon Gold serisi, her biri en az 3.0 GHz hızında, en az 24 çekirdekli, en az 35.75 MB L3 önbellekli işlemciler bulunacaktır.

### Teklif edilecek her uç üzerinde toplamda en az 1024GB bellek kapasitesi ile teklif edilecektir. Teklif edilecek bellekler en az 64 GB DIMM’ler şeklinde ve her bir bellek modülü en az 3200 MHz hızında DDR4 bellekler olacaktır.

### Teklif edilecek her uca atanmış olarak çalışan ve çalışma esnasında sökülüp takılabilen en az 10 adet disk yuvası bulunacaktır.

### Teklif edilecek her uç için en az 3.84TB kapasitede 10 adet SSD SATA disk bulunacaktır.

### Teklif edilecek her uç için en az 2 adet 1.6TB SSD cache verilmelidir. Verilmemesi durumunda herbir node üzerindeki şartnamede talep edilen bellek(DRAM) miktarı (veri depolama yönetimi için kullanılanacak olan sanal makine kaynakları haricinde) en az 4 katı olarak teklif edilmelidir.

### Teklif edilecek her uç için en az 2 adet iki portlu 10/25 Gbps hızında fiber ağ portu bulunacaktır.

### Teklif edilen uçların şartnamede belirtilen ağ anahtarları ile bağlantılarının sağlanması için gerekli kablolar teklif edilecektir.

### Teklif edilecek sunucular üzerinde USB, VGA port çıkışları bulunacaktır.

### Teklif edilecek bütünleşik sistem üzerinde herhangi bir (1) uç arızasına karşı veri koruma yöntemi kullanılarak yapılandırılmış 100 TiB (1KB=1024B) net kullanılabilir alan sağlanacaktır. Bu alan hesaplanırken tekilleştirme ve sıkıştırma gibi veri azaltma fonksiyonları ile kazanılabilecek alanlar değerlendirilmeyecektir. Uç yedekliliği hesaplandıktan sonra hiper bütünleşik sistemler kümesinde görülecek alandır.

### Sistem iki farklı lokasyonda aktif/aktif çalışma özelliğini desteklemelidir. Eğer bunu desteklemiyorsa talep edilen net kapasitenin en az %25 oranında fazlası teklife dahil edilmelidir.

### Teklif edilecek sunucu üzerinde yukarıda belirtilen adetlerde bileşenlerin sağlanamaması durumunda, toplam adedi yukarıda belirtilenden az olmamak kaydıyla ilave uç sunucularla gerekli kapasiteler sağlanabilir.

### Bütünleşik altyapı ile birlikte gerekli olan VSAN Enterprise sanallaştırma lisansları CPU bazlı olacak şekilde teklife dahil edilecektir.

### İlk lokasyon için 4 node’u destekleyecek şekilde yeni vSphere Enterprise Plus lisansı teklife dahil edilecektir. İkinci lokasyonda mevcut lisanslar kullanılacağı ikinci lokasyon için yeni lisans teklif edilmeyecektir.

### Teklif edilen bütünleşik altyapının teklif edilen sanallaştırma katmanı limitasyonları haricinde büyüyebilme limitasyonu bulunuyorsa teklifte belirtilmelidir.

### Teklif edilecek sanallaştırma yazılımı, güvenli, kararlı ve yüksek performanslı sanallaştırma (hypervisor) katmanı içermelidir.

### Sanallaştırma yazılımı, misafir işletim sistemi (Guest OS) olarak Windows Server 2008/2012/2016 Datacenter, Windows 8/10 Enterprise, SUSE Linux Enterprise Server 9 SP4, RedHat Enterprise Linux 5/6/7, Sun Solaris 10/11, Oracle Linux 6/7, CentOS 6/7, FreeBSD 8/9, Debian GNU/Linux 6, Apple OS X Server 10.10/10.1 ve Amazon Linux 2 işletim sistemlerini desteklemelidir.

### Sanallaştırma yazılımı, SAN, yazılımsal/donanımsal iSCSI ve NFS protokollerini kullanan veri depolama sistemlerini desteklemeli ve bu protokolleri kullanarak sisteme disk tanımlaması yapılabilmelidir.

### Sanallaştırma yazılımı, sanal makinalar çalışır durumda iken işlemci, bellek, disk ve ağ adaptörü eklenmesine olanak sağlamalıdır.

### Sanallaştırma yazılımı, sanallaştırma sistemi içerisinde tanımlanmış lokal ya da ortak depolama alanları arasında sanal disklerin yerlerini herhangi bir kesinti yaşatmadan değiştirebilmeye olanak sağlamalıdır.

### Teklif edilecek sistemdeki sanallaştırma çözümü, sanal makine yaratma, silme, güncelleme, anlık görüntü (snapshot), klon ve konsol görüntüsü alma özelliklerine sahip olacaktır.

### Teklif edilecek sistemdeki sanallaştırma çözümü, sanal makineler ve fiziksel ortam ile ilgili performans bilgilerini yönetim yazılımı üzerinden gösterecektir ve analiz ekranlarına sahip olacaktır.

### Teklif edilecek sistemdeki sanallaştırma çözümü, replikasyon özelliğine sahip olacaktır.

### Teklif edilecek sistemdeki sanallaştırma çözümü, kullanıcı bazlı erişim yetkilendirme özelliğine sahip olacaktır.

### Teklif edilecek veri depolama sanallaştırma yazılımı, fiziksel sunucular üzerinde atanmış diskleri sanallaştırarak cluster yapısı üzerinde bunları ortak bir veri depolama kaynağı olarak gösterecektir.

### Teklif edilecek veri depolama sanallaştırma yazılımı, verileri atanacak politikalar çerçevesinde Erasure Coding RAID-5 dağıtık olarak “inline” çalışacak şekilde depolama yapmalıdır. RAID-5 dağılımı aktif veri üzerinde sağlanmalıdır.

### Teklif edilen veri depolama sanallaştırma yazılımı ilerideki büyümeleri desteklemesi için tek bir kümede (cluster) en az 64 adet fiziksel ucun üzerinde atanmış diskleri sanallaştırabilmelidir. Veri depolama sanallaştırma yazılımı 64 adet fiziksel uç üzerinde atanmış diskleri sanallaştıramıyorsa desteklediği teknik detayları teklifte belirtilmelidir.

### Teklif edilecek veri depolama sanallaştırma yazılımı, tekilleştirme ve sıkıştırma özelliklerini desteklemelidir. Teklif edilen çözüm bütünleşik altyapı olarak çalışmak veya tekilleştirme ya da sıkıştırma işlemleri için PCIe kartları gibi özel donanımlar içeriyorsa kartın arızası durumunda sistemin çalışma yöntemi teklif ile birlikte detaylı şekilde iletilecektir.

### Performans darboğazı yaşanmaması ve talep edilen kaynakların verimli kullanılabilmesi adına teklif edilecek altyapı mimarisinde veri depolama sanallaştırma işlemini gerçekleştirme amacı ile ayrıca bir yönetim sanal makinası (Örneğin: Virtual Storage Appliance, Controller VM, Virtual Controller, Data Platform Contoller)’ kurulmayacak ve kullanılmayacaktır. Veri depolama sanallaştırma yazılımı sanal makinelerin çekirdeğinde (kernel) çalışacaktır.

### Teklif edilecek bütünleşik sistem mimarisinin, verilerin güvenliğini sağlaması için aşağıdaki özelliklerde replikasyon yazılımı verilecektir.

### Teklif edilen replikasyon çözümü, teklif edilen bütünleşik altyapı ile aynı üretici ya da sanallaştırma yazılımı üreticisi tarafından üretilmelidir.

### Teklif edilen replikasyon çözümü, teklif edilen bütünleşik altyapıdan herhangi bir üreticinin sunucuları üzerinde çalışan, aynı marka sucunu sanallaştırma yazılımı kullanan ortamlara replikasyon yapabilmelidir.

### Replikasyon yazılımı, teklif edilecek bütünleşik sistemde çalışacak tüm sanal makinaları , destekleniyorsa senkron , desteklenmiyorsa asenkron replikasyon yapacak şekilde lisans ile teklif edilecektir.

### Teklif edilecek replikasyon yazılımı uzak lokasyonlara replikasyon yapmayı destekleyecektir.

### Teklif edilecek replikasyon yazılımı, veri depolama sanallaştırma yazılımı ve/veya sanallaştırma yönetim yazılımı ile tam entegre çalışacaktır.

### Teklif edilecek sistem içerisindeki tüm donanım ve yazılımlar 3 yıl 7x24 destek alacak şekilde yerinde üretici garanti destek paketi ile teklif edilecektir.

### Teklif edilecek sistem ile ilgili online destek araçlarına 3 yıl boyunca 7x24 erişebilecektir.

* 1. **BÜTÜNLEŞİK ALTYAPI İÇİN ANAHTAR MODÜLLERİ - EŞLENİK 2 LOKASYON (Toplam 4 Adet)**

### Anahtar Modüler Şasi veya Standalone/Fixed mimaride teklif edilebilir. Birden fazla anahtarın yığınlanarak oluşturulduğu Stack mimarisi çözümler kabul edilmeyecektir.

### Ağ anahtarı lokasyon başına 2 adet olarak teklif edilecektir.

### Ağ anahtarı üzerinde en az 48 Adet SFP28 yuva bulunmalıdır. Bu yuvalar 1, 10 ve 25 Gbps hızlarını desteklemelidir.

### Anahtar üzerine en az 48 adet 25GBase-SR veya 25GBaseLR transceiver modül takılabilmelidir.

### Bu portlar için 12 adet en az 3 mt. passive copper DAC kablo teklif edilmelidir.

### Anahtar’ın en az 6 adet 40/100 Gbps QSFP28 portu olmalıdır.

### Bu portlar için en az 2 adet 40GbE QSFP+ SR Transceiver ve 2 adet en az 2mt 100GbE Copper DAC kablo teklif edilmelidir.

### Cihaz IO to PSU hava akışına sahip olmalıdır. Hava akışı ön IO modulünden güç kaynağı yönüne doğru olmalıdır.

### Cihaz yedekli çalışabilen ve hot-swap özellikli en az 2 adet AC güç kaynağına sahip olmalıdır.

### Cihaz fanları yedekli yapıda ve çalışırken sökülüp takılabilir mimaride olmalıdır.

### Cihazın backplane kapasitesi 4 Tbps değerinden az olmamalıdır.

### Cihazın data iletim kapasitesi 2.4 Billion pps değerinden az olmamalıdır.

### Adres tablosunda en az 160.000 adet MAC adresi desteği olmalıdır.

### Yönlendirme tablosunda en az 256.000 adet yön bilgisi tutulabilmelidir.

### Birden fazla konfigürasyon dosyası tutulması için yeterli Flash bellek ile teklif edilmelidir.

### Cihazın işletim sisteminin güncellenmesi esnasında yedeklilik için birbirinden bağımsız iki imaj desteği olmalıdır.

### IEEE 802.3ad link aggregation özelliği ile 16 portu destekleyen 128 adet bağlantı noktası (LAG) oluşturulabilmelidir.

### IEEE 802.1s Multiple-Instance Spanning Tree protokolü desteği olmalıdır. Desteklenen instance sayısı en az 32 adet olmalıdır.

### IEEE 802.1w Rapid Spanning Tree Protokolü desteği olmalıdır.

### IEEE 802.1Q (4,096 VLAN ID) VLAN ID’si işaretleme desteği ve en az 4000 adet port bazında VLAN tanımlanabilmelidir.

### Teklif edilecek cihazın Data Center Bridging desteği olmalıdır. VxLAN Desteklemelidir. Eğer bu özellikler icin lisans gerekiyorsa teklife dahil edilmelidir.

### Cihaz Data Center kullanımlarında yönetim için scripting dillerinden birini desteklemedir.

### IEEE 802.1D Spanning Tree protokolü desteği olmalıdır.

### Teklif edilecek cihazın VRRP veya benzeri bir aktif-pasif Layer3 yedekleme desteği olacaktır.

### Teklif edilecek cihaz, cihaz seviyesinde aktif-aktif yedekleme yapılmasını sağlayan VPC, VSS, veya VLT protokollerinden en az birisini desteklemelidir. Bu özelliklerin kullanımı için gerekli olan tüm donanım veya lisanslar ile beraber verilmelidir. Ayrıca bu cihaz seviyesi yedekleme uygulamasında OSPF ve BGP dinamik yönlendirme protokolleri, PIM-SM ve PIM-SSM Multicast iletişim protokolleri tekliflendirilmelidir.

### IEEE 802.1w Rapid Convergence/ Reconfiguration Spanning Tree protokolü desteği olmalıdır.

### 9,216 byte büyüklüğüne kadar iletim birimi (Jumbo Frame) desteği bulunmalıdır.

### Layer 3 yönlendirme desteklenecektir. Statik yönlendirme OSPFv3 ve BGP desteği olacaktır. Bu protokollerin çalışması için gerekli olan lisanslar teklife dahil edilecektir.

### Gereksiz yayın trafiğinin engellenmesi için IGMPv1/v2/v3 snooping desteği olmalıdır.

### Yeni jenerasyon IPv6 desteği bulunmalıdır. IPv4 protokolünden IPv6 protokolüne geçiş için her iki protokolün kullanımına imkan vermelidir.

### IP kaynak/hedef adreslerine göre, UDP/TCP port numarasına göre Access Control List’ler (ACL) yazılabilmelidir.

### Port güvenliği özelliği ile kullanıcı listeleri oluşturularak sadece belli MAC adreslerinin ilgili portlara bağlantı kurmasına izin verilebilmelidir. Bu sayede izinsiz kullanıcı ve cihazların ağa girişleri engellenebilmelidir.

### RADIUS ve TACACS+ protokolleri ile kimlik tanımlama özelliklerini desteklemelidir.

### Anahtarı yönetmek isteyen kişiler Radius sorgulama protokolü tarafından sorgulanabilmelidirler.

### IEEE 802.1x kimlik tanımlama protolü desteği bulunmalıdır.

### Port başına aynı anda birden fazla 802.1x kullanıcısı desteği bulunmalıdır.

### İstenmeyen ARP Broadcast saldırılarına karşın güvenlik önlemi olarak dinamik ARP koruması özelliği bulunmalıdır.

### Port başına gereksiz yayın (broadcast) trafiğini engelleme mekanizması olmalıdır.

### İstenmeyen DHCP sunucularına karşın güvenlik önlemi olarak DHCP koruması özelliği bulunmalıdır.

### BPDU ataklarına karşın STP BPDU port koruması bulunmalıdır.

### STP Root olarak seçilmiş anahtarı ataklara ve yapılandırma hatalarına karşı koruma özelliği bulunmalıdır.

### SSHv2 Secure Shell protokolü ile uzaktan güvenli şekilde yönetilebilir olmalıdır.

### Cihaz üzerinde yüklemeler için en az 1 adet usb portu bulundurmalıdır.

### Cihaz yönetimi için ayrı bir yönetim portu olmalıdır.

### SNMPv1/v2/v3 protokolleri desteklenmelidir.

### sFlow versiyon 5 veya Flexible Netflow veri akışı izleme protokol desteği bulunmalıdır.

### Network trafiğini takip etmek için Port-Mirroring özelliği bulunmalıdır. Birden fazla bakır veya fiber portun tek tek veya vlan yada ait olduğu lag grubun üzerinden trafiği takip edilebilmeli ve aynalanabilmelidir.

### TFTP Protocol dosya transfer protokolü desteği bulunmalıdır. TFTP protokolü ile anahtar yazılımı (firmware) güncellemesi yapılabilmelidir.

### IEEE 802.1AB Link Layer Discovery Protocol (LLDP) keşif protokolü veya benzeri bir protokol desteği bulunmalıdır.

### Port başına 8 fiziksel kuyruk yapılandırması QoS yapısında kullanılabilmelidir.

### İstek dışı multicast baskınlarına karşı multicast snooping desteği bulunmalıdır.

### IEEE 802.1p trafik önceliklendirme desteği olmalıdır.

### QoS Class of Service özelliği ile, 802.1p önceliklendirmeler IP adresi, IP Type of Service, Layer 3 protokol, ACL, TCP/UDP port numarası, DiffServ ve kaynak portuna göre yapılabilmelidir.

### TCP/UDP Port numaralarına göre Layer 4 düzeyinde trafik önceliklendirme desteği olmalıdır.

### Anahtar Enhanced Transmission Selection (802.1Qaz), Priority Flow Control (802.1Qbb), DCBx ve iSCSI TLV ozelliklerini desteklemelidir.

### Cihaz tüm portları ve özellikleri aktif halde en yüksek lisans seviyesi ile teklif edilmelidir.

### Cihaz 3 yıl 7x24 destek alacak şekilde yerinde üretici garanti destek paketi ile teklif edilecektir.

* 1. **YEDEKLEME ÇÖZÜMÜ TEKNİK ÖZELLİKLERİ**

### Teklif edilecek çözüm, tekilleştirme-sıkıştırma teknolojileri dahil edilmeden en az 2 PB net kullanılabilir kapasiteye kadar (kafa ünitesi veya controller unit değişikliği gerekmeden) büyüyebilir olmalıdır.

### Teklif edilecek çözüm, yazma esnasında değişken blok temelli tekilleştirme (inline variable length deduplication) teknolojisini kullanmalıdır. Sabit blok temelli tekilleştirme (fixed lenght deduplication) veya yazma sonrası tekilleştirme (Post-process deduplication) teknolojisini kullanan çözümler kabul edilmeyecektir.

### Teklif edilecek çözüm, global tekilleştirme (global deduplication) teknolojisini kullanmalıdır. Farklı iş yükleri için farklı tekilleştirme alanı kullanan çözümler kabul edilmeyecektir.

### Teklif edilecek çözüm, birinci veri merkezi için en az 96TB (Doksan altı Terabayt) brüt disk kapasitesi ve Erasure Coding veya RAID koruma sonrası en az 64TB (Altmış dört Terabayt) net disk kapasitesi sağlamalıdır, ikinci veri merkezi için en az 72TB (Yetmiş iki Terabayt) brüt disk kapasitesi ve Erasure Coding veya RAID koruma sonrası en az 48TB (Kırk sekiz Terabayt) net disk kapasitesi sağlamalıdır. Bu alana veri azaltma teknolojilerinden kazanılan değerler dahil edilmemelidir. Bu alan için lisans gereksinimi var ise bu alan kadar lisans teklife dahil edilmelidir.

### Teklif edilecek çözümde en az 1 (bir) node’un (kafa ünitesi, controller unit veya node) kaybı veya 2 (iki) diskin kaybı durumda dahi veri kaybı olmayacak ve net kapasite hesaplaması bu yedeklik seviyesinde yapılmalıdır.

### Teklif edilen çözüm, yedekleme yazılımlarının “Instant Recovery/Instant Access” özellikleri için gereken disk I/O performansını sağlamak üzere kullanılacak solid state diskler (SSD) içerecektir. Çözüm, SSD disk alanı olarak, birinci veri merkezi için en az 6.4TB (Altı nokta dört Terabayt), ikinci veri merkezi için en az 4.8TB (Dört nokta sekiz Terabayt) brüt disk alanı sağlamalıdır.

### Teklif edilecek çözüm, ihtiyaç durumunda dosya saklama alanı olarak da (NFS/SMB protokollerini desteklemelidir) kullanılabilmelidir.

### Teklif edilecek çözüm, ihtiyaç durumunda obje saklama alanı olarak da (S3/Swift protokollerini desteklemelidir) kullanılabilmelidir.

### Teklif edilecek çözüm, kesintisiz kod güncellemelerini ve kesintisiz kapasite artırımını hem yazılımında hem de donanımında desteklemelidir.

### Teklif edilecek çözüm, yüksek erişilebilir (High-Available) yapıda olmalıdır.

### Teklif edilecek çözüm, hiper-bütünleşik yapıda çalışıyorsa herhangi iki node’un kaybında sistemin ayakta kalabilmesi için gerekli olan teknolojiyi desteklemelidir.

### Teklif edilecek çözüm üzerinde birbirini yedekleyen güç kaynağı ve fanlar bulunmalıdır. Sistem üzerindeki güç kaynakları ve fanları maksimum tüketim/kapasite için yedekleri ile takılı olarak teslim edilmelidir.

### Teklif edilecek çözüm RAID veya Erasure Coding (EC) koruma yöntemi ile veri koruma özelliklerini desteklemelidir.

### Teklif edilecek çözüm, talep edilen tüm protokolleri GUI (graphical user interface) CLI (command line interface) ve Rest API’ler üzerinden yönetebilme imkânı sağlamalıdır.

### Teklif edilecek çözüm, aynı anda birden fazla arşivleme veya yedekleme uygulamasını destekleyebilmelidir.

### Teklif edilecek çözüm üzerindeki kapasite, farklı uygulamalar arasında ortak kullanımı sağlayabilmeli ve farklı uygulama ya da departmanlar için ayrıştırılmış yapı (multi-tenancy) tanımlanmasına olanak sağlamalıdır.

### Teklif edilecek çözümde, yeni node/kontrol veya disk çekmecesi ünitelerin eklenmesi herhangi bir kesinti yaşanmadan yapılabilmelidir. Çözüm, node/kontrol ünitesi veya disk çekmecesi eklenmesi durumunda, var olan kapasiteyi manuel bir müdahaleye gerek kalmaksızın otomatik olarak mevcut node/kontrol ünitelerine veya disk çekmecelerine dengeleyebilmelidir.

### Teklif edilen çözüm, üzerinde yapılan tüm işlemler denetleme (audit) mekanizmasından geçmeli ve yapılan işlemler kayıt altına alınmalıdır.

### Teklif edilecek çözüm, RBAC desteklemelidir. Sistem içinde kullanıcılar özelleştirilmiş roller oluşturulabilmeli, bu roller gruplara ve kullanıcılara atanabilmelidir. Sistem kullanıcılarına obje bazında yetkiler atanabilmeli ve sadece bu objeler üzerinde yönetim yapması sağlanabilmelidir.

### Teklif edilen çözüm, verilerin şifrelenerek (encryption) saklanması için gereken tüm lisanslar sağlamalıdır.

### Teklif edilecek çözüm, yazılan veriler için WORM (write once read many) özelliğini etkinleştirilebilmeli ve sistem yöneticisinin bu verileri değiştirmesine veya silmesine izin vermemelidir.

### Teklif edilen çözüm, tek noktadan birden fazla noktaya ve birden fazla noktadan tek noktaya replikasyonu desteklemelidir. Bu özellikleri kullanmak için gereken lisanslar teklife dahil edilmelidir.

### Teklif edilen çözüm, replikasyon sırasında verileri şifreleyebilmelidir.

### Teklif edilen çözüm 3 (üç) yıl 7/24 yazılım ve ertesi iş günü donanım için üretici garantisi ile teklif edilmelidir.

* 1. **YEDEKLEME ÇÖZÜMÜ YAZILIM TEKNİK ÖZELLİKLERİ**

### Teklif edilecek çözüm, VMware vSphere, Microsoft Hyper-V, Acropolis ve Redhat KVM sanallaştırma platformlarında çalışan sanal makinaların yedeklemesini, sanal makine üzerine ajan kurulumu gerektirmeden yapabilmelidir.

### Teklif edilecek çözüm, VMware vSphere üzerinden yedeklenen sanal makinayı doğrudan diskte bulunan tam veya artımlı yedek dosyasından ilave bir kopyalama veya müdahaleye gerek kalmadan çalışır duruma getirebilmelidir.

### Teklif edilecek çözüm, VMware vSphere üzerinden yedeklenen sanal makinanın sadece seçilen sanal disklerini geri yükleyebilmelidir.

### Teklif edilecek çözüm, VMware vSphere üzerinde çalışan sanal makinaların I/O bazlı sürekli veri korumasını (Continious Data Protection, CDP) sağlayacak teknolojileri desteklemelidir. Sanallaştırma platformundaki bütün sanal makinelerin CDP ile yedeklenebilmesi için gerekli lisanslar teklife dahil edilmelidir.

### Teklif edilecek çözüm, yedeklenen sanal makinanın içerisinden tek bir dosyayı, sanal makinayı sistem üzerinde veya kendi üzerinde yeniden oluşturmaya gerek kalmadan geri dönebilmelidir.

### Teklif edilecek çözüm, bir veya birden fazla sanal makinayı doğrudan yedek dosyasından veya replikasyon noktasından, aynı sanallaştırma veya başka bir sanallaştırma ortamına aktarabilmelidir.

### Teklif edilecek çözüm, bir sanal makinayı doğrudan diskte bulunan tam veya artımlı yedek dosyasından ilave bir kopyalama veya müdahaleye gerek kalmadan çalışır duruma getirebilmelidir.

### Teklif edilecek çözüm, Microsoft Active Directory yedekleme işlemini gerçekleştirebilmelidir. Yedekler içerisinden grupları, grup kuralları objelerini, konfigürasyon bölümlerini, kullanıcıları ve bilgisayar hesaplarını orijinal yerine geri dönebilmelidir.

### Teklif edilecek çözüm, fiziksel sunucu üzerinde kurulu olan işletim sistemlerinin (Windows, Linux) yedeklerini alabilmelidir.

### Teklif edilecek çözüm, SQL ve ORACLE uygulamalarının veri tabanı yedeklerini alabilmelidir. Aldığı veri tabanı yedeklerini farklı bir uygulama sunucularına geri dönebilmelidir.

### Teklif edilecek çözüm, Microsoft SQL ve Oracle uygulamaları içerisinden belirtilen disk alanına veya yedekleme görevinin zamanlama ayarlarından bağımsız frekanslarda ‘Transaction Log’ yedeği alabilmelidir.

### Teklif edilecek çözüm, fiziksel sunucular üzerinde çalışan Microsoft SQL ve Oracle uygulamalarının, uygulamanın çalıştığı sunucuya veya başka sunucu üzerinde çalışan uygulamaya anlık kopyalama (clone) işlemini gerçekleştirebilmelidir.

### Teklif edilecek çözüm, NAS sistemlerinin yedeklerini alabilmelidir. Bu yedekleri başka bir NAS ortamına geri dönebilmelidir.

### Teklif edilecek çözüm, yedeklenmesi istenmeyen sanal makinalara bağlı RDM diskleri yedekleyebilmelidir. Ayrıca istenilmesi durumunda sanal makinalara bağlı RDM disklerin yedeklememe veya replikasyon işlemi dışında bırakıma işlemlerini gerçekleştirmelidir.

### Teklif edilecek çözümde, tek politika altında, farklı yedekleme aralık zamanları, farklı saklama zamanları, replikasyon aralıkları ve arşivleme aralıkları belirlenebilmelidir.

### Teklif edilecek çözüm, politikalar ayarlarında WORM (write once read many) özelliğini etkinleştirilebilmeli ve sistem yöneticisinin bu politikaları değiştirmesine veya politikalara bağlı verileri silmesine izin vermemelidir.

### Teklif edilecek çözüm, disk alanına alınmış yedekleri uzun dönemli arşivlenmesi amacı ile NFS tabanlı veri depolama, S3 tabanlı depolama veya AWS, Azure gibi bulut sağlayıcılarına gönderebilmeli ve bunlardan geriye dönüşü sağlayabilmelidir.

### Teklif edilecek çözüm, birden fazla veri merkezi arasında aktif-aktif replikasyon sağlayabilmeli, bunun için gerekli tüm donanım, yazılım ve lisanslar teklif edilen çözüme dahil olmalıdır.

### Teklif edilecek çözüm, birinci veri merkesi için en az 60TB (Atmış Terabayt) back-end veya 120TB (Yüz yirmi Terabayt) front-end yedekleme kapasite lisansı ve ikinci veri merkesi için en az 40TB (Kırk Terabayt) back-end veya 80TB (Seksen Terabayt) front-end yedekleme kapasite lisansı ile teklif edilmelidir.

### Teklif edilen çözüm 3 (üç) yıl 7/24 yazılım ve ertesi iş günü donanım için üretici garantisi ile teklif edilmelidir.

# **NETWORK TEKNİK ŞARTNAMESİ**

* 1. **OMURGA ANAHTAR CİHAZI (4 ADET)**

### Üzerinde en az 48 (kırk sekiz) adet 1/10/25Gbps (bir/on/yirmibeş Gbps) fiber downlink port bulunmalıdır.

### Anahtar üzerinde en az 4 (dört) adet 40/100Gbps (kırk/yüz Gbps) fiber uplink port bulunmalıdır.

### Anahtarlama bant genişliği en az 3.2 (üç nokta iki) Tbps olmalıdır.

### Anahtarın L2 anahtarlama performans değeri en az 1 (bir) Bpps olmalıdır.

### Anahtar en az 36 (otuz altı) MB buffer’a sahip olmalıdır.

### Anahtar IPv4 ve IPv6 protokolleri için tıkanmasız yapıda çalışmalıdır.

### Anahtarın modüler güç kaynağı desteği olmalıdır. İkinci bir dahili güç kaynağı takılarak güç kaynağı yedeklemesine sahip olabilmelidir. Anahtarın üzerinde dahili yedek güç kaynağı bulunmalıdır. Yedek güç kaynağı anahtar çalışmaya devam ederken değiştirilebilmelidir.

### Anahtar programlanabilir bir ASIC’e sahip olmalıdır. Yazılım güncellemesi ile ileride gereksinim desteği gerekebilecek olan yeni protokollerin de anahtarlanmasına açık olmalıdır.

### Anahtarın kontrol ve yönetim katmanı için kullandığı işlemci mimarisi çok çekirdekli yapıda olmalıdır.

### Anahtar 3. (Üçüncü) parti uygulamaların çalıştırılabileceği bir container altyapısı bulunmalı ve bu altyapıyı destekleyebilecek CPU ve bellek kapasitesi olmalıdır.

### Anahtarın işletim sistemi modern programlama dillerinden NETCONF, RESTCONF ve YANG modellerini ve cihaz üzerinde Python scripting desteklemelidir.

### Anahtar en az 16Gb (onaltı Gb) DRAM ve 16Gb (onaltı Gb) Flash belleğe sahip olmalıdır.

### Anahtar üzerinde en az bir adet USB 3.0 (üç nokta sıfır) ara yüz bulunmalıdır. Bu arayüz üzerinden anahtara işletim sistemi yüklemek veya log dosyalarını aktarmak mümkün olmalıdır.

### Anahtarın 9100 (dokuz bin yüz) byte’lık jumbo frame desteği olmalıdır.

### Anahtar envanter yönetimi için kullanılacak pasif bir RFID etiketine sahip olmalıdır.

### Anahtar üzerinde veri merkezi içinde yerinin kolay bulunabilmesi için açılıp kapatılabilen mavi ışık (Blue Beacon) desteğine sahip olmalıdır.

### Anahtar yazılımsal olarak Bluetooth desteğine sahip olmalıdır. Opsiyonel olarak bağlanacak bluetooth aparatı üzerinden anahtarın WEB ve komut arayüzüne erişmek, log ve işletim sistemi transferi yapmak mümkün olmalıdır.

### İki anahtar portları üzerinden birbirine bağlanarak, sanal olarak tek anahtar olarak çalışabilmeli ve tek IP erişimi ile yönetilebilmelidir. Cihaz Stackwise Virtual teknolojisini desteklemelidir.

### Anahtar en az 82.000 (seksen iki bin) adet MAC adresi desteklemelidir.

### En az 4000 (dört bin) adet aktif VLAN desteği olmalıdır.

### IEEE 802.1d Spanning Tree Protocol(STP), 802.1w Rapid Spanning Tree ve 802.1s Multiple Spanning Tree Protocol (MSTP) desteklenmelidir. Vlan’ler arası yük dengelemesi için 802.1d ve 802.1w protokolleri her VLAN için ayrı ayrı çalıştırılabilmelidir.

### Anahtar L2 loop’ları engelleme konusunda Spanning Tree yardımcı özelliklerinden, BPDU guard, Root Guard, LoopGuard özelliklerini desteklemelidir.

### Anahtar Resilient Ethernet Protokolünü (REP) desteklemelidir.

### Fiberoptik arayüzlerde, bağlantıların tek yönlü olarak fiberoptik kablolama veya port hatalarından dolayı arızalanması durumunda bunu algılayan ve tek yönlü olan linkleri kapatan UniDirectional Link Detection özelliği bulunmalıdır.

### Anahtarın iki cihaz arasında otomatik olarak L2 trunk oluşturmak için bir protokol desteği bulunmalıdır.

### Anahtar IEEE 802.3ad-LACP desteklemelidir. Cihaz üzerinde minimum 8 adet 10/100/1000 ya da 1000BaseX port, aynı kanal altında toplanıp, tek port gibi çalışabilmelidir.

### Anahtar, 802.1AB protokolünü desteklemelidir. Bu sayede kendisine doğrudan bağlı diğer anahtarları öğrenme (neighbor learning) özelliğine sahip olacaktır.

### Anahtar en az 212.000 (ikiyüz oniki bin) adet IPv4 ve IPv6 route bilgisini tutabilecek bir donanım yapısına sahip olmalıdır.

### Anahtar L3 statik yönlendirme ve IPv4 ve IPV6 dinamik yönlendirme protokollerinden RIP, RIPng, OSPF, OSPFv3, BGP, multiprotocol BGP ve IS-IS desteklemelidir.

### Anahtar NAT (Network Address Translation), PAT (Port Address Translation) desteklemelidir.

### Anahtar VRRP gibi üçüncü katman bir yedekleme protokolü desteklemelidir

### Anahtar politika tabanlı yönlendirme (PBR) desteklemelidir.

### Anahtar örnekleme yapmadan Netflow desteklemelidir. Üzerinde en az 64.000 adet flow bilgisi tutabilmelidir.

### Anahtarın IGMP v1, v2 ve v3 desteği olmalıdır.

### Anahtarın IGMP snooping ve MLD snooping desteği olmalıdır.

### Anahtar en az 2.000 (iki bin) adet IGMP snooping girdisi desteklemelidir.

### Anahtarın, IGMP filtering özelliği bulunacaktır. Bu sayede multicast grubuna üye olmayan kullanıcıların multicast yetkilendirmesi ve port bazında multicast yayın sınırlandırması yapılabilecektir.

### Anahtar, RADIUS authentication, authorization ve accounting (AAA) servislerini desteklemelidir.

### Anahtar, TACACS+ desteğiyle ağ güvenliğinin bir TACACS sunucu tarafından yönetimini desteklemelidir.

### Cihaz, paketleri L2 başlığındaki kaynak/hedef MAC adresi, L3 başlığındaki kaynak/hedef IP adresi, L4 başlığındaki TCP/UDP port numarası bilgilerine göre erişim denetiminden (ACL) geçirebilmelidir. Cihaz üzerinde tanımlanan erişim denetim listeleri zamana bağlı olarak aktif hale getirilebilmelidir.

### Erişim kontrol listeleri Port, VLAN ve SVI (Switched virtual interface) seviyesinde uygulanabilmelidir.

### Erişim kontrol listeleri donanım tabanlı olarak kullanılmalıdır.

### Anahtar her porttan belirlenen adet kadar MAC adresinin bağlantı kurmasını sağlayabilmelidir. Belirlenen limit dışındaki MAC adresleri isteğe bağlı olarak belirlendiğinde port kapatılabilmeli veya limit dışı MAC adreslerinin bağlanması engellenebilmelidir.

### Anahtar DHCP, ARP ve IP ataklarını engellemek için DHCP snooping, Dynamic ARP Inspection ve IP Source Guard özelliklerine sahip olmalıdır.

### Anahtar 802.1x desteklemeli, bir RADIUS sunucu üzerinden dinamik ACL ve VLAN Ataması yapılabilmelidir. Anahtar yetkilendirme değişikliklerinde tekrar kimlik doğrulama işlemi gerektirmemelidir (CoA-Change of Authorization).

### 802.1x desteklemeyen cihazlar için bir RADIUS sunucu üzerinden MAC adres tabanlı kimlik doğrulama yapabilmelidir.

### 802.1x desteklemeyen cihazlar için WEB tabanlı kimlik doğrulama işlemi yapılabilmeli ve bir HTTP sunucuya yönlendirme yapılabilmelidir.

### Aynı porttan birden fazla istemci bağlandığında her biri için ayrı ayrı 802.1x kimlik doğrulama yapılabilmelidir.

### Anahtarın 802.1x desteklemeyen istemciler için misafir VLAN desteği bulunmalıdır.

### Anahtar kontrol katmanını korumak için CoPP (Control Plane Policing) desteklemelidir.

### Anahtar hem uplink hem de downlink portlarında 802.1AE, MACSec desteklemelidir.

### Anahtar Voice VLAN yaratılmasını destekleyecektir. Bu sayede IEEE 802.1p class of service (CoS) uyumlu IP telefonların otomatik olarak tanınması ve Voice Vlan a eklenmesine olanak sağlamalıdır.

### Anahtar üzerindeki her portun en az 8 (sekiz) adet çıkış öncelik kuyruğu (Engress Queue) bulunmalı ve kuyruk uzunluklarını kontrol ederek tıkanıklıkları engelleyen otomatik sistemi bulunmalıdır.

### Anahtarın "QoS (Quality of Service)" desteği bulunmalıdır. Üçüncü seviyede (L3) DiffServ Code Point (IP ToS/DSCP) ya da ikinci seviyede (L2) IEEE 802.1p CoS (Class of Service) ile sınıflandırılmış paketlerin öncelik değerlerini anlayabilmeli, gerektiğinde bu öncelik değerlerini değiştirebilmelidir.

### Anahtar üzerindeki 10/100/1000 (on/yüz/bin) portlarının hızı sınırlandırılabilmelidir (Rate Limiting).

### Anahtarın IPV4 ve IPv6 için DHCP istemci ve sunucu desteği olmalıdır. Hem statik hem dinamik olarak istemcilere atamalar yapabilmelidir.

### Anahtar uzak lokasyondaki DHCP sunuculara DHCP isteklerini iletmek için DHCP relay desteğine sahip olmalıdır. Bu özellik IPv4 ve IPv6 için desteklenmelidir.

### Anahtarda detaylı gerçek zamanlı trafik analizi yapabilmek için VLAN ve port bazında port aynalama desteği bulunmalıdır. Anahtarın aynı anahtar üzerinde (SPAN) ve farklı anahtarlar arasında (RSPAN) aynalama yeteneği olmalıdır.

### TFTP, FTP, SCP protokolleri ile işletim sistemi güncellemesi yapılabilmelidir.

### Anahtar syslog sunuculara log gönderebilmeli, hata, kaynak kullanımı ve zaman aşımı gibi bilgileri raporlayabilmelidir. Raporlanacak bilgi başlıkları seçilebilir olmalıdır.

### Anahtar, saat ve tarih bilgisini ağ üzerindeki diğer tüm anahtarlarla senkron hale getirebilmek için NTP protokolünü desteklemelidir.

### Anahtar, SNMP v1, v2c, v3, Telnet, Secure Shell (SSH) v2, HTTP (web), SSL, konsol ve ethernet yönetim portu aracılığı ile yönetilebilmeli veya gözlenebilmelidir.

### Anahtar SNMP trap yeteneğine sahip olmalıdır.

### En az 4 grup RMON (history, statistics, alarms, events) desteği olmalıdır. HTTP (web) yönetim sunucusu hem IPv4 hem IPv6 istemcilere servis sağlayabilmelidir.

### Cihaz aynı anda 16 (on altı) adete kadar telnet bağlantısını ve 5 (beş) SSH bağlantısını destekleyebilmelidir.

### Anahtarda detaylı gerçek zamanlı trafik analizi yapabilmek için VLAN ve port bazında port aynalama desteği bulunmalıdır. Anahtar port aynalama yöntemlerinden SPAN, RSPAN ve ERSPAN özellikleri olmalıdır.

### Anahtar anormallik tespiti yapabilen sistemler tarafından kullanılmak üzere, şifrelenmiş trafiklerle ilgili, şifrelemeyi açmadan analitik bilgiler oluşturabilmeli ve netflow paketleri üzerinden paylaşabilmelidir.

### Anahtar en az 1400 (bin dörtyüz) adet uygulamayı tanıyabilmeli, bu bilgileri QoS tanımlarında kullanabilmeli, anahtar üzerinde raporlayabilmeli veya netflow üzerinden yönetim sistemleriyle paylaşabilmelidir.

### Anahtarın işletim sistemi yazılım seviyesini değiştirmeden belli hataları düzeltmek için üretilen yamalama (Patch) yeteneğine sahip olmalıdır.

### Anahtar Wireshark desteğine sahip olmalıdır. Anahtar üzerindeki herhangi iki port arasındaki trafik yakalanıp yine anahtar üzerinde paket paket incelenebilmeli veya Wireshark uygulaması kurulu bir sisteme gönderilebilmelidir.

### Anahtar HSRP üçüncü katman yedekleme protokolünü desteklemelidir.

### Anahtar en az 32.000 (otuziki bin) adet IPv4 ve IPv6 multicast route kapasitesine sahip olmalı ve L3 multicast protokollerinden en az PIM-Sparse, Bidirectional PIM (PIM-BiDir), Source-Specific Multicast (SSM) ve Multicast Source Discovery Protocol (MSDP) desteği bulunmalıdır.

### Anahtar hem uplink hem de downlink portlarında AES-256 tabanlı 256-bit 802.1AE, MACSec desteklemelidir.

### Anahtar VRF-lite, L3-MPLS-VPN, L2VPN (EoMPLS, VPLS) ve GRE desteklemelidir.

### Cihaz ile birlikte en az 12 adet 10G SR SFP+ modül, en az 1 adet 100GBASE PSM4 QSFP Transceiver, MPO, 500m over SMF, en az 3 adet 40GBASE-SR4 QSFP Transceiver Module with MPO Connector teklif edilecektir ve tüm fiber optik modüller aynı üreticinin orijinal ürünleri olmalıdır. OEM parça teklif edilmeyecektir. Modüllerle birlikte en az 5 metre fiber optik patch kablolar dahil teklif edilecektir.

### Anahtar bir uç noktaya olan erişimin kalitesini (paket kaybı, gecikme, jitter) ölçmek için IP SLA desteğine sahip olmalıdır.

### Teklif edilen ürün, üretici garantisine sahip olacaktır ve bununla birlikte üretici tarafından sağlanan en az 3 yıllık 8x5xNBD (çalışma saatleri ve çalışma günleri içerisinde ertesi gün değişim) servis paketi ile birlikte teklif edilecektir.

* 1. **KENAR ANAHTAR CİHAZI (2 ADET)**

### Teklif edilecek anahtar, sabit (fixed), modüler veya şasi mimarisinde olabilecektir. Aşağıda istenilen port sayıları, tipleri, performans ve diğer özellikler bu mimarilerin herhangi birinde sağlanabiliyor olmalıdır. Yüklenici hangi mimaride bu değerlere ulaştığını kuruma sunacaktır.

### Teklif edilecek anahtarın modüler veya şasi mimarisinde olması durumunda; cihaz üzerindeki süpervizör (yönetim) modülleri, switching fabric (anahtarlama) modülleri, güç (power supply) modülleri, üreticinin duyurduğu en yeni ve en yüksek kapasitedeki ürünler ile tam dolu olarak teklif edilecektir.

### Anahtar IPv4 ve IPv6 protokolleri için tıkanmasız yapıda çalışmalıdır.

### Anahtarın modüler güç kaynağı desteği olmalıdır. İkinci bir dahili güç kaynağı takılarak güç kaynağı yedeklemesine sahip olabilmelidir. Anahtarın üzerinde en az 350/715/1100 Watt gücünde dahili yedek güç kaynağı bulunmalıdır.

### Anahtar modüler ve N+1 yedekli çalışan fan’lara sahip olmalıdır.

### Anahtarın kontrol ve yönetim katmanı için kullandığı işlemci mimarisi çok çekirdekli yapıda olmalıdır.

### Anahtar en az 8Gb DRAM ve 16Gb Flash belleğe sahip olmalıdır.

### Anahtar üzerinde en az bir adet USB 2.0 ara yüz bulunmalıdır. Bu arayüz üzerinden anahtara işletim sistemi yüklemek veya log dosyalarını aktarmak mümkün olmalıdır.

### Anahtarın uplink portları modüler olmalı ve en az 4 adet 1GbaseX, 8 adet 10GbaseX, 2 adet 40GBaseX, 2 adet 25GBaseX ve 4 adet MultiGig ara yüzlerini destekleyen uplink modül opsiyonları olmalıdır, şasi anahtar teklif edilmesi durumunda bu port tipleri ve adetleri şasi üzerinde line-card olarak teklif edilecektir. Cihaz üzerinde en az 8 adet 10GBaseX ara yüzü bulunan uplink modül ile teklif edilmelidir.

### Anahtar üzerinde en az 48 adet 10/100/1000Base-T bakır yuva bulunmalıdır. Anahtar üzerinde paylaşımlı (combo) portlar kesinlikle bulunmayacaktır.

### Anahtarlama backplane kapasitesi (yığınlama kapasitesi hariç) en az 256 Gbps olmalıdır. Anahtarın L2 anahtarlama performans değeri en az 190 Mpps olmalıdır.

### Anahtar en az 16 MB buffer’a sahip olmalıdır.

### Anahtarın 9000 byte’lık jumbo frame desteği olmalıdır.

### Anahtar envanter yönetimi için kullanılacak bir RFID etiketine sahip olmalıdır, RFID desteği entegre biçimde sağlanamıyorsa her bir anahtar ile birlikte en az 1 adet aktif RFID tag teklif edilecektir.

### Her anahtar üzerinde 2 adet yığınlama portu olmalıdır. Yığınlama için kullanıcı veya uplink portları kullanılmamalı ve yığınlama çalıştırıldığında hiçbir kullanıcı portu ve uplink portu devre dışı kalmamalıdır. Stack arayüzleri ve en az 0.5 metre uzunluğunda stack kabloları teklife dahil edilecektir.

### Tüm yığın tek IP Adresi ve tek bir konfigürasyon üzerinden yönetilebilmeli ve yığın çalışırken yeni bir anahtarı yığına eklenebilmelidir.

### Yığın bant genişliği en az 480 Gbps olmalı, yığındaki tüm anahtarlar bu bant genişliğine tam erişime sahip olmalıdır.

### Yığındaki farklı anahtarlar üzerinden Etherchannel yapmak mümkün olmalıdır. (Multi-Chassis Etherchannel)

### Anahtar, eğer isteniyorsa gerekli kablolar kullanılarak, yığın içinde çalışırken yığındaki diğer anahtarlarla güç kaynağı paylaşımı yapabilmeli, ya da yığındaki güç havuzundan yararlanarak güç yedekli modda çalışabilmelidir, güç havuzu özelliği desteklenmiyorsa şasi tipli cihaz üzerindeki tüm güç kaynağı yuvaları dolu biçimde teklif edilecektir.

### Anahtar en az 32.000 adet MAC adresi desteklenmelidir.

### En az 4000 adet VLANID ve en az 1000 adet SVI (Switched Virtual Interface) desteği olmalıdır.

### IEEE 802.1d Spanning Tree Protocol (STP), 802.1w Rapid Spanning Tree ve 802.1s Multiple Spanning Tree Protocol (MSTP) desteklenmelidir. Vlan’ler arası yük dengelemesi için 802.1d ve 802.1w protokolleri her VLAN için ayrı ayrı çalıştırılabilmelidir.

### Anahtar L2 loop’ları engelleme konusunda Spanning Tree yardımcı özelliklerinden, BPDU guard, Root Guard, LoopGuard özelliklerini desteklemelidir.

### Fiberoptik arayüzlerde, bağlantıların tek yönlü olarak fiberoptik kablolama veya port hatalarından dolayı arızalanması durumunda bunu algılayan ve tek yönlü olan linkleri kapatan UniDirectional Link Detection(UDLD) özelliği bulunmalıdır.

### Anahtar IEEE 802.3ad - LACP desteklemelidir. Cihaz üzerinde minimum 8 adet aynı tipte kullanıcı veya uplink portu, aynı kanal altında toplanıp, tek port gibi çalışabilmelidir.

### Anahtar, 802.1AB protokolünü desteklemelidir. Bu sayede kendisine doğrudan bağlı diğer anahtarları öğrenme (neighbor learning) özelliğine sahip olacaktır. Bu amaçla LLDP, LLDP-MED desteklenmelidir.

### Anahtar en az 32.000 adet IPv4 veya 16.000 adet IPv6 route bilgisini tutabilecek bir donanım yapısına sahip olmalıdır.

### Anahtar L3 statik yönlendirme ve IPv4 ve IPV6 dinamik yönlendirme protokollerinden RIP, RIPng, OSPF, OSPFv3, IS-IS, BGP desteklemelidir.

### Anahtarın işletim sistemi yazılım seviyesini değiştirmeden belli hataları düzeltmek için üretilen yamalama (Patch) yeteneğine sahip olmalıdır.

### Anahtar HSRP üçüncü katman yedekleme protokolünü desteklemelidir.

### Anahtar en az 8000 adet multicast route kapasitesine sahip olmalı ve L3 multicast protokollerinden en az PIM-Sparse, Bidirectional PIM (PIM-BiDir), Source-Specific Multicast (SSM) ve Multicast Source Discovery Protocol (MSDP) desteği bulunmalıdır.

### Anahtar VRF ve VXLAN desteklemelidir.

### Anahtar bir uç noktaya olan erişimin kalitesini (paket kaybı, gecikme, jitter) ölçmek için IP SLA desteğine sahip olmalıdır.

### Anahtar üçüncü katman yedekleme protokollerinden olan HSRP desteklemelidir.

### Anahtar Flexible Netflow desteklemelidir. Üzerinde en az 64.000 adet flow bilgisi tutabilmelidir.

### Anahtarın IGMP v1, v2 ve v3 desteği olmalıdır.

### Anahtar, RADIUS authentication, authorization ve accounting (AAA) servislerini desteklemelidir.

### Anahtar, TACACS+ desteğiyle ağ güvenliğinin bir TACACS sunucu tarafından yönetimini desteklemelidir.

### Cihaz, paketleri L2 başlığındaki kaynak/hedef MAC adresi, L3 başlığındaki kaynak/hedef IP adresi, L4 başlığındaki TCP/UDP port numarası bilgilerine göre erişim denetiminden (ACL) geçirebilmelidir. Cihaz üzerinde tanımlanan erişim denetim listeleri zamana bağlı olarak aktif hale getirilebilmelidir.

### Erişim kontrol listeleri Port, VLAN ve SVI (Switched virtual interface) seviyesinde uygulanabilmelidir.

### Anahtar en az 5000 adet ACL desteğine sahip olmalıdır.

### Anahtar her porttan belirlenen adet kadar MAC adresinin bağlantı kurmasını sağlayabilmelidir. Belirlenen limit dışındaki MAC adresleri isteğe bağlı olarak belirlendiğinde port kapatılabilmeli veya limit dışı MAC adreslerinin bağlanması engellenebilmelidir.

### Anahtar DHCP, ARP ve IP ataklarını engellemek için DHCP snooping, Dynamic ARP Inspection ve IP Source Guard özelliklerine sahip olmalıdır.

### 802.1x desteklemeyen cihazlar için bir RADIUS sunucu üzerinden MAC adres tabanlı kimlik doğrulama yapabilmelidir.

### 802.1x desteklemeyen cihazlar için WEB tabanlı kimlik doğrulama işlemi yapılabilmeli ve bir HTTP sunucuya yönlendirme yapılabilmelidir.

### Anahtar 802.1AE 128 bit AES MACSec desteklemelidir. Lisans artırımı ile 802.1AE 256 bit AES MACSec destekleyebilecektir.

### Anahtar Voice VLAN yaratılmasını destekleyecektir.

### Anahtar üzerindeki her portun en az 8 adet çıkış öncelik kuyruğu (Engress Queue) bulunmalıdır.

### Anahtarın "QoS (Quality of Service)" desteği bulunmalıdır. Üçüncü seviyede (L3) DiffServ Code Point (IP ToS/DSCP) ya da ikinci seviyede (L2) IEEE 802.1p CoS (Class of Service) ile sınıflandırılmış paketlerin öncelik değerlerini anlayabilmeli, gerektiğinde bu öncelik değerlerini değiştirebilmelidir.

### Anahtarda detaylı gerçek zamanlı trafik analizi yapabilmek için VLAN ve port bazında port aynalama desteği bulunmalıdır. Anahtarın aynı anahtar üzerinde (SPAN) ve farklı anahtarlar arasında (RSPAN) aynalama yeteneği olmalıdır. Anahtar en az 4 adet SPAN oturumu (session) desteklemelidir.

### Anahtar, saat ve tarih bilgisini ağ üzerindeki diğer tüm anahtarlarla senkron hale getirebilmek için NTP protokolünü desteklemelidir.

### Anahtar, SNMP v1, v2c, v3, Telnet, Secure Shell (SSH) v2, HTTP, HTTPs, SSL, konsol ve Ethernet yönetim portu aracılığı ile yönetilebilmeli veya gözlenebilmelidir.

### Anahtar ileride lisans artırımı ile BGP, IS-IS, PIM Sparse Mode (PIM-SM), Source-Specific Multicast (SSM) ve Multicast Source Discovery Protocol (MSDP) destekleyebilecektir.

### Teklif edilen ürün, üretici garantisine sahip olacaktır ve bununla birlikte üretici tarafından sağlanan en az 3 yıllık 8x5xNBD (çalışma saatleri ve çalışma günleri içerisinde ertesi gün değişim) servis paketi ile birlikte teklif edilecektir.

* 1. **AĞ ÜRÜNLERİ EK ALIM VE LİSANS YENİLEME**

### Mevcutta kullanılan Cisco marka Ağ Erişim Kontrol Yazılım (NAC) yedek alımı ve lisans yenileme, ek alım kısmı da projeye dahil edilecektir. İhtiyaç listesi aşağıdaki gibidir.

|  |  |
| --- | --- |
| **AÇIKLAMA/CISCO ISE YENİLEME MERKEZ KAMPÜS** | **ADET** |
| ISE-SEC-SUB | 1 |
| ISE-A-LIC | 2500 |
| ISE-P-LIC | 1650 |
| SVS-ISE-SUP-B | 1 |
| L-AC-APX-LIC= | 500 |
| L-AC-APX-1Y-S4 | 500 |
| L-ISE-VMC-UPG= | 3 |

### Mevcutta kullanılan Cisco marka Ağ ürünlerine ait üretici servis destek paketi alımı olacaktır. Üretici servis paket içeriği 8x5xErtesi İş gününü kapsayacak ve en az bir yıl destekli olacak şekilde teklif edilmelidir. Ek alım kısmı da projeye dahil edilecektir. İhtiyaç listesi aşağıdaki gibidir.

|  |  |
| --- | --- |
| **AÇIKLAMA/CISCO SMARTNET YENİLEMELERİ MERKEZ KAMPÜS** | **ADET** |
| CON-SNT-P7PK94P1 | 9 |
| CON-SNT-P8MUN2M0 | 10 |
| CON-SNT-N9KC921Y | 1 |
| CON-SNT-AIRCTRTK | 1 |
| CON-ECMU-RISEV9SM | 1 |

### Mevcutta kullanılan Sestek ürünlerine ait üretici servis destek paketi alımı olacaktır. Üretici servis paket içeriği 8x5xErtesi İş gününü kapsayacak ve en az bir yıl destekli olacak şekilde teklif edilmelidir. Ek alım kısmı da projeye dahil edilecektir. İhtiyaç listesi aşağıdaki gibidir.

|  |  |
| --- | --- |
| **AÇIKLAMA/SESTEK IVR LİSANS & BAKIM** | **ADET** |
| IP SANTRAL KARŞILAMA ANONS BAKIM HİZMETİ | 1 |
| IP SANTRAL KARŞILAMA ANONS LİSANSLAR | 1 |

# **BİLGİ GÜVENLİĞİ ŞARTNAMESİ**

* 1. **BİLGİ GÜVENLİĞİ ÜRÜNLER YENİ ALIM YAPILACAK ÇÖZÜMLER**

### Bu kısım bilgi güvenliği çözümleri içerisinde yer alacak, yeni çözümlerin teknik özelliklerini içerir. Bilgi güvenliği çözümleri içerisinde yeni tekliflendirilecek cihazlar, 1 yıl süreyle üretici destek paketleri dahil tekliflendirilecektir. 1 yıl boyunca cihaz ile alakalı yaşanacak herhangi yazılımsal , donanımsal bir hatada yurt dışına kayıt açma , sorunun çözülmesi gereken çalışma için ilave bir bedel talep edilmeyecektir.

* 1. **TRELLİX LOG YÖNETİM YAZILIMI YENİLEME**

### Mevcutta Log yönetimi amaçlı kullanılan Trellix yazılım ürünü için 1 yıllık lisans yenileme paketi alımı olacaktır. İhtiyaç listesi aşağıdaki gibidir.

|  |  |
| --- | --- |
| **AÇIKLAMA** | **ADET** |
| MFE Ent Sec Manager VM 8 Cores P:1 BZ | 1 |
| MFE Ent Sec Mngr VM 4 Cores Add-On P:1BZ | 1 |
| MFE ELM VM 8 Cores P:1 BZ | 1 |
| MFE Event Receiver VM 8 Cores P:1 BZ | 1 |
| MFE Event Rec VM 4 Cores Add-On P:1BZ | 2 |
| MFE GTI for ESM-VM-8 1:1BZ | 1 |
| MFE Datacenter Sec Suite DbaseP:1BZ [P+] | 1 |
| MFE Adv Corr Eng VM 8 Cores P:1 BZ | 1 |

* 1. **SUNUCU ve UÇ NOKTA GÜVENLİĞİ ÇÖZÜMÜ**

### Sistem en az merkezi yönetim, yönetim ara yüzü ve ajan bileşenlerinden oluşacaktır.

### Yapı merkezi yönetimden uç istemci ve sunuculardaki ajanların yönetilmesi esasıyla çalışacaktır.

### Önerilen çözüm minimum 1400 kullanıcıyı destekleyecek şekilde lisanslanacaktır. Bakım süresi boyunca son kullanıcı, üreticinin destek merkezine telefon ya da e-posta ile destek isteğinde bulunabilecektir.

### Önerilen çözümün teknolojik sürekliliği açısından, üretici YÜKLENİCİ’ nin geliştirme süreçleri önemlidir. Dolayısıyla önerilen ürün/teknoloji için herhangi bir End-of-Life (EoL) ve End-of-Sale (EoS) duyurusu yapılmamış olmalıdır.

### Önerilen çözüm IPv6 konfigürasyon desteğine sahip olacaktır.

### Önerilen Çözüm KURUM tarafından kullanılacak olan SIEM ile (syslog, db okuma, cef formatı gibi) entegre olabilmelidir.

### Önerilen çözüm 1 yıl üretici destek paketi ile birlikte tekliflendirilecektir.

### Önerilen çözüm ile ilgili, teklif verecek olan firma, teklif verdiği çözüm ile alakalı kendi bünyesinde yetkin ve tüm teknik sertifikasyonlarını tamamlamış olan personel bulundurmalıdır

### Önerilen çözüm ile ilgili, teklif verecek olan firmanın teklif verdiği çözüm ile ilgili daha öncesinde benzer proje deneyimi olmak zorundadır. KURUM tarafından referans istenildiği taktirde firma tarafından bu bilgilerin paylaşılması zorunludur.

### Merkezi yönetim sunucusu en az Windows 2012, Windows 2012 R2, Windows 2014, Windows 2016, Windows 2019 işletim sistemleri üstüne kurulabilecektir. Ek olarak Wmvare, Hyper-V ve Citrix XenServer desteklenmelidir.

### Merkezi yönetim yazılımı HTTP tabanlı yönetime uygun olmalıdır.

### Merkezi Yönetim Arabirimi en az şunları yapacaktır:

### Sistemlerde (istemci ve/veya sunucular) ilgili ajanların uygulamasının kurulması, kaldırılması ve güncellenmesi işlemlerini takvime bağlı olarak yapabilecektir.

### KURUM içindeki MS AD entegrasyonu ile alan ağına (domain) yeni katılan sistemlere otomatik ajan kurulumunu sağlayacaktır. Bu senkronizasyon sırasında AD yapısında fark edilen istemci sistemler el ile oluşturulmuş gruplara otomatik atanabilecek ve o grup için atanan görevler otomatik işletilebilecektir.

### Merkezi yönetim sistemi aracılığıyla uç noktalarda uzak ambar yaratılabilecektir. Bu uzak ambarın, o uç noktada bulunan sistemlerdeki kurulum/yama ve imza güncellemesi görevlerinde kullanılabilmesi sağlanacaktır. Böylelikle uzak uçtaki güncelleme ve kurulumlar için geniş alan ağının mükerrer trafikle meşgul edilmesi engellenebilecektir. Uzak ambarların seçilmesi sırasında istemcilerin kendi IP alt ağlarından ambar seçmesi ve ping sürelerinin kalitesine göre seçme yöntemleri mümkün olabilecektir.

### İstemci ve sunucu tarafında bulunan zararlı kodlarla ilgili olarak KURUM içinde en çok hangi zararlı kodun bulunduğu, en çok zararlı kodun hangi sistemde bulunduğu, yönetilen sistemlerdeki anti-virüs imza versiyonu, yönetilen sistemlerdeki tarama motoru versiyonu, yönetilen sistemlerdeki ürün sürüm bilgisi raporları alınabilecektir.

### Bölgeler IP aralığı gibi parametrelere göre belirlenebilecek, sistemlerin gruplanması istenirse, en az şu kriterlerine göre gruplamalar yapılabilecektir.

### İşletim sistemi

### Yama seviyesi (service pack version)

### Dahil olduğu alan adı (domain)

### Farklı politikalar tanımlanarak bu politikalar gruplara ya da istemcilere uygulanabilecektir.

### Üretici web sitesinden periyodik güncelleme kontrolü yapılabilmeli ve bunun dağıtık ambarlara gönderilmesi mümkün olmalıdır. Rol tabanlı yönetim kabiliyeti olacaktır

### İstemcilerde yüklü ürünlerin özelliklerine göre tagleme yapılabilmelidir.

### Yönetim konsolunun yüklü olduğu makine ve veritabanı üzerinde performans ve bakım işleri için yönetim konsolu üzerinden görevler tanımlanabilecektir.

### Son Kullanıcı Güvenlik Çözümü yönetilen sistemlere uzaktan kurulacak ve bu yazılım en az şu özellikleri destekleyecektir:

### Virüs, spyware, adware, APT ve rootkitler engellenecektir.

### Ransomware zararlılarına karşı özel geliştirilmiş koruma tekniklerini içermelidir.

### Kurulum sistemin yeniden başlatılmasını gerektirmemelidir.

### Minimum 20 (yirmi) farklı güncelleme noktası belirlenebilmelidir.

### Windows kullanıcı haklarının değiştirilmesi engellenebilmelidir.

### Registry editör disable edilebilmelidir.

### Cscript ve Wscript ile betiklerin tetiklenmesi engellenebilmelidir.

### Yeni CLSIDs, APPIDs, TYPELIBs kurulumu engellenebilmelidir.

### Ağ ayarlarının değiştirilmesi engellenebilmelidir.

### Uzaktan auto-run oluşturma engellenmelidir

### Internet Explorer ayarlarının değiştirilmesi engellenebilmelidir.

### Çalıştırılabilir dosyalar MD5 hash ve Signer bilgileri ile engellenebilmelidir.

### SMEP, GPEP Windows DEP desteklenmelidir.

### MS Office uygulamaları gibi bilinen uygulamaların Powershell etkileşimleri denetlenebilmelidir.

### Microsoft AMSI ile entegre olabilmelidir.

### Henüz imzası yayınlanmamış yeni tehditlerin sistem üzerinde değişiklik yapması engelleyecek özelliğe sahip olmalıdır.

### Önerilen anti-virüs çözümü davranışsal virüs tespitine dönük teknikleri içermeli, bu sistem, ajan kurulu makinalardaki şüpheli aktivitelerin imza veritabanında olmaması durumunda merkezi istihbarat sunucularına sorup, zararlı kod ile ilgili bir bilginin bulunması durumunda aksiyon (delete, vb.) alabilmelidir.

### Özellikle APT’ lere karşı ek bir sandbox gerektirmeden makine öğrenimi, istatistiksel ve dinamik analiz teknikleri kullanılabilmelidir

### Çözüm paketi, Internet Explorer veya Mozilla Firefox ile entegre olan ve gidilen sitelerin güvenlik durumlarının sorgulanabileceği add-in desteği ile gelmelidir. Bu add-in ayrıca Google, Yahoo gibi popüler tarama motorlarına entegre olabilmeli ve sorgulamalar sırasında listelenen URL adreslerinin güvenlik durumlarını aynı ekran üzerinde gösterebilmelidir. Aynı web kontrol ajanı son kullanıcının gidebileceği URL kategorilerini de yönetebilmeli, bu yolla son kullanıcının gittiği web adresleri denetlenebilmelidir. Çözüm en az 90 (doksan) farklı kategoriyi tanımalıdır.

### Uç nokta güvenlik çözümü APT ve Lokal İstihbarat Servisi en az aşağıdaki özellikleri sağlamalıdır.

### Bilinmeyen bir malware tespiti sırasında local reputasyon (file hash ve file certificate) bilgileri dışında, malware davranışlarından da faydalanabilmelidir. Davranış bilgileri güncellemeler yoluyla geliştirilebilir olmalıdır.

### Makine öğrenimi (machine learning) algoritması kullanılarak imzası olmayan bilinmeyen/sıfırıncı gün zararlılarına karşı koruma sağlanabilmelidir.

### Makine öğrenimi algoritması çevrimiçi ve çevrimdışı çalışabilmelidir.

### Makine öğrenimi algoritması PE (portable executable) dosya tipleri için denetleme sağlayabilmelidir.

### Makine öğrenimi algoritması çalışma öncesi (pre-execution) ve çalışma sonrası (post-execution) sırasında dosya özelliklerine veya davranışlarına bakarak imzası olmayan sıfırıncı gün zararlılarını tespit edebilmelidir.

### Çözüm sahip olduğu kurallar sayesinde zararlıların sistem üzerinde yapmaya çalıştığı değişiklikleri algılayıp engelleyebilmelidir.

### Malware tespiti sırasında lokal reputasyon ve davranış bilgilerinin yetersiz

### kalması durumunda aynı üreticiye ait malware araştırma (sandbox) çözümüyle entegre çalışarak bilinmeyen malware in tespiti mümkün olmalıdır.

### Son kullanıcı güvenlik sistemi olası bir malware tespiti sonrası malware bilgileri detaylı olarak raporlanabilmeli, file hash bilgisi yoluyla bu malware in ağ içinde başka hangi makinalarda çalıştığı tespit edilebilmelidir.

### Bulunan malware başka makinada çalışması durumunda ilgili process otomatik olarak durdurulabilmelidir. Benzer dosyanın bir sonraki aşamada çalıştırılması engellenebilmelidir.

### STIX çıktıları sisteme import edilip zararlı tespitinde kullanılabilmelidir.

### Sistem bir dosyanın zararlı olduğuna karar vermesi durumunda bunla ilgili “zararlı” bilgisi Kurumsal itibar servisine anlık olarak iletilebilmeli ve aynı ağdaki diğer son kullanıcı sistemleri, aynı üreticiye ait Web Gateway ve Network IPS sistemi bu bilgiyi kullanabilmelidir. Bu sayede aynı dosya web gateway üzerinden indirilmeye kalkarsa otomatik kesilebilmeli. Bir başka son kullanıcıda çalışması durumunda ilgili process otomatik olarak durdurulabilmelidir (kill).

### Tüm mesajlaşmalar anlık yapılacak şekilde özel bir iletişim katmanında gerçekleşmelidir.

### Lokal istihbarat servisi başka üreticilere ait olan güvenlik ürünlerine de istihbarat bilgisinin sorgulanmasına izin verebilmelidir.

### İlgili ajanlar aynı üreticinin son kullanıcı güvenlik sisteminin merkezi yönetim sistemi ile dağıtılabilmeli ve yönetilebilmelidir.

### Sistem virustotal ile entegre olabilmeli bu yolla yeni bir zararlının durumu online sorgulanabilmelidir.

### Sistem üzerinden ağ üzerinde çalışan tüm sistemlerin dosya ve sertifika durum bilgeleri anlık olarak sorgulanabilmelidir.

### Bir dosyanın Kurumsal itibar seviyesi el ile değiştirilebilmelidir. Örneğin trusted görünen bir dosya malicous olarak değiştirilebilmelidir.

### Sistem merkezi olarak ajanların durumlarını izleme ve bloklama moduna çekilebilmelidir.

### Sitem üzerinden dosyaların sertifika durumları anlık kontrol edilebilmeli istenilirse sertifika durumu el ile değiştirilebilmelidir.

### Sandbox analizi için maximum dosya boyutu tanımlanabilmelidir.

### Dağıtık mimariler için modüler mimari alt yapısı sağlanmalıdır.

### Kurumsal itibar servisi üzerinde kayıtlanmış bir dosyanın en az aşağıdaki bilgileri sorgulanabilir yapıda olmalıdır:

### File name

### File Path

### Company Name

### File Version

### Cloud Reputation

### Enterprise Reputation

### SHA-1,MD5 ve SHA-256 hash bilgileri

### First Contact

### Last Update

### Register as a service

### Registered for auto run

### Executed from Removable media

### Executed from CD-ROM

### Enterprise Count

### Last Detection name

### Önerilen güvenlik paketi son kullanıcılar makinalarında donanım kontrolünü sağlamalıdır. Device Control ürünü aşağıdaki özellikleri desteklemelidir:

### Donanım kontrolü modülüyle birlikte, Bluetooth, cd/dvd, floopy disk, imaging device, network adapter, pcmci adapter, tape drives, usb drives, wireless ethernet donanımları ön tanımlı olarak gelmeli ve gerekirse el ile yeni donanım tipleri sisteme tanıtılabilmelidir. Bu amaçla donanım GUID bilgileri kullanılabilmelidir.

### Donanım tipleri en az bus tipi, donanım adı, seri numarası, instance ID, compatible ID, vendor ID, Product ID parametreleri ile özelleştirilebilmelidir. Tanımlanan donanım tipleri donanım erişim kontrollerinde kullanılabilmelidir.

### Donanım kontrolleri bloklama, read-only, notify veya monitor aksiyonları ile sonuçlandırılabilmelidir.

### Oluşan tüm olaylar merkezi rapor ara yüzünden izlenebilmelidir. Kim, ne zaman, hangi donanımı kullandı? Bu donanımın özellikleri nedir? vb.

### Tüm kurallar AD grup ve kullanıcılarına, lokal kullanıcı ve makinaya özel olarak atanabilmelidir. Kurallar online ya da offline duruma göre özelleştirilebilmelidir. Bu kapsamda kullanıcı KURUM dışında olduğu zaman farklı bir politika ile kısıtlanabilmelidir.

### Harici diskler üzerinde read-only politika kapsamında belirlenen uygulamalar politika harici tutularak çalıştırılması sağlanabilmelidir.

### Politikalar uygulanmadan önce analizden geçirilebilmeli, olası kural ihlalleri arayüz üzerinden gösterilebilmelidir.

### Oluşturulan politikalar html olarak export edilebilmelidir.

### Yönetim arayüzü üzerinden tüm kayıtlar takip edilebilmeli, kayıtlar için filtreler yazılıp istenilen kayda hızlı ulaşılması sağlanmalıdır.

### Yönetim yazılımının raporlama aracıyla, önerilen çözümle ilgili detaylı istatistiksel raporlar alınabilmeli bunlar istenildiği takdirde html, csv, xml, pdf olarak kayıt edilebilmelidir.

### Önerilen çözüm paketi, son kullanıcı sistemler için aynı zamanda dinamik beyaz liste (dynamic whitelisting) çözümünü sağlayan ajan da sağlamalıdır. Bu çözüm:

### Dinamik beyaz liste çözümü en az aşağıdaki işletim sistemlerini desteklemelidir:

### Windows 7 32 ve 64 bit

### Windows 8 32 ve 64 bit

### Windows 8.1 32 ve 64 bit

### Windows 10 32 ve 64 bit

### Windows 2008

### Windows 2012

### Windows 2016

### İşletim sistemleri üzerinde çalışan tüm binary executables (exe,com,dll...), script (.bat, .cmd, .vbs, vb.) ve java kodları beyaz listeye dâhil olabilmelidir.

### Beyaz listeye alınan tüm uygulamaların SHA-1 envanterleri veri tabanında tutulabilir yapıda olmalıdır.

### Hafıza taşmalarına (memory buffer overflow) karşı koruma sağlamalı, bu yolla izin verilen (örneğin: Internet Explorer) uygulamalara doğru yapılacak ataklar engellenebilmelidir.

### Sistem üzerinde çalışan uygulamaların itibar durumu aynı üreticinin reputation servisi tarafından kontrol edilebilir yapıda olmalıdır. Dolayısıyla, izin verilen uygulamaların risk seviyeleri ile ilgili raporlar oluşturmaya imkân vermelidir.

### Ajan sisteme kurulduktan sonra izleme (observe) modda çalıştırılabilmelidir.

### Sistem sunucular/istemciler üzerinde çalışan binary kodlarla ilgili tüm envanter bilgisini çıkarabilmeli, belirlenen bu imajlar arasındaki farklar raporlanabilmelidir. Örneğin: Baz alınan bir imajın sahadan gelen envanter bilgilerine istinaden farkları (image deviation) raporlanıp, uyumsuz sistemler tespit edilebilmelidir.

### Trusted Installer tanımı ile katılaştırılmış sistemler üzerinde whitelist imkânı sağlanabilmelidir. Örneğin: Microsoft SSCM yoluyla bir uygulamanın kurulması.

### Beyaz liste için uygulama yayıncısının dijital sertifikaları sisteme tanıtılabilmeli, bu yolla söz konusu imzaya sahip tüm uygulamalar otomatik olarak beyaz listeye alınabilmelidir.

### İsteğe bağlı olarak kullanıcı onay yöntemi ile çalışabilmeli ve onaylanan uygulamalar, aktiviteler yönetim konsolu üzerinde görülebilmeli, görülen dosyalar beyaz listeye eklenebilmelidir.

### Devreye alındıktan sonra uygulamalarda ve işletim sistemlerinde yapılabilecek toplu güncelleştirmeler için bakım modunda çalışabilmeli ve işlemler tamamlandıktan sonra tekrar koruma modunda devreye alınabilmelidir.

### Beyaz liste güvenlik ajanı kernel driver seviyesinde çalışmalı dolayısıyla kullanıcı tarafından etkisiz hale getirilememelidir.

### Son kullanıcı tarafında oluşan uyarı ekranları özelleştirilebilmelidir.

### Çözüm Firewall Modülü içermeli inbound/outbound yönünde detaylı (process, zaman, vb.) firewall kuralları yazmaya elverişli olmalıdır. Bu çözüm:

### Firewall modülü adaptive modda (allow) çalıştırılarak trafikle ilgili otomatik öğrenim sağlamalı ve olası kurallar otomatik oluşturulabilmelidir.

### Firewall kuralları, IP adresi, IP alt ağı, IP aralığı, wireless, virtual bağlantı tipine göre, transport protocol, uygulama adı, uygulama yolu (path), MD5 hash değeri ve signer bilgisine göre yazılabilmelidir.

### Kurallar in, out yönlerinde yazılabilmelidir.

### Firewall modülü aynı üreticinin buluttaki tehdit istihbaratında kayıtlı IP bilgilerinin risk seviyelerine göre aksiyon alabilmelidir.

### Önerilen son kullanıcı güvenlik çözümünün firewall ve web güvenlik modülüne ait kurallar MS AD grup, OU ve kullanıcılarına göre atanabilmelidir

### Önerilen disk şifreleme ve dosya şifreleme ürünü aşağıdaki gereksinimleri desteklemelidir

### Bilgisayarlarda kullanıcı adına ve grubuna göre login olabilecek kullanıcılar belirlenebilmelidir.

### Kriptolama algoritması için en az AES-NI 256 bit kullanılabilmelidir.

### Solid state disk sistemleri kriptolama amaçlı olarak desteklenmelidir.

### Kimlik doğrulama pre-boot aşamasında devreye girmeli ve bu kimlik doğrulama sırasında USB token/smart card kullanılabilmelidir.

### Kriptolama için kullanılan kimlik doğrulama mekanizması Windows işletim sistemi kimlik doğrulama ile entegre olabilmelidir bu yolla işletim sistemi açıldıktan sonra tekrar kullanıcı adı ve şifre girilmesine gerek kalmamalıdır.

### Çözüm düzenli olarak Active Directory’den kullanıcı şifre değişikliğini sorgulayabilmeli ve değişiklik görecek olursa kullanıcıyı gerekli aksiyonu alması konusunda uyarabilmeli ve böylelikle preboot şifresi ile Active Directory şifresi eşitlenebilmelidir.

### Kullanıcının sisteme giriş zamanları ayarlanabilmelidir.

### Parola geçmişi, kaç yanlış girişte engellenebileceği, ne kadar zaman sonra tekrar şifre yenilenmesinin zorlanabileceği, minimum ve maximum uzunluk ve parolanın içermesi gereken karakter tipleri ayarlanabilen parametreler olmalıdır.

### Sadece boot disk kriptolanabilmelidir.

### Kimlik doğrulama sırasında sanal klavye kullanılabilmelidir.

### USB ve PCMCI cihazların pre-boot aşamasında kullanılıp kullanılamayacağının kararı politikalarla belirtilebilmelidir.

### Pre-Boot da kullanılan arka plan görüntüsü değiştirilebilir yapıda olmalıdır.

### Oluşturulabilecek rapor şablonları ile kriptolanmış istemci sistemlerinin disklerinin kriptolanma süreçlerinin durumu, büyüklüğü, hangi sistemlerde hangi kripto yazılımın kurulu olduğu veya kurulu olmayan sistemler, kurulu kripto yazılımlarının sürümleri, kriptolama süreçlerinin detayları, Disk model number, disk tipi gibi bilgileri içermeli ve gerekirse bu parametreler için kriter yazılıp spesifik bilgilere ait raporlara ulaşabilmelidir. Raporlar PDF ve html olarak alınabilmelidir.

### Olası şifre unutmaları durumunda kullanıcının kendi kendine şifre yenilemesi imkanı verilebilmelidir. Bu amaçla sadece kullanıcının bileceği sorulara doğru cevap vermesi durumunda şifre değişikliğine imkân verilmelidir.

### Olası şifre unutmalarında challenge/response yöntemi ile kullanıcı ile sistem yöneticisinin karşılıklı üretilen kodlarla yeni şifre girilmesine imkân sağlayacak senaryoları desteklemelidir. Oluşturulacak anahtarların boyutları politikalarla ayarlanabilmelidir.

### Olası şifre unutmalarında aynı üreticiye ait olan bir mobil uygulama ile kullanıcılar barkod okutma işlemi ile kendiler şifre değiştirme işlemi yapabilmelidir. Mobil uygulama Android ve IOS desteklemelidir.

### Olası problem senaryolarında kripto ajanının manual kaldırılması mümkün olmalıdır.

### Desteklenen smartcardlarda kimlik doğrulama sırasında PIN kullanımına imkân vermelidir.

### Domaine yeni katılan sistemlere ek bir müdahale gerektirmeden otomatik olarak ilgili kripto ajanları bağlı bulundukları gruba atanmış politikalarla kurulabilmelidir. Arayüz yoluyla istenilirse bir istemci başka bir gruba taşınırsa o grubun politikasını otomatik olarak alabilmelidir.

### Olası felaket senaryolarında kullanılmak üzere diske harici donanımlarla ulaşarak recover edilmesi ya da pre-boot sistemin silinmesi desteklenmelidir.

### Cold boot ataklara karşı koruma sunmalıdır.

### Belirli senaryolar için TPM chipseti şifreleme anahtarını saklamak üzere kullanmalıdır.

### Çözüm şifreleme başlamadan önce bilgisayarın şifrelemeye uygun olup olmadığını kontrol edebilmelidir.

### Çözümün yönetim konsolu aynı zamanda MS Bitlocker’ı yönetilebilmelidir.

### Dosya ve klasör kriptolama çözümü en az MS Active Directory kullanıcı veri tabanıyla entegre olabilmelidir. Bu yolla politikalar kullanıcı adlarına göre tanımlanabilmelidir.

### Kullanıcıların dosya ve klasör kriptolama çözümü için kullandığı kripto anahtarı authentication (kimlik doğrulama işlemi) smart card ya da Active Directory bilgileri ile yapılabilmelidir.

### Kullanıcının dosya ve klasör kriptolama çözümü için kullandığı kripto anahtarına erişimini tetikleyecek mekanizmalar olmalı. Bu mekanizmalar; Windows’a logon, kriptolama anahtarına erişim isteği ya da system tray üzerinde erişim isteği olmalıdır.

### Sistemin belirli süre kullanılmaması durumunda dosya ve klasör kriptolama çözümü tarafından kullanılan kripto anahtarları otomatik olarak kilitlenebilmeli ve bu süre politika ile belirlenebilmelidir.

### Kriptolama anahtarı için kimlik doğrulama İşletim sistemime login olma, şifre girme ya da smart card ile yapılabilmelidir.

### Aynı üreticiye ait mobil uygulama ile mobil cihaz üzerinden dosya ve klasör kriptolama çözümü ile kriptolanan dosyalara güvenli erişim sağlanabilmelidir.

### Kullanıcıya gösterilecek uyarı mesajları özelleştirilebilmelidir.

### İstenildiği takdirde şifrelenecek dosyaların boyutu belirlenebilmelidir.

### İstenildiği takdirde silinen dosyaların wipe edilebilmesi sağlanabilmelidir.

### İstenildiği takdirde proseslerin şifrelenmiş dosyalara erişimi engellenebilmelidir.

### Belirli dosya tiplerinin kriptolama işlemi dışında bırakılması sağlanabilmelidir.

### Belirli bir süre bilgisayar üzerinde aktivasyon olmaması durumunda kripto anahtarına erişim doğrulaması gerektirmelidir

### Önerilen çözüm dosya ve klasör kriptolama dışında harici veri depolama sistemlerini kriptolayabilecek yapıda modül içermelidir, bu modül herhangi ek lisans gerektirmemelidir.

### Son kullanıcıya politikalar dâhilinde kendi dosya veya klasörlerini kriptolama ya da kriptoyu çözme hakkı verilebilmelidir.

### Son kullanıcı, sağ tuş ile işletim sistemi üzerinde kriptolanmış kaynaklara arama fonksiyonu ile kolayca ulaşabilmelidir.

### Varsayılan şifre atanması durumunda otomatik şifre değişikliğini algılamalı ve değişikliğe imkân vermelidir.

### Spesifik uygulamaların ürettiği dosyaların kriptolanması sağlanabilmelidir.

### Uygulama ile birlikte hangi dosya uzantısına sahip dosyaların otomatik kriptolanması sağlanabilmelidir. Kriptolama için kullanılacak anahtar belirlenebilmelidir.

### Kritpolanması hedeflenen USB belleklerin tamamı veya belli boyutu kriptolanabilmelidir.

### Kriptolanan USB belleklerin şifre ile şirket dışı bilgisayarlarda açılması sağlanabilmelidir.

### Şifrelerin uzunluğu, kullanılabilecek karakter tipleri, ne sıklıkla değiştirilebileceği, kullanılamayacak karakterler (örneğin: kullanıcı adı) gibi ayarlar politika ile belirlenebilmelidir.

### Olası şifre unutmalarına karşı challenge/response mantığıyla kurtarım senaryoları desteklenmelidir.

### Harici USB disklerde device ID ye göre kripto politikalarının haricinde tutmak mümkün olmalıdır.

### CD/DVD lerin kriptolanması mümkün olmalıdır.

### Kriptolama süreçlerinin sisteme olan yükünü azaltmak için peformans değerleri girilebilmelidir. Örneğin maximum I/O utilization vb.

### Network paylaşımları üzerinden kriptolama işlemi yapılıp yapılmayacağı politikalarla belirlenebilmelidir.

### Network üzerinden encryption için bandwidth limiti belirlenebilmelidir. Latency limiti belirlenerek yavaş olan networkler için kriptolama pasif hale getirilebilmelidir.

### Şifrelenmiş network klasörlerine maksimum kaç kişinin erişebileceği belirlenebilmelidir.

### Box, Dropbox, Google Drive ve MS OneDrive üzerindeki dosyalar kriptolanabilmelidir.

### Offline çalışma senaryoları durumunda ilgili anahtarların localde geçici barındırılması mümkün olmalıdır. Belli süre sonra bu anahtarın silinmesi politika ile mümkün olmalıdır.

### Kriptolama algoritması için en az AES -256 bit desteklemelidir.

### Kriptolama anahtarları yaratılırken ne zaman expire olacağı belirlenebilmelidir.

### Kripto anahtarları kullanıcıya, kullanıcı grubuna, organizational unit’e ya da bilgisayara atanabilmelidir.

### Herhangi bir doya sağ tuş ile kriptolanabilmeli ve bu yolla o dosyaya has şifre atanabilmelidir. Yaratılan bu hazır paket ilgili kişi tarafından şifresi bilinmesi durumunda açılabilmeli ve dosyaya erişilebilmelidir

* 1. **AĞ TABANLI ATAK ÖNLEME SİSTEMİ**

### Sistem üzerinde saldırı tespit ve engelleme amaçlı olarak su port dagılımlarını desteklemelidir:

### 8 adet 1 Gbps hızında bakır arayüz hazır gelmelidir. Bu hazır portlar Fail-Open ozelliğine sahip olmalıdır.

### En az 2 adet Fixed 10 GigE/1 GigE (SFP+) Port hazır gelmelidir.

### En az 2 adet network I/O modul takılabilmeli ve bu modullere en az aşağıdaki konfigurasyonlarda port tipleri saglanabilmelidir.

### 4-port 10 GigE/1 GigE SR (dahili fail-open özelliği ile)

### 4-port 10 GigE/1 GigE LR (dahili fail-open özelliği ile)

### 8-port (SFP+/SFP) 10 GigE/1 GigE,

### 6-Port 1000Base-T 1GigE (dahili fail-open özelliği ile)

### 4-port (RJ45) 10GigE/1 GigE (dahili fail-open özelliği ile)

### En az 1 adet 10 Gbps/1 Gbps RJ45 yönetim portu,1 adet responce port ,1 adet konsol portu ve 2 adet USB port olmalıdır.

### Sistem üzerinde 2 adet 10GB MM fail open kitli I/O modül takılı olarak gelecektir.

### Sistemin performansı (throughput) en az 3 Gbps ve eş zamanlı oturum sayısı en az 4.000.000 olacaktır.Atak anında cihazın ağ üzerindeki bekletme süresi en fazla 100 microsn olacaktır.

### Sistem, donanım ve yazılım bütününden oluşacaktır.. Sunulacak çözüm UTM veya yeni nesil firewall modulu şeklinde olmayacaktır.

### Sistem, katman iki (layer 2) seviyesinde çalışacaktır. Ağ üzerinde sistemin varlığı atak yapan tarafından herhangi bir şekilde algılanamayacaktır. Monitor portları hiç bir şekilde IP adresi içermeyecektir.

### Sistem üzerinde trafiği dinleyen fiziksel port bazında, VLAN ID ya da IP aralığı bazında ayrı ayrı politikalar uygulanabilecektir.

### Önerilen port tiplerine uygun olarak Fail-Open kitler önerilecektir. Fail-Open kitler olası arıza,güç kesintisi ve cihazın kapasitesinin üzerinde trafik oluşması durumunda devreye girecektir..

### Atak önleme sistemi Inline,span ve tap modlarında çalışabilmelidir.

### Önerilen donanım yedekli güç üntesi içermelidir.

### Istenilmesi durumunda aktif-aktif ve aktif-pasif yedekli çalışma tekniklerini desteklemelidir.

### İmza, anomali, istatiksel tespit ve DoS/DDoS tekniklerini bir arada kullanarak atak tespiti ve önleme yapacaktır.

### Yeni çıkan atak imzaları İnternet üzerinden otomatik veya manuel olarak indirilebilecektir.

### Cihazın, üzerinden geçen trafiğin durum kontrolü için kullanacağı yöntemlerden en az aşağıda sıralanan yöntemleri içerecektir:

### IP Defragmantation ve TCP Stream Reassambly

### Anomaly detection

### Signature-based detection (üretici temelli,el ile imza ve snort imzaları)

### Reputation-based detection

### Heuristic bot detection

### Multi-attack correlation

### Layer 7 protocol detection

### Advanced evasion protection

### Protocol Normalization

### DoS ve dağıtık servis dışı bırakma (DDoS) ataklarını istatistiki eşik değer ile tespit edebilecek, algılayıcı (sensör) tabanlı öğrenim/profil ve DoS profilleri tabanlı olarak tespit edebilecek ve kesebilecektir. Connection limit tanımlanabilecek ve limit üzeri trafikler engellenebilecektir.En az 5000 farklı DoS profilini saklayabilir ve inceleyebilir yapıda olacaktır.

### LOIC gibi karmaşık DdoS atak araçlarına karşı özel koruma teknikleri içermelidir.

### Brute force,Host sweep,Finger printing,Port scan,Service sweep gibi atak öncesi tespit ve ele giçrme tekniklerine karşı özel kural setleri içermelidir. Bu koruma tekniklerinin tespit istatistikleri ayarlanabilir yapıda olmalıdır. Örneğin aynı kaynaktan 5 sn de 10 farklı şifre denemesi yapılması durumunda ilgili saldırgan belirlenen süre boyunca karantinaya alınabilmelidir.

### El ile özelliştirilmiş keşif atakları yazılamaya uygun alt yapı sağlanmalıdır.

### DNS flood ve DNS poisining tekniklerine karşı izam yöntemleri dışında özel koruma mekanizmaları içermelidir.

### Interface seviyesinde antispoof ayarı yapılabilmelidir.Özellikle DoS/DdoS ataklarında kullanılan Ip spoof mekanizmaları tespit edilebilmelidir.

### Syn ataklarına karşı istatistiksel yöntemler dışında SYn cookie ve syn proxy method larını kullanabilmelidir.

### Vlan,Double vlan,MPL , fragmanted ve unfragmented trafik örneklerinde Jumbo frame desteklenmeli ve atak tespiti yapabilmelidir.

### IPv6,V4-in-V4, V4-in-V6, V6-in-V4, V6-in-V6 tunnel ,MPLS,GRE,Q-in-Q Double VLAN desteği olmalı ve bu tunel tekniklerinde atak tespiti yapabilmelidir.

### OS fingerprinting özelliği ile IPS üzerinde oluşan olaylara ait source ve destination lar için OS tespiti yapılabilmeli ve olay ekranlarında bunlar sorgulanbilmelidir.

### Exploit teknikler arasında en az aşağıdaki tiplerde saldırı koruma tekniklerine sahip olmalıdır.

### Protocol Violation

### Buffer Overflow

### Shellcode Execution

### Remote Access

### Privileged Access

### Probe

### DoS

### Evasion Attempt

### Arbitrary Command Execution

### Code/Script Execution

### Bot

### Trojan

### DDoS Agent Activity

### Backdoor

### Worm

### Virus

### Read Exposure

### Write ExposureAudit

### Sensitive Content

### Phishing

### Potentially Unwanted Program

### Önerilecek IPS sistemi SSL ile kriptolanmış trafik’i açabilmeli ve atak tespiti yapabilmelidir.

### Bandwidth kontrol özelliği olmalıdır.Bu amaçla Rate limiting, DiffServ tagging ve

### VLAN 802.1p tagging özellikleri kullanılabilmelidir. Band genişliği kontrolü port ve servis temelli uygulanabilmelidir.

### HTTP response atak tiplerine karşı özel koruma teknikleri içermelidir. Bu özellikler istenilen port seviylerinde uygulanabilir olmalıdır.Özellikle istemcilerin malicious web siteleri üzerinde oluşabilecek saldırı tekniklerinin önlenmesi sağlanmalıdır. Örneğin encoded pdf ler içersindeki zararlı atak kodlarının tespit edilmesi.

### Önerilen IPS sistemi davranışsal malware tespit motrouna sahip olmalıdır. Şüpheli dosyaları ozet bilgileri çıkarılabilmeli ve bu ozet bilgilerin üreticinin bulut sistemine sorulmasına mütakip gerekli tespit ve aksiyonlar alınabilmelidir.Bu özellikler port temelinde uygulanabilir olmalıdır.

### Connection limit kuralları reputation servis ve geo-location parametreleri ile desteklenebilmelidir. Örneğin X ülkesinde ilgili destination ip ye sn de 100 connection açılabilir ve bu açılan ip ler high risk içermemelidir denebilmelidir. Özellikle DoS atakları açısıdan bu tip kombinasyonlar kullanılabilir olmalıdır.Aksiyon olara drop ve dny dışında quarantine uygulanabilir olmalıdır.

### Önerilen IPS sistemi L7 firewall özelliğine sahipp olmalıdır.1000 nin üzerinde uygulama bu yolla denetlenebilir olmalıdır.Bu yolla ilgili iç kaynakların internet eişiminde kullandıkları uygulamalar tespit edilebilmeli ve bloklanabilmelidir. IPS dashboardları hangi uygulamaların ne miktarda trafik oluşturduğunu gösterebilmelidir. Firewall kurallarının çalışabileceği zamanlar ayarlanabilmelidir.

### IPS sistemi davranışsal web application server koruma özelliğine sahip olmalıdır. Bu sayede özellikle HTTP ve HTTPS trafikleri içersinde gerçekleşen SQL Injection atak tipleri tespit edip engellenebilmelidir.

### Advanced Botnet detection özelliği ile oluşan olaylar kendi içersinde korele edilerek CCC ve Zombi sistemlerin tespiti mümkün olmalıdır. Tespit ve raporlama için gerekli hassasiyet ayarı yapılabilmelidir.

### Önerilen IPS sistemi FLOW v5 ve V9 verisi üretebilmeli ve çözümle birlikte sağlanan anomaly sistemine aktarılabilmelidir. Flow verileri üzerinde ağ anomalileri tespit edilebilmelidir. Anomaly sistemi Vmware ESX platformunda çalışabilir yapıda olmalıdır.Bu çözüm aynı zamanda switch lerin ürettiği netflow verileride desteklemeli ve korele edebilmelidir.Anomaly çözümü en az aşağıdaki bilgileri sunabilmelidir.

### İstemciler arası trafik bilgileri

### Bilinmeyen worm ve smtp botnelerin tespiti

### Ağ üzerinde dolaşan IP ler,servisler,portlar ve protokoller

### Port scan ve host sweep lerin flow data ile tespiti.

### Istemcilerin standart olmayan uygulama kullanışlarının tespiti

### Ağ üzerindeki yeni varlıkların tepiti ve uyarılması

### Ağ üzerindeki IP lerin risk durumlarının reputation servis ile tespiti

### Oluşan ağ trafiğinin miktarı

### En çok trafik oluşturan istemciler

### Interface bandiwdth durumları(Utilization,throughput)

### Oluşan olay bilgilerinde AD kullanıcılarının tespit edilmesi.(istemci ajanı gerektirmeden)

### IPS sistemi tunelleme yapan P2P uygualamalarını tespit edip engelleyebilmelidir.

### İkinci katman (OSI 2) “ARP Spoofing” atakları tespit edilip kesilebilecektir.

### En az 170 Protokolu tanımalı ve decode edebilmelidir.Bu yolla protokol anomaly ler tespit edilebilmelidir.

### Port temelli olarak asimetrik trafikler içerisinde atak tespiti ve engellenmesi yapılabilmelidir. Bu yolla belli port aralıkları asimetrik trafik incelemesi yapabilecek şekilde konfigüre edilebilmelidir.

### Trinoo, Tribal flood network, TFN2K, Stacheldraht, Trinity, Mstream gibi DoS atak araçlarına karşı özel koruma tekniklerini barındırmalıdır.

### IPS sistemi TCP syn attack, TCP full connect attack, TCP ACK/FIN attack, TCP RST attack, DNS flood attack, UDP flood atttack ve ICMP flood attack larına karşı profil temelli DoS/DdoS koruması sağlamalıdır.

### Bilinmeyen uygulama temelli flood saldırıları için elile özel imza yazmaya imkan tanımalıdır.

### Snort temelli imzaların eklenmesine imkan sağlamalıdır.

### Syn Cookie nin aktik olabileceği yön ayarlanabilir olmalıdır.(inbound,outbound seklinde)

### X-Forwarded-For (XFF) HTTP header parsing özelliği ile proxy arkasından yapılan ataklarda istemcilerin gerçek ip lerinin tespiti mümkün olmalıdır.

### Smtp ve http trafiği içersindeki encoded içerikler zararlı kod ve ataklara karşı denetlenebilmelidir.

### MS RPC ve SMB protokolleri için segmente ve fragmente iletişim teknikleri içersinde atak tespiti ve engellenmesi mümkün olmalıdır

### IPV6 desteği tam olmalı ,atakların tespiti dışında yönetim portunda IPV6 adresleri ayarlanabilmelidir

### Önerilen çözüm aynı üreticin malwareforensic ürünü ile entegre çalışabilmelidir. Tespit edilen bilinmeyen kod lar otomatik olarak IPS sistemi tarafından kesilebiliyor olmalıdır.En az http,ftp ve smtp protokolu bu operasyon için kullanılabiliyor olmalıdır.

### Yönetimsel ve raporlama amacıyla fonskiyonel farklılıklar olması kaydıyla sensor üzerinden CLI ve merkezi yönetim yazılımı kullanılabilir olmalıdır.

### Merkezi yönetim yazılımı Windows 2008 temelli olup arka planda kendisine has Mysql veritabanını kullanıyor olmalıdır.

### Algılayıcı (sensör) ve yönetim yazılımı SSL ile şifrelenmiş bir hat üzerinden iletişim kuracaktır. Yönetim yazılımı detaylı istatistiksel raporlar üretebilemeli ve olusan raporlar mail ile otomatik alıcılara gonerilebilmelidir.Yönetim arayüzüne HTTPS üzerinden güvenli kanal ile ulaşılmalıdır.

### CLI üzerinden yapılandırmaya elvermelidir.

### Merkezi yönetim yazılımı en az 2 adet IPS cihazını yönetebilecek şekilde lisanslanmalıdır.

### Yönetim yazılımı üzerinden anlık atakların izlenmesi mumkun olmalı bu amaçla olası filtrelerle ilgili olay kaydına ulaşılabilmelidir. Aynı zamanda geçmişe dönük istatiksel raporlar alınabilmeli bunlar otomatize edilebilmeli ve ilgili kullanıcılara otomatik mail ile ulaştırılabilmelidir.Oluşturulan raporlar HTML ve pdf olarak alınabilmelidir.

### Yönetim yazılımı farklı rollerde sistem yöneticileri atayabilmelidir.

### Sensor ler üzerinde sanal IPS tanımlama imkanı sağlanmalı bu yolla tanımlanan sanal IPS lere yönetimsel anlamda farklı rollerde cok sayıda sistem yöneticisi atanbilmelidir.Her bir sanal IPS e ozel atak ve DoS politikası atanabilmelidir.

### Gereğinde delil amaçlı kullanılmak üzere detaylı trafik log’u ürettirilebilmelidir.(TCPDUMP seviyesinde). Üretim CLI ile olabileceği gibi yönetim GUI si üzerinden olabilmelidir.

### GUI ye ulaşabilecek IP ve IP blokları tanımlanabilmelidir.

### Merkezi yönetim yazılımına ulaşım için kimlik doğrulama mekanizmalarından LDAP,Radius ve tacacs kullanılabilir durumda olmalıdır.

### Merkezi yönetim yazılımı gerektiği takdirde yedekli çalışabilecek mimaride olmalıdır

### Atak olaylarını içeren ekran elile değiştirilmeye imkan tanımalaı bu yolla sistem admin kendisine özel dashboard ları olusturabilmelidir.

### Olay ekranlarında Layer-7 datası izlenebiliyor olmalıdır.

### Olay ekranları drill down menu yapısını desteklemeli fronsic arastırmalar çok kolay bir şekilde ilişkilendirilmiş sorgulama teknikleri ile destekleniyor olmalıdır.

### Atak olaylarına karşı block,icmp unread,TCP reset(source,destination,souce/destination seklinde) ve karantina aksiyonları alınabilmelidir. Karantina süreleri ayarlanabilir yapıda olmalıdır.

### Atak olaylarının oluşması durumunda snmp,syslog ve e-mail uyarıları oluşturulabilmelidir.SNMP v3 desteklenmelidir.

### Atak imzaları ile ilgili olarak CVE, Bugtrack, CERT ve NSP gibi endüstri standartları listelebiliyor olmalıdır.

### Atak imzaları ile ilgili politikalar oluşturulurken atak imzaları kategorize edilmiş olmalıdır. Örneğin sadece P2P imzaları,malware ler,phising ile ilgili ataklar kolayca listelenebiliyor olmalı ayrıca sadece özel bir kelime aranabiliyor olmalıdır. Elile özel filtrelere yazmaya imkan tanımalıdır. Ornegin son 2 imza guncellemesi arasındaki farklar nelerdir seklinde.

### Gelen imzalarla birlikte üreticinin önerdiği imza tipleri gerekirse otomatik aktif ve block şeklinde kullanılabilmelidir.

### Atak önem seviyeleri el ile değiştirilebilir yapıda olmalıdır.

### Bir atak patterninin birden fazla imzayı tetiklemesi durumunda false-positive i azaltmak adına sadece high risk olanların bloklanması sağlanabilir olmalıdır.

### IPS cihazının cpu,throughput, interface throughput ,trafik flowları gibi performans değerleri göresel ve grafiksel olarak izlenebiliyor olmalıdır.

### Belli trafik örnekleri için atak imzalarında ayrıştırma yapılabiliyor olmalıdır veya belli trafik örnekleri için tamamen IPS denetiminden çıkarılma mümkün olmalıdır.

### Bulk edit yöntemi ile birden fazla atak imzasının aynı anda değiştirilmesine imkan tanımalıdır.

### Oluşan olaylar realtime olarak izlenebilmeli oluşan bir olay istenilmesi durumunda bloklanabilmeli yada belirlenen bir süre ile karantinaya alınabilmelidir. Karantinaya alından host lar ayrıca izlenebilmeli,karantina sureleri uzatılabilmeli yada serbest bırakılabilmelidir.

### Merkezi yönetim yazılımı aynı üreticinin zaafiyet tespit,Host IPS,risk tespit sistemi ile entegre olabilmeli bu yolla ortak aksiyonlar alabilmelidir. Örneğin IPS admin oluşan olaylar üzerinden belli bir ip sahibini otomatik zaafiyet tarama testinden geçirebilmeli ve sonuçları yine aynı ekrandan görebilmelidir.Son kullanıcılarda çalışan HIPS modulu ile ise korelasyon imkanı sağlanmalı ve forensic araştırmalar yapılabilmelidir.

### Hazır rapor şablonları dışında elile özelleştiriliş alanlar sayesinde kişiye özel rapor şablonları oluşturmak mümkün olmalı,grafiksel ve geçmişe dönük görsel raporlar oluşturulabilmelidir.

### Oluşan atak olaylarında ip lerin sahip olduğu risk seviyeleri(reputation servisden alınan) ve ülke bilgileri görülebiliyor olmalıdır.

### Ajan gerektirmeyen yöntemle oluşan atak olaylarında source ve destination ip bilgileri görülebilmeli ve raporlanabilmelidir.

### Merkezi yönetim yazılımına ait tüm loglar ve konfigurasyonlar kolayca yedek alınabilir ve ihtiyac olması halinde geri dönüme imkan tanımalıdır. Bunun gereklı GUI sağlanmalıdır.

### Kritik sistem sorunları durumunda otomatik uyarı oluşturulabilmelidir(snmp,syslog-e-mail)

### Merkezi yönetim yazılımı veritabanı otomatik bakım prosedurlerini içermeli,otomatik arsivleme ve yedeklemeyi desteklemelidir.

### Oluşan olaylar bir IPS admin tarafından farklı adminlere incelenmesi adına atanabilmelidir.

### Gerektiği durumda cihaz tamamen Layer2 moda çekilip trafik denetleme dışında tutulabilmelidir.

### Merkezi yönetim sistemi üzerinde her bir IPS yöneticisinin ne yaptıgı audit log lar üzerinden detaylı incelenebilmelidir.

### Sensor firmware leri TFTP yoluyla veya merkezi GUI tarafından güncellenebilir olmalıdır.

### Son kullanıcı 7x24 üreticiye sorunlarla ilgili e-mail veya telefon ile bildirimde bulunabilmelidir

### Sistemin, bakım ve güncelleme desteğiyle kesin kabul tarihinden itibaren en az 1 (BİR) yıl süre ile garantisi olacaktır

* 1. **VERİ SIZINTISI ENGELLEME YAZILIMI**

### Veri Sızıntısı Tespit ve Engelleme Sistemi, ağda bulunan KURUM bilgilerinin kaybını ve istenmeyen kişiler tarafından sızdırılmasını, kurulu olduğu tüm kullanıcı bilgisayarlarında, sunucularda, bulut ortamında var olan depolama alanlarında, mail sunucularında tespit edip engelleyecektir.

### Teklif edilecek olan veri sızıntısı engelleme yazılımı minimum 1400 kullanıcıyı kapsayacak şekilde 1 yıl üreticinin destek paketi dâhil tekliflendirilecektir.

### Önerilen çözüm ile ilgili, teklif verecek olan firma, teklif verdiği çözüm ile alakalı kendi bünyesinde yetkin ve tüm teknik sertifikasyonlarını tamamlamış olan personel bulundurmalıdır.

### Önerilen çözüm ile ilgili, teklif verecek olan firmanın teklif verdiği çözüm ile ilgili daha öncesinde benzer proje deneyimi olmak zorundadır. KURUM tarafından referans istenildiği taktirde firma tarafından bu bilgilerin paylaşılması zorunludur.

### KURUM, teklif verecek olan firmadan proje süresince veya daha sonrasında lokal bakım, destek, danışmanlık, eğitim gibi talepleri olduğu taktirde firma bunu kendi bünyesindeki personeli ile hizmet verebilecek yetkinlikte olması gerekmektedir.

### Teklif edilecek DLP çözümü son 3 yıla ait Gartner firmasına ait DLP değerlendirme raporlarında liderler konumunda olmalıdır.

### DLP ajanları Microsoft AD yapısı ile tam uyumlu çalışacaktır.

### Rol tabanlı yönetimi olacaktır. Yani yöneticiler farklı seviyelerde erişim ve yönetim hakkına sahip olacaktır.

### DLP ajanları en az aşağıdaki işletim sistemlerini hem 32 hem de 64 bit olarak çalışan tüm versiyonlarını desteklemelidir:

### Windows 7

### Windows 8

### Windows 8.1

### Windows 10

### Windows Server 2008

### Windows Server 2008 R2

### Windows Server 2012

### Windows Server 2012 R2

### Windows Server 2016

### Windows Server 2019

### Mac OS 10.11.x

### Mac OS 10.12.x

### Mac OS 10.13.x

### Mac OS 10.14.x

### Bilgi sızıntısı çözümünün merkezi yönetim yazılımı Windows Server 2008 R2, 2012, 2012 R2, 2016,2019 64-bit sunucular üzerinde çalışabilmeli, veri tabanı olarak Microsoft SQL Server 2008, 2008 R2, 2012, 2014, 2016 ve 2017 ile çalışabilmelidir.

### Bilgi sızıntısının denetlenmesi için kullanılacak son kullanıcı ajanı aynı zamanda donanım kontrolü yapabilmelidir.

### Donanım kontrolü modülü Blutooth, cd/dvd, floopy disk, imaging device, network adapter, pcmci adapter, tape drives, usb drives, wireless ethernet donanımları ön

### tanımlı olarak gelmeli ve gerekirse elile yeni donanım tipleri sisteme tanıtılabilmelidir. Bu amaçla donanım GUID leri kullanılabilmelidir.

### Donanım tipleri en az bus tipi, donanım adı, seri numarası, instance ID, compatible ID, vendor ID/Product ID parametreleri ile özelleştirilebilmelidir. Tanımlanan donanım tipleri donanım erişim kontrollerinde kullanılabilmelidir.

### Donanım kontrolleri bloklama, read-only, notify veya monitor aksiyonları ile sonuçlandırılabilmelidir. Oluşan tüm olaylar merkezi rapor arayüzünden izlenebilmelidir. (Kim ne zaman, hangi donanımı kullandı? Bu donanımın özellikleri nedir? Vb.)

### Harici depolama aygıtları üzerinde bulunan ve istenmeyen dosya tiplerine göre erişim engellenebilmelidir.

### Son kullanıcı gerekçesine (justification) göre bloklama olasılığındaki bir vaka devam edilebilmeli ve kurallarla sağlanmalıdır.

### Kural setlerine bağlı olarak en az aşağıdaki aksiyonlar alınabilmelidir:

### Apply RM Policy

### Monitor

### Notify User

### Request Justification

### Store Evidence

### Encrypt

### Block

### Tüm kurallar Active Directory grup ve kullanıcılarına, lokal kullanıcı ya da makinaya has atanabilmelidir.

### Kurallar online ya da offline duruma göre özelleştirilebilmelidir. Bu kapsamda kullanıcı KURUM dışında olduğu zaman farklı bir politika ile kısıtlanabilmelidir.

### Harici diskler üzerinde read-only politika kapsamında belirlenen uygulamalar politika harici tutularak çalıştırılması sağlanabilmelidir.

### Önerilen çözüm Adobe LiveCycle Rights Management ile entegre çalışabilmelidir.

### Ajan seviyesinde sızıntının izlenmesi/engellenmesi amacıyla bilgilerin şu yollarla özelleştirilmesi mümkün olmalıdır:

### Uygulamaların bilgi içeren dosyalara ulaşımlarının denetlenmesi. Uygulama tipleri e-mail client, Explorer, IM, P2P, Web browser, Media Burner, MS Office, Scanner, Winrar gibi hazır uygulama kalıpları desteklenmeli. Gerekirse bu listeler el ile genişletilip değiştirilebilmelidir. Uygulamalar çalıştığı PC üzerinden gösterilerek listeye dâhil edilebilmelidir. Uygulamalar filename, hash, product name, vendor name, working directory parametreleri ile özelleştirilip tanıtılabilmelidir.

### Dokümanlar; Title, subject, Author, Date Created, dat-we modified, Last Saved date gibi parametrelerle özelleştirilebilmelidir.

### Bilginin gitmesinin sakıncalı olduğu e-mail adresleri ya da domainler hedef olarak tanımlanabilmelidir.

### Ön tanımlı dosya tipleri dışında elile yeni tipler sisteme tanıtılabilmelidir.

### Ağ üzerinde çalışan dosya sunucuları tanımlanabilmelidir.

### Network IP blokları dışında Network port grupları tcp/udp seviyesinde tanımlanabilmelidir.

### Network yazıcılar tanımlanabilmelidir

### Web Uploadlar için hedef URL ler tanımlanabilmelidir. Bu yolla bilgilerin Web upload yolu üzerinde denetlenmesi mümkün olmalıdır.

### Aynı üreticiye ait dosya, klasör ve usb şifreleme yazılımının kullanılması durumunda kullanıcı tarafından dosyanın harici bir depolama aygıtına çıkarılması durumunda şifreleme yapabilmelidir.

### Ön tanımlı sözlüklerin dışından el ile bilginin takibi açısından politikalarda kullanılabilecek özel sözlükler tanımlanabilmelidir.

### Kredi kartı numarası, TC kimlik, Mac adres, Ip adres, tarih gibi yapısı

### kurallanabilen tanımlar ön tanımlı gelmeli, regex gibi yöntemlerle özel kelime kalıpları hazırlanabilmeli ve kurallarda kullanılabilmelidir.

### İzlenmesi istenilen bilgiler lokasyon bazında ya da belirlenen uygulamaların ürettiği bilgiler şeklinde işaretlenebilmelidir (Tagging). Bu yolla kurallarla bu bilgilerin hareketleri denetlenebilmelidir.

### Bir dosya üzerinde birden sınıflandırma etiketi tanımlanabilmelidir.

### Daha önceden çeşitli kriterlerle(Dosya tipi, uzantı, dosya detay özellikleri vs...) belirlenen bilgiler ağ ortamında olmaması gereken kaynaklarda bulunması durumunda (discover) otomatik olarak bu dosyalar karantinaya alınabilmeli, kriptolanabilmeli, sınıflandırabilmeli, fingerprint yaratabilmeli, delil amaçlı kayıtlanması ya da sadece monitor yöntemi ile olay kayıt bilgisi oluşturulabilmelidir.

### Bilgilerin dışarı çıkması amacıyla isminin değiştirilmesi, sadece bir kısmının yollanması, paragrafların yerlerinin değiştirilmesi gibi bilgi manipülasyonları fark edilebilmeli ve engellenebilmelidir.

### Bloklama olayları, gerektiği noktada karşılıklı kod çözümüne dönük üretim yöntemleri ile geçici serbest bırakma sağlanabilmelidir (release code).

### Bilgiler; dosyalara ulaşım (file access), geçici hafızaya alma (clipboard), E-posta ile yollanması, Web upload ile gönderilmesi, screen capture, uygulamaların bilgiye ulaşması, Yazıcıdan yollanması, harici disklere yazılması, bulut uygulamaların ajanları ile dosyaların gönderimi, pdf/image writer ve belirlenen network ve portlar üzerindeki hareketleri sırasında takip edilebilmeli ve gerektiğinden kesilebilmelidir.

### Harici disklere yazma kuralları incoming a da outgoing yönünde kontrol edilebilmelidir.

### Son kullanıcı ajanı en az aşağıdaki bulut sistemleri üzerinde koruma tekniklerini desteklemelidir.

### Box

### Dropbox

### GoogleDrive

### iCloud

### Office 365

### OneDrive (personal)

### Syncplicity

### Politikaların genelinde monitor modunda olmaları için özel kullanıcı grupları tanımlanabilmelidir.

### Politikalar uygulanmadan önce analizden geçirilebilmeli olası kural ihlalleri arayüz üzerinden gösterilebilmelidir

### Oluşturulan politikalar export edilebilmelidir.

### Yönetim arayüzü üzerinden tüm kayıtlar takip edilebilmeli, kayıtlar için filtrelere yazılıp istenilen kayıda hızlı ulaşılması sağlanmalıdır.

### Yönetim yazılımının raporlama aracı ile önerilen çözümle ilgili detaylı istatistiksel raporlar alınabilmeli bunlar istenildiği takdirde html, csv, xml, pdf olarak kayıt edilebilmelidir.

### Active Directory e yeni üye edilen bir sisteme otomatik ajan basılabilmeli ve bunlar özet/rapor ekranlarından takip edilebilmelidir.

### Yönetim yazılımı ağa yeni katılan ve Active Directory nin bir üyesi olmayan sistemleri tespit edebilmeli ve merkezi yönetim yazılımı üzerinden bunlara MS Windows yetki yetenekleri çerçevesinde ajan basılabilmelidir.

### MS SharePoint Portal gibi doküman yönetim uygulamalarını destekleyecek, bunlarda bulunan bilgileri otomatik olarak tarayacaktır. MS Exchange dokuman yönetiminin desteklenmediği durumda Outlook uygulamasında local pst taraması desteklenmelidir

### DLP çözümünün keşif(discover) modülü en az aşağıdaki bilgi alanlarını desteklemelidir:

### Box

### File Server

### SharePoint

### MS-SQL Veritabanları

### Oracle Veritabanları

### MySql commercial versiyonları

### Discovery işlemi en az aşağıdaki amaçlarda kullanılabilmelidir:

### Hassas verilerin keşfi ve sınıflandırılması

### Tespit edilen verilerin özet bilgilerinin oluşturulması ve sonrasından kullanılması

### Hassas verilerin tespit edilmesi durumunda düzeltme amacıyla dosyaların harici bir alana kopyalanması ve taşınması

### Belirtilen zaman aralığında örneğin boş dosyaların tespiti, dosyalardaki permissionların tespiti ve dosya değişimlerinin tespiti.

### Keşif taramalarında bandwidth limitasyonu ayarı yapılabilmelidir.

### Keşif taramalarının geçmiş sonuç bilgileri takip edilebiliyor olmalıdır.

### Keşif taramaları sonucunda GUI üzerinde analitik raporlar üretilebilmelidir.

### Keşif taramalarında en az aşağıdaki filtreler kullanılabilmelidir:

### File Extension: Elile tanımlamaya imkân sağlamalı ve hazır gruplara sahip olmalıdır. Örneğin: Database files, executable files, Audio files, Source code, Script File vb…

### File Information: File size, File name, File Owner, File Size, Date created, Date modified, Date Accessed vb…

### E-posta kontrolü için MS Outlook 2010, 2013 SP1, 2016, 2019 ve 365 sürümleri ile tam entegre olabilmelidir.

### Discovery kuralları ile hassas bilgilerin istemciler üzerinde tespit edilmesi ve tespit sonrası bu dosyaların monitor edilmesi, karantinaya alınması, kriptolanması, fingerprint oluşturması, sınıflandırma yapması ya da hak yönetim politikası uygulaması mümkün olmalıdır.

### Keşif modülü OCR tekniği ile resim dosyalarında sınıflandırma yapabilmelidir.

### DLP sisteminin ağ modülü switch ler üzerinde verilen span port (veya tap cihazı ile) vasıtasıyla trafiği dinleyebilmeli ve trafik karakteristiğini çıkarabilmelidir. Monitor modülü en az aşağıdaki protokolleri desteklemelidir:

### SMTP

### IMAP

### POP3

### HTTP

### LDAP

### TELNET

### FTP

### IRC

### SMB

### HTTPS (Web Gateway span model veya TAP cihazı ile)

### Monitor modülü Vmware dâhil yük dağılımı yapacak şekilde kümele tekniği ile çalışabilmelidir.

### Monitor modülünün yakaladığı ip olaylarında MS AD kullanıcı bilgileri eşleştirilip görüntülenebilmelidir.

### Bilgi sızıntısı çözümünün ağ seviyesinde çalışan prevent modülü email ve web trafiğini bloklayabilmelidir. Bu amaçla mevcut proxy sistemi ile ICAP protokolü entegre olabilmelidir. EMail trafiği için ise MTA modda çalışmalı ve X-header eklentileri yapabilmelidir. Prevent modülü yük dağılımı yapacak şekilde kümeleme modunda çalışabilmelidir.

### Mobile Device Management, Microsoft Exchange ActiveSync ve Microsoft Office 365 ActiveSync ile entegre çalışabilmelidir.

### Önerilen çözüm aynı üreticinin CASB çözümü ile entegre çalışabilmelidir.

### DLP ajanı istenilirse kural ayarları ile Windows SafeMode seviyesinde çalışabilir olmalıdır.

### Çözüm aynı üreticiye ait lokal merkezi istihbarat sistemi ile entegre olmalı ve böylelikle zararlı bir yazılım hassas veriyi dışarı çıkartmak isterse engelleyenbilmelidir.

### KURUM içersinde hâlihazırda kullanılmakta olan log yönetim platformuna syslog vasıtası ile logları iletebilecektir.

### Bilgi sızıntısı çözümü manual ve otomatik sınıflandırma tekniklerini desteklemelidir.

### Manual sınıflandırma ile son kullanıcılar en az Microsoft Office (Microsoft Word Microsoft PowerPoint, Microsoft Excel), XPS dokuman, PDF, Audio ve video formatları (AIF, AIFF, AVI, MOV, MP2, MP3, MP4, MPA, MPG, MPEG, SWF, WAV, WMA, WMV), Grafik ve imaj formatlar(PNG, JPG, JPEG, TIF, TIFF, DNG, WMF, PSD) desteklenmelidir. Email sınıflandırma için ise MS Outlook desteklenmelidir.

### Bilgi içeriğine göre email iletişiminde eklenen dosya otomatik sınıflandırmayı desteklemelidir.

### İçerik sınıflandırma için en az aşağıdaki teknikler desteklenmelidir:

### Sözlükler: Hazır gelen şablonlar dışında elile tanımlamalara imkân sağlamalıdır. Sözlük içeriklerinin tanımlamalarında kelime başlangıçları, sonları ve case sensitive gibi özellikler denetlenebilir olmalıdır.

### Advanced Pattern: Hazır gelene şablonlar dışında (TC kimlik no, IBAN, Kredi kart numaraları vb.) el ile tanımlamaya imkân sağlamalıdır. Bu amaçla Regex kullanılabilmelidir.

### Döküman özellikleri: Title, author, keyword, subject vb. filtrelerle tanımlanabilmelidir.

### File extension: hazır gelen şablonlar dışında elile tanımlamaya imkân sağlamalıdır.

### True File Type Grupları(html dosyaları, grafik dosyaları vb.): Hazır olarak gelen şablonlar kullanılabilmelidir.

### Application Templates: Hazır gelen uygulama şablonlarına (Installers, Firefox, Java compiler vb…) ek olarak eli le tanımlamaya imkân sağlamalıdır. BU amaçla command line, executable directory, file hash, file name, vendor name vb. kriterler kullanılabilmelidir.

### Son kullanıcı tanımlamaları

### Ağ paylaşımları

### URL listeleri

### Doküman kayıtlama tekniği ile hassas olan dökümanlar el ile sisteme upload edilebilmeli ve bu yolla fingerprint verileri çıkarılabilmelidir. Ayrıca Keşif taramaları yoluyla da belirlenen kriterlere istinaden otomatik olarak benzer işlem yapılabilmelidir. Bu bilgiler daha sonra koruma kurallarında kullanılabilmelidir.

### Beyaz liste kullanımıyla belirli dökümanlar sınıflandırma dışında tutulabilmelidir.

### DLP sisteminde Data-in-Use, Data-in-Motion ve Data-in-Rest olayları için hazır dashboard lar sağlanmalı ve ekranlar yoluyla ilgili bilgi sızıntılarının detaylarına inmek mümkün olmalıdır.

### Oluşan DLP olayları ile ilgili detaylı izleme arayüzü sağlanmalı bu vaka izleme ekranında en az aşağıdaki bilgiler sunulmalıdır:

### Oluşma zamanı

### Incident Type

### Severity

### Destination

### Actual Action

### Son kullanıcı bilgisi

### Computer name

### IP bilgisi

### Eşleşen politika

### Device Friendly Name

### Device Description

### Disk drive

### Device Class Name

### Disk drives

### Device Class GUID

### Compatible ID

### Instance ID

### Bus Type

### USB Class

### USB Serial Number

### Device Plug Local Time

### File System Type

### Volume Serial Number

### USB (VID/PID Codes)

### Audit log (Bu vakayı kimin incelediği)

### Vaka ile ilgili açık durumda olan CASE ler.

### Vaka ekranlarında delil bilgileri izlenebilir olmalıdır. (Örneğin: Clipboard da alınan dosyanın orijinal hali)

### Oluşan vakalar karşılığında uyarı mailleri oluşturulabilmelidir.

### Oluşan vakalarla ilgili arayüzden Case açılabilmeli ve ilgililere atanabilmelidir.

### Merkezi yönetim sistemi üzerinde farklı rollerde sistem yöneticileri tanımlanabilmeli.

### DLP süreçleri konusunda yetkilendirilebilmelidir. MS AD veya LDAP kullanıcı eşleştirmede kullanılabilmelidir.

### Help Desk alt yapısı ile merkezi olarak son kullanıcıların karantinaya alınmış olayları serbest bırakılmalı.

### Politika serbest bırakılabilmeli ve son kullanıcı ajanları uzaktan uninstall edilebilmelidir. Bunun için farklı kullanıcılar bu operasyon için tanımlanabilmelidir.

### Önerilen DLP çözümü doküman sınıflandırma amacıyla Titus ve BoldonJames, Azure Information Protection ürünleri ile tam entegre çalışabilmelidir.

### DLP çözümü Microsoft Right Management çözümü ile tam uyumlu çalışabilmelidir.

### Önerilen çözüm aynı üreticinin CASB çözümü ile entegre çalışabilmelidir. Bu sayede aynı yönetim konsolundan bulut için kural yazılabilmeli, kural ya da sınıflandırma bilgileri bulut ile paylaşılabilmelidir.

### DLP çözümü rest API alt yapısını sunabilmelidir.

### GUI üzerinden politikalar dâhil konfigürasyon yedeği alınabilmeli ve ihtiyaç halinde geri dönülebilmelidir.

### DLP yönetim sistemi üzerinde operasyonel olayların kayıtlarını izlemek mümkün olmalıdır.(Örneğin: Politika değişiklikleri, taramalarla ilgili atamalar vs.)

### Vaka analizlerinde hassas verilerin sistem kullanıcısı tarafından görülmesini engelleyecek teknikleri içerisinde barındırmalıdır.

* 1. **TRELLİX LOG YÖNETİM YAZILIMI LİSANS ALIMI**

### Yönetim, log toplama, ham log kaydetme modülleri fiziksel olarak sunulmalı, tek ekrandan yönetilmelidir.

### Sunulacak mimari yönetim, log toplama, ham log kaydetme modülleri için en az 5000 EPS değerinde hizmet verecek şekilde planlanmalıdır.

### SIEM çözümünde teklifin verildiği tarih itibarı ile ileride üreticiye ait sonradan satın alınabilecek uygulama ve veri tabanı aktivitelerini denetleyen modüllerin bulunması tercih sebebi olacaktır.

### Önerilen sistem gerçek zamanlı olarak korelasyon, benzer olayları aynı imza, aynı kaynak ve hedef IP doğrultusunda birleştirebilmeli ve bunun için ayrı bir ürüne ihtiyaç duymamalıdır. Olayları ait aktiviteleri tek tek RAW log biçiminde saklayabilmelidir.

### Tek bir klik ile orijinal log dosyasına ve raw log verilerine ulaşılabilmelidir. Tek bir GUI ile korelasyon, log ve olay araştırması, custom parser, raporlama imkanı sağlanmalıdır.

### Sisteme ait yönetim modülü alt modüllerin merkezi olarak tek noktadan yönetimine imkan tanımalıdır (Security Manager, Log Manager , Receiver, Reputation feed, reporting, creations of custom parsers..)

### Canlı ve tarihsel verilere ulaşım için kendisine ait native veri tabanı kullanılmalı bu amaçla 3’ncü parti veri tabanı (SQL temelli) ürünleri kullanılmamalıdır.

### Hızlı analitik araştırmalar için tüm index’ler primary memory ’de saklanabilmelidir

### Sistem yöneticisi, olaylara istinaden oluşan temel eşiklerin (Baselining) aşılması durumlarından haberdar edilebilmelidir.(uyarı gibi yöntemlerle) Bu eşikler otomatik olarak düzenli sistem tarafından oluşturulmalıdır. Baselining ile monitör edilen tüm aktiviteler, ağ kullanıcıları uygulamalara ait anomaliler ve tarihsel veriler üzerinde farkların incelenmesi mümkün olmalıdır.

### Korelasyon kuralları için kolay kullanılan ve öğrenilen GUI sağlanmalıdır.

### En az 260 adet ön tanımlı korelasyon kuralı bulunmalıdır. Bu kurallar güncellemelerle gelişen yapıda olmalı ve aktif olmalıdır.

### Sistemin firmware güncellemeleri ve yamaları GUI üzerinden kolayca yapılabilmelidir.

### Kural ve Geo Location güncellemeleri gerek internet gerekse manual yapılabilir yapıda olmalıdır.

### Yönetim sistemi zone kavramını desteklemeli bu yolla örneğin DMZ bölgesindeki log kaynakları farklı zone altında birleştirilebilmelidir.

### Önerilen SIEM GUI si hazır ve amaca özel dashboard ’lar barındırmalı, sistem yöneticisi kolayca yeni dahboard’lar ekleyebilmelidir.

### Yönetim ara yüzü üzerinden politikalar yaratılabilmeli, kurallar ve alertler oluşturulabilmeli, bunlara istinaden düzeltme(mitigation) yapılabilmelidir.

### Yönetim sistemi herhangi bir ek lisans veya çözüme gerek duymadan iş akışlarını destekleyen olay yönetim ve alarm alt yapısını desteklemelidir.(case management)

### Oluşan alarm’lar ayrı bir dashboard üzerinde kolayca izlenebilmeli, filtrelenebilmeli ve içerikleri görülebilmelidir.

### Sistem üzerindeki tüm sistem yönetici aktiviteleri (Audit) detaylı şekilde raporlanmalı ve filtrelenebilmelidir.

### Merkezi yönetim birimi harici helpdesk yazılımlarına SNMP ve Email üzerinden çağrı kaydı açabilmelidir.

### Her bir log kaynağı için ayrı storage pool tanımlanabilmeli bu yolla bu her kaynak için disk üzerinde farklı miktarda bir disk alanı rezerve edilebilmelidir. Bunun için kurum tarafından harici disk alanı sağlanacaktır.

### Her bir kayda ait olay tanımlarında, olaya ait atanan severity ve aggregation ayarları el ile değiştirilebilmelidir. Örneğin şu tip bir Windows event’i oluşursa; kayıtlama, aggregation yapma yada severity şu olsun gibi.

### Varlıklar üzerinde “String Nomalization” desteklenmelidir. Örneğin belli kalıplarlar tanımlanmış kullanıcı isimleri gerçek kullanıcı isimleri ile map edilebilmeli ve bu bilgiler raporlarda görülebilmelidir.

### Yönetim arabirimi zengin(en az 800) ön tanımlı raporlara sahip olmalı sistem yöneticisi el ile kendi raporlarını kolayca oluşturabilmelidir.

### Çözüm bağlamsal bilgiye göre olay zenginleştirmeyi desteklemeli bu yolla vulnerability assessment, identity, authentication management systems, privacy solutions gibi çözümlerle entegre olabilmelidir.

### SIEM çözümü PCI-DSS, HIPAA, NERC-CIP, FISMA,GLBA, SOX gibi standartları destekleyen hazır rapor şablonlarına sahip olmalı ve ekstra lisans gerektirmemelidir.

### Üretici tarafından otomatik ve ücretsiz olarak içerik paketleri sağlanmalı ve bu paketler ile farklı üreticilere ait Firewall ve Web Gateway ürünleri ile ürün bağımsız olarak kimlik doğrulama, Active Directory politikaları, Windows kimlik doğrulama, IPS/AntiVirus olaylarına ait özel içerikler sunulmalı. İçerik paketleri ile monitör, alarm, raporlama, izleme listeleri, değişkenler ve korelasyonlar kuralları otomatik olarak gelmeli.

### Merkezi yönetim arabirimi aşağıdaki liste seçeneklerini desteklemelidir:

### Statik Liste: Spesifik Kullanıcı, IP adres ve grup. Bu listelere el ile, dosya import yoluyla ya da API ile doldurulabilmelidir.

### Dinamik Liste: Regex, Database, Ldap aramaları

### Korelasyon kurallarına istinaden otomatik update edilen listeler

### Önerilen çözüm üzerinde dinamik listeler ile internet ortamında bulunan kaynaklardan otomatik olarak besleme yapılabilmelidir. Örnek olarak siber tehdit olarak daha önceden belirlenmiş IP adreslerinin otomatik olarak bir listede tutulmalı, liste güncellenmeli ve bu liste kullanılarak riskli aktiviteler tespit edilerek alarm üretilmeli, raporlanabilmeli. Güncelleme işlemleri otomatik olmalı ve MITRE Threat Information Exchange (TAXII) ve benzeri otoriteler desteklenmeli.

### Önerilen çözüm ile loglar üzerinde ilgili alanlardaki bilgiler internet ortamında bulunan kaynaklardan kolayca çağırılarak sorgulanabilmeli. Örnek olarak Firewall loglarında yer alan IP adreslerinin DShield.org, MXToolBox.com, Robtex.com, TrustedSource ve benzeri sitelerden otomatik olarak çağırılabilmeli.

### Önerilen çözüm aynı markaya ait antivirus, Network IPS ile entegre çalışarak olası risk senaryolarında bu güvenlik sistemleri üzerinde aksiyon alarak risk’i engelleyebilmelidir.

### Korelasyon kurallarına istinaden e-mail, görsel, sms gibi yöntemlerle uyarı oluşturulabilmelidir.

### En az 2 farklı korelasyon kuralı birleştirilerek tek bir sonuç üretilebilmelidir.

### SIEM appliance’lar en az FIPS 140-2 level 2 seviyesinde sertifikalara sahip olmalıdır.

### Olaylar üzerinden Geo Location bilgileri ile ülke raporları alınabilmelidir.

### Receiver modülü en az aşağıdaki tipteki cihazlardan log alabilmelidir:

### Identity and authentication Systems

### Firewalls

### Vulnerability Scanner

### Physical Security Devices

### IDS/IPS devices

### UTMs

### Switches

### Routers

### Applications

### Servers and workstations

### En az aşağıdaki yöntemlerle log alabilmelidir:

### Ftp

### Syslog

### Cifs

### Nfs

### OPSEC

### ODBC

### WMI

### Ajan yöntemi

### Snmp trap

### Flow

### HTTP

### Bilinmeyen ve desteklenmeyen log tipleri için SDK veya ek lisansa gerek kalmadan custom parser yazma imkanı sağlanmalıdır.

### Custom Parser için ek GUI ye gerek kalmamalıdır.

### Sistemden PDF, HTML ve CVS yapısında raporlar alınabilmelidir.

### Auto Discovery ile bilinmeyen log kaynakları tespit edilip otomatik olarak sisteme eklenebilmelidir.

### Ham (Raw) datalar için integrity kontrolü sağlanmalıdır. Ham veriler kurumun sağlayacağı harici disk alanında saklanacaktır.

### Log Manager üzerinde yapılacak raw data aramalarında strings (Örn:Confidential) ve integers(Örn:IP adres) ve regex kullanılabilmelidir.

### Log Manager için sıkıştırma oranı ayarı ile hem performans hem de kapasite planlaması yapılabilmelidir.

### Log Manager, lokal hdd, SAN, CIFS, NFS yoluyla storage pool yaratabilmelidir. Bu poollar log kaynakları temelinde özelleştirilebilmelidir.

### Log Manager üzerinden tarihsel ve arşivlenmiş veri üzerinde tarama yapmak mümkün olmalıdır.

### Merkezi yönetim arabirimi üzerinden delil araştırmaları yapılırken; farklı kaynaklardan kategorize edilmiş parametreler “ve, veya, değil” gibi mantıksal işlemlerle birleştirilebilecektir.

### Oluşan tehdit görünümlerinde Bugtrak, ICE, CVE gibi referans bilgileri gösterilebilmelidir

### Yaratılan kurallara istinaden oluşan olaylarla ilgili alarmlar oluşturulabilmelidir. Oluşan alarmlar; ilgili kişilere atanabilmeli, kayıtlanabilmeli, case açılabilmeli, görsel uyarı oluşturulabilmeli, sms ve e-mail atabilmeli, ozel bir script çalıştırılabilmelidir.

### Network cihazlarından gönderilen SNMP trapleri ve flow dataları sistem tarafından toplanabilmelidir.

### Çözüm ip temelli Ağ tarama özelliğine sahip olmalı bu yolla ağ içerisindeki varlıkların tespiti mümkün olmalıdır. Tespit edilen varlıklar otomatik gruplandırılabilmelidir

### Toplanan logların kaynağı ne olursa olsun normalizasyon desteklenmelidir.

### Uzun dönem log kayıtlarının rapor ve disk alanı açısından optimizasyonu nedeniyle log aggregation teknikleri desteklenmelidir.(Belli süre içerisinde gerçekleşen, aynı tipteki benzer olaylara ait kayıtların tek bir kayıt şeklinde gösterilmesi)

### Ara yüz üzerinde EPS değeri, log istatistikleri ve alarmlar görülebilecektir.

### Çözüm Active Directory ve/veya Radius kimlik doğrulama yöntemlerini kullanabilmeli bu yollar kullanıcı tanımları ile eşleştirmek mümkün olmalıdır. Ayrıca raporlarda, olay görünümlerinde ve korelasyon kurallarında AD yoluyla filtreleme imkanı sağlanmalıdır.

### Kullanıcılar için farklı gruplar tanımlanabilmeli, grup için yetkili kılınan device’lar, politikalar ve zone lar atanabilmelidir. Böylece grup içerisindeki bir kullanıcı yetkileri dahilindeki cihazlar, politikalar ve zone’lara erişimi sağlanmalıdır. Kullanıcılar kendi ara yüzlerini kişiselleştirebilecektir.

### Geo Location, IP kaynak ve hedefleri, Port, Application, Host gibi kriterleri istinaden izleme listeleri tanımlanabilmeli bu tanımlar alarm kuralları kapsamında kullanılabilmelidir. Dolayısıyla örneğin sadece bir IP bloğu ile ilgili oluşan olaylar belli eşik değerlerde olay oluşturması durumunda görsel ve işitsel uyarılar oluşturabilmeli ve özel rapor ya da görünüm ekranlarında izlenebilir yapıda olmalıdır. Görsel ekranlar grafiksel kalıpların dışında network topoloji ve Geo Location haritalar şeklinde sağlanmalıdır

### Alarm oluşturulurken birden fazla kriter seçilebilmeli ve oluşturulacak alarmlar için ticket oluşturulabilmeli ve ticketin’in atandığı kullanıcılara tarafından aksiyon alınmaması durumuna belirlenen zaman sonrasında farklı bir kişiye risk seviyesi yükseltilerek atanabilmeli.

### Teklif edilecek sistem API ile erişime destek vermelidir.

### Teklif edilecek çözüm toplanan logu başka veri kaynakları ile zenginleştime kabiliyeti sağlamalıdır.

### En az 450 farklı log tipi için hazır log tanıma bileşeni bulunmalıdır. Otomatik ya da manuel güncellemelerle bu veri tabanı gelişen yapıda olmalıdır.

### Loglar en az 1:20 oranında sıkıştırılabilmelidir. Bu sıkıştırma oranları GUI üzerinden ayarlanabilir yapıda olmalıdır.

### Çözüm 1 yılı içerecek şekilde lisanslanmalı lisans suresi boyunca üreticinin destek merkezine sorun bildirilebilmelidir

* 1. **VERİ TABANI GÜVENLİĞİ ÇÖZÜMÜ YENİ ALIMI**

### Önerilecek veritabanı güvenlik çözümü; SQL sunucular için DB aktivite ve takibi, sanal yama güvenliği ve zaafiyet tespitinden oluşacaktır. Çözüm engelleme kabiliyeti sağlayabilmelidir.

### DB aktivite ve takip çözümü ajan temelli olup en az aşağıdaki işletim sistemleri ve veri tabanı çözümlerini desteklemelidir:

### Microsoft Windows 20012 veya üzeri (32bit, 64 bit ve Itanium), Red Hat Linux 7.0 ve sonrası, SUSE Linux 11.4, 12.2 ve sonrası ya da CentOS 7 ve sonrası sürümleri, Oracle Linux 6 ve sonrası

### Oracle 8i ve üzeri - Oracle RAC ve Oracle Exadata dahil (Solaris, IBM AIX, Linux, HP-UX, MS Windows)

### Microsoft SQL Server 2000 ve üzeri

### PostgreSQL 9.3 ve üzeri

### SAP HANA SPS 09, R91 ve sonrası

### Sybase ASE 12.5 ve sonrası

### MariaDB 5.5 (5.5.32 ve sonrası), 10.0 ve 10.1 (Linux)

### MySQL 5.1 ve sonrası (4.6, 4.7, 5.2 ve 5.3)

### Teradata 12, 13, 13.10, 14.15, ve 15.1 (Linux)

### IBM DB2 9.5 ve sonrası (Linux, Unix ve windows)

### Çözüm SQL aktivitelerini takip edebilmek için ağ üzerinden her hangi bir yönlendirmeye (SPAN, Mirror, TAP, Proxy) ihtiyaç duymamalı ve ağ yapısında bir değişikliğe sebep olmamalıdır.

### Çözüm FIPS uyumluluğu sağlayabilmelidir.

### Çözüm PCI-DSS, Sabanes Oxley (SOX), SAS-70, GLBA, HIPAA regülasyonları ve en iyi yapılandırma (Best Practise) için ücretsiz olarak hazır şablonlar sunmalı.

### Zaafiyet tespit ağ temelli olmalı ve herhangi bir ajan gerektirmemelidir. Zaafiyet tespit modulu en az 6000 adet zaafiyete sahip olmalı ve guncelleme mantığıyla genişlemeye imkan sağlamalıdır.

### Sanal yama (Virtual Patch) özelliği ile SQL sunucular üzerinde bulunan yama açıklarına ve ataklara karşı koruma sağlamalıdır. En az 600 adet ön tanımlı kural sunmalıdır.

### Entegre veri tabanı güvenliği çözümünün merkezi yönetim modulu, aynı üreticinin son kullanıcı antivirus, encyption, HostDLP, Host IPS, application control, change control ürünlerinide aynı zamanda yönetebilen ara birim olmalı, bu arabirim Microsoft Windows 2008 R2, 2012, 2012 R2 veya 2016 üzerinde çalışabilmelidir. Backend veritabanı olarak ise Microsoft SQL server 2008, 2008 R2, 2012, 2014 veya 2016 kullanabilmelidir.

### Entegre veri tabanı güvenliği çözümünün merkezi yönetim modülü istenmesi durumunda standalone olarak çalışabilmeli ve aşağıda belirtilen İşletim sistemlerini desteklemelidir:

### Microsoft Windows 2008, 2008 R2, 202, 2012 R2 ve 2016

### Linux RedHat 4.0 ve sonrası, SUSE Linux 10.0 ve sonrası, CentOS 4 ve sonrası

### Entegre veri tabanı güvenliği çözümünün merkezi yönetim modülünün Standalone sürümü backend veri tabanı olarak MS SQL 2008, 2008 R2, 2012, 2014 sürümleri ve Oracle 11g ve sonrasında çalışabilmelidir.

### Entegre veri tabanı güvenliği çözümünün merkezi yönetim modülü istenmesi durumunda ücretsiz olarak Cluster yapısında çalışabilmeli.

### Teklif edilecek yazılımlar, veri tabanı konusundaki genel güvenlik problemlerini çözebilecek ve kurum içinden gelebilecek tehditleri tespit edebilecek özelliklere sahip olmalıdır.

### Çözüm ağ üzerinde çalışan veri tabanlarını tespit edebilmelidir.

### Teklif edilen çözüm, yetkisiz ip lerden gelen kullanıcıların veritabanına erişimini tespit edebilmeli ve engelleme kabiliyeti gösterebilmelidir.

### Teklif edilen çözüm, yönetim yazılımına yetkisiz kullanıcıların login olmasını engellemelidir.

### Teklif edilen çözüm kullanılarak veri tabanında çalıştırılabilecek her türlü komutun kullanımı tespit edilebilmeli veya kurallara bağlanabilmelidir.

### Çözüm üzerinde her hangi bir kural oluşturulmadan yada aktif edilmeden takip edilen veri tabanı sunucularına bağlanan uygulama, ip ve kullanıcı bilgileri için baseline oluşturulmalı ve sunulmalıdır.

### Entegre veri tabanı güvenliği çözümü regülasyonlara uyumluluk açısından kullanıcılar, uygulamalar tarafından çalıştırılan sorguların sonuçlarını (cevaplarını) saklamamalı, sadece sorgunun kendisini tutmalıdır.

### Kullanıcılar tarafından çalıştırılan belirli kritik sorgular için maskeleme yapabilmelidir. Bu şekilde sorgu içerisinde yer alan kritik bir bilgi veri tabanı güvenlik yazılımının yöneticisi tarafından görülemeyecektir.

### Kullanıcılar tarafından çalıştırılan sorguların SQL sunucu üzerinde hata oluşturması durumunda bu olayları tespit edebilecek bir yöntem sunmalıdır

### Kullanıcılar tarafından çalıştırılan uzun sorguların tespit edilebilmesini sağlayacak bir yöntem sunmalıdır.

### SQL sunucular üzerinde standart olmayan portlar üzerinden yapılan aktiviteler trafiğin şifreli olması (IPSec, SSL ve benzeri) fark etmeksizin tespit edilebilmelidir

### Güvenlik ile ilgili olarak yapılmış olan tanımlamaların kullanımı veya bu tanımlamaları aşma girişimleri denetlenebilmeli ve raporlanabilmelidir

### Uç kullanıcılar tarafından gerçekleştirilen işlemler tetikleyici (trigger), saklı prosedür (stored procedure) ve fonksiyonlar (function) içerisinde de yapılsa tespit edilerek engellenebilmelidir.

### Uç kullanıcı ile veri tabanı sunucusu arasındaki trafiğin şifrelenmesi durumunda da tanımlı güvenlik kuralları çalışabilmelidir.

### SQL sorgu seviyesinde audit yapabilecektir. (SELECT SQL statements)

### Önerilen çözümün veritabanı ajanı shared memory de çalışmalı ve tüm query ve DB erişimleri(tablolar dahil) izlenebilmelidir.

### Insert,update,delete gibi komut aktiviteleri izlenebilmelidir.

### Ajan ile yönetim sunucusu arasında ki bağlantının kesilmesi durumunda mevcut politikalar uygulanmaya devam etmeli ve yönetim sunusu ile aradaki bağlantı tekrar sağlandığında olaylar gönderilmelidir.

### Ajan ile yönetim sunucusu arasındaki bağlantı şifreli olarak gerçekleştirilmelidir.

### SQL aktivitelerinin takibi için kullanılan kurallarda yapılan değişiklikleri saklamalı ve kurallar arasında karşılaştırma yapılabilmesine imkan sağlamalıdır.

### Çözüm hazır rapor şablonları ile gelmeli ve raporlar html, ve PDF olarak üretilebilmelidir.Raporlar otomatik olarak e-posta ile ilgilileri ulaştırılabilmelidir.

### Raporlar içerisinde veri tabanı sunucusu, IP adresleri, seviye, OS kullanıcısı, kullanıcı, kural ve ajan parametrelerine göre guruplama imkanı sağlamalı. 2 farklı guruba göre (IP ve Kullanıcı) raporlar süzülebilmelidir.

### Önerilen çözüm hazır audit şablonları ile sunulmalıdır.

### Kural yazma ekranı akıllı sihirbaza sahip olmalı olası syntax sorunları uyarılmalı ve cumle yazımına yardımcı olmalıdır.

### Kural ihlalleri durumunda proaktif uyarı mekanizmaları olmalı, bu uyarılar syslog, email ile gönderilebilmelidir..

### Zaafiyet tespit modulü, veri tabanı sunucularının patch durumunu, zayıf şifrelere sahip olup olmadığını tespit edebilmelidir. Backdoor tespiti yapabilmeli,PL/SQL kodlarında herhangi bir güvenlik sorunu olup olmadığını raporlayabilmelidir. Elile yazılmıs ozel kontrol kurallarına imkan sağlamalıdır(Custom check)

### Veri tabanı güvenlik çözümü session’ın terminate edilmesi dışında kullanıcıyı belli süre ile karantinaya alabilmelidir.

### Veri tabanı platformunun VM olması durumunda sanal sistemleri arasındaki veri iletisiminin denetlenmesi mumkun olmalıdır.

### Hassas verilerin veri tabanı tablolarında olup olmadıgının tespiti mumkun olmalıdır(PII,SSN vb..).Ayrıca ağ üzerinde hazlihazırda çalışan veri tabanlarının keşfi mümkün olmalıdır.

### Rootkit vb. şüpheli davranışların neden olduğu değişiklikler tespit edilebilmelidir.

### Tespit edilen zaafiyet tespitlerine istinaden detaylı duzeltme raporları sunulabilmelidir.

### Merkezi Yönetim arayüzü üzerinden veri tabanı guvenliği çözümü için farklı rollerde adminler atanabilmelidir. Kullanıcı tanımlamalarında LDAP,MS AD yoluyla mevcut kullanıcı veritabanından faydalanılabilmelidir.

### Denial of service,SQL injection,buffer overflow vb saldırı tipleri denetlenip engellenebilmelidir.

### Önerilen çözüme ait ajanın veri tabanı sunucusuna kurulması sonrası, güncellenmesi, upgrade edilmesi, kaldırılması gibi işlemlerde herhangi bir reboot ve servisin yeniden başlatılma gereksinimi olmamalıdır.

### Ajanların bir sebepten dolayı stop edilmesi durumunda yönetim sunucusu üzerinden bu durum görülmeli ve alert edilebilmelidir.

### Ajanların durdurulmaya karşı korunması için aynı üreticiye ait uç nokta güvenlik yazılımı ile entegre olarak koruma sağlayabilmelidir.

### Güncelleme işlemleri isteğe bağlı olarak sadece uyarı, yeni sürüm yayınlandığı anda anlık olarak yüklenme veya belirli günlerde ve saatlerde otomatik olarak yüklenebilmelidir.

### Yönetim yazılımı üzerinde SQL aktivitelerine ait eski olayların arşivlenmesini ve şifreli bir şekilde tutulmasını sağlamalıdır.

### Arşivlenen olaylar çözümün veri tabanına restore edilmeden mount edilme yöntemi ile yüklenebilmeli ve işlemler sonrasında yükleme işlemi iptal edilebilmelidir. Bu şekilde eski arşivlenmiş olaylara hızlı bir şekilde erişim sağlanmalıdır.

### Çözüm tarafından tespit edilen olaylar için terminate session, arşivleme, SNMP Trap, Syslog, Windows Event Log, disk üzerinde belirli bir alana alert yazabilme ve email gönderebilme askiyonları sağlanabilmelidir.

### Çözüm tarafından tespit edilen olaylar SIEM çözümlerine syslog üzerinden CEF formatında gönderilebilmelidir.

### Teklif edilecek çözüm 1 instance sayısına gore 1 yıl olacak şekilde lisanslanacaktır. Lisans süresi boyunca son kullanıcı üreticinin support ekibine 7x24 e-mail veya telefon ile sorun bildirebilecekti

* 1. **CRYPTTECH HOTSPOT YAZILIMI LİSANS YENİLEMELERİ**

### Mevcutta HOTSPOT amaçlı kullanılan 6 farklı lokasyonda yer alan Crypttech yazılım ürünü için 1 yıllık lisans yenileme paketi alımı olacaktır. İhtiyaç listesi aşağıdaki gibidir.

|  |  |
| --- | --- |
| **AÇIKLAMA** | **LOKASYON** |
| CryptoSPOT HotSPOT 250 USER | MERKEZ KAMPÜS |
| CryptoSPOT HotSPOT 250 USER | MERKEZ KAMPÜS DİĞER BLOKLAR |
| CryptoSPOT HotSPOT 250 USER | ÇARŞI POLİKLİNİK |
| CryptoSPOT HotSPOT 50 USER | KALAMIŞ POLİKLİNİK |
| CryptoSPOT HotSPOT 50 USER | ETİLER POLİKLİNİK |
| CryptoSPOT HotSPOT 50 USER | TIP FAKÜLTESİ |
| CryptoSPOT PRO - HotSpot - 100 USER | DİŞ HEKİMLİĞİ |

* 1. **F5 YÜK DENGELEME YAZILIMI LİSANS YENİLEME**

### Mevcutta kullanılan yük dengeleme cihazlarının ve IP Reputation cihazının 1 yıllık lisans yenileme paketi alımı olacaktır. İhtiyac listesi aşağıdaki gibidir.

|  |  |
| --- | --- |
| **AÇIKLAMA** | **ADET** |
| F5-BIG-LTM-I2600 | 1 |
| F5-ADD-BIG-ASM-I2XXX | 1 |
| F5-BIG-LTM-I2600 | 1 |
| F5-ADD-BIG-ASM-I2XXX | 1 |
| F5-SBS-BIG-IPI-3-1YR | 2 |

* 1. **AĞ GÜVENLİK CİHAZLARI YENİLEME**

### Ağ güvenliği tarafında kullanılan fortinet marka fiziksel firewall cihazların, analyzer ve manager yazılımlarının bu sene 1 yıl üretici destek paketleri dahil yenilenecektir. Teklif verecek firmanın teklif edeceği ürün için Expert partnerlık seviyesine sahip olmalıdır.

|  |
| --- |
| FortiGate-100E- FG100ETK18014380 |
| FortiGate-100E - FG100ETK19044047 |
| FortiGate-600E -FG6H0ETB21901409 |
| FortiGate-600E -FG6H0ETB21901474 |
| FortiGate-1000D - Renewal --- Seri No : FGT1KD3914800280 |
| FortiGate-1000D - Renewal --- Seri No : FGT1KD3914800437 |
| ÜNİVERSİTE ANALYZER UPGRADE -- FAZ-VM-GB5- UPGRADE 25GB -FAZ-VMTM22001441 |
| FORTI ANALYZER - FAZ-VM-GB5 - FAZ-VMTM22010620 |
| FORTIMANAGER - FMG-VMTM22010340 |
| FORTI ANALYZER UPGRADE LİSANS -- FAZ-VM-GB5 -- Upgrade license for adding 5 GB/Day of Logs and 3 TB storage capacity. |

* 1. **ALDATMA PLATFORMU ( DECEPTION) YAZILIMI YENİ ALIMI**

### Teklif edilecek çözüm, saldırı tespit amacıyla gerçekçi ve saldırganın sorgularına interaktif olarak cevap verebilen tuzak sistemlerin kurum ağında konumlandırılmasını sağlamalıdır

### Teklif edilecek çözüm üzerinde, hazırda desteklenen Windows7, Windows10, Windows Server 2016/2019, Ubuntu, SCADA, IoT, VPN, ERP, IP Kamera, Printer, Medikal cihazlar, POS gibi tuzak sistemleri bulunmalıdır

### Teklif edilecek çözüm Windows10 ve Windows Server 2016/2019 için kişiselleştirmeyi desteklemelidir ve gerçek işletim sistemleri kullanılmalıdır. Böylelikle belirli yamanın kurulması, kurum alanına (domain) dahil edilmesi gibi tanımlamaları desteklemelidir

### Teklif edilen çözüm EKS sistemleri özelinde tuzak sistemler konumlandırma yeteneğine sahip olmalıdır. Ek bir entegrasyon/emülasyon gerekmeden Siemens, Schneider, Rockwell gibi OT üreticilerine ait sistemler tuzak olarak konumlandırılabilmelidir

### Teklif edilecek çözüm üzerinde SSL VPN, SSH, SAMBA, SMB, RDP, HTTP, HTTPS, FTP, TFTP, SNMP, NBNSSpoofSpotter, Telnet, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, DNP3, KAMSTRUP, GUARDIAN-AST, IEC104, DICOM Server, PACS, GIT, Microsoft SQL servislerine sahip tuzak sistemler oluşturabilmelidir

### Tuzak sistemlerin kurum ihtiyacı doğrultusunda belirli TCP portları için tuzak sistemler üzerinde dinleme yeteneği olmalıdır. Böylelikle yapılandırılan port üzerinden gerçekleştirilmeye çalışılan haberleşme tespit edilebilmelidir

### Çözüm, kurum altyapısında tuzakların kurulacağı VLAN'larda tarama yaparak varlıkları otomatik olarak keşfedecek ve tuzak sistemleri belirleyebilecektir.

### Çözüm üzerinde bilinen güvenli kaynaklardan kaynaklanan uyarılar hariç tutulabilir olacaktır. (Safe list)

### Uç nokta cihazlara, kurulması gereken herhangi bir ajana ihtiyaç duymadan yem-ekmek kırıntısı (token) konumlandırılabilmelidir. Salgırganın bu bilgiler/dosyalar ile etkilişimde bulunması halinde alarm üretilebilmelidir

### Çözüm uç noktalar için aşağıdaki tuzakları (token) desteklemelidir

### Cache Credentials

### Fake Network Connections

### HoneyDocs (office/PDF)

### RDP, SSH links

### Mapped SMB drives

### Uç noktalar üzerine konumlandırılacak tuzaklar için lisans gerekmesi durumunda en yüksek sayıdaki lisanslama ile birlikte teklife eklenmelidir

### Oluşturulan tuzak sistemler tek arayüz üzerinden yönetilebilmelidir

### Teklif edilecek çözüm, tuzak sistemlerin konumlandırabilmesi için otomatik VLAN tespit yeteneğine sahip olmalıdır.

### Teklif edilecek çözüm, izole-kapalı (air-gapped) mimarilerde çalışabilmelidir.

### Konumlandırılan tuzak sistemin belirli bir zaman aralığında sıfırlanması, default durumuna dönmesi, (reset) desteklenmelidir

### Teklif edilecek çözüm saldırgana ait teknik, taktik ve prosedürleri ilişkilendirerek, alarmları gruplayabilmeli ve yönetim arayüzünde sunabilmelidir

### Teklif edilen çözümün üreticisi gelişmiş bir tehdit istihbarat servisine sahip olmalıdır. Çözüm bu tehdit istihbarat veritabanına sorgu yapılarak saldırgan aksiyonlarını otomatik olarak risk seviyesi belirleyebilmeli ve sınıflandırabilmelidir. Bu istihbarat veritabanında IPS (Intrusion Prevention System) imzaları, AV(Antivirüs) imzaları, URL güvenilirlik ve kategori bilgileri yer almalıdır

### Tuzak sisteme bir zararlı indirilmesi durumunda tespit edebilmelidir. Virustotal ve sandbox entegrasyonlarına sahip olmalıdır

### Teklif edilecek sistem, ransomware saldırılarını tuzak sistemler ve token konumlandırılan uç noktalar üzerinde tespit edebilmelidir

### Saldırganın tuzak sistem üzerinden eriştiği URL ler kategorize edilebilmeli ve raporlanabilmelidir

### Tespit edilen IOC (indicator of compromise) verileri GUI üzerinden indirilebilmeli ve dışarı çıkartılabilmelidir

### Teklif edilecek çözüm, tespit ettiği bulgular için paket kaydı (pcap) yapabilmeli ve sistem yöneticisi, çözümün web yönetim arayüzü üzerinden bu dosyayı indirebilmelidir

### Teklif edilecek çözüm, tek bir sistemden oluşmalı ve web servisi üzerinden yönetilebilmelidir. Yönetim için ayrı bir kuruluma ihtiyaç olmamalıdır

### Teklif edilecek çözüm, tespit edilen geçmiş atakları zaman çizelgesi üzerinde filtreleyerek grafik arayüzünde gösterebilmelidir

### Çözüm, tuzak olarak konumlandırılan sistemleri ve tuzaklar üzerindeki servisleri konumlandırıldığı ağ ile ilişkilendirilerek görsel olarak sunabilmelidir

### Tespit edilen bulgular, IOC olarak dışarı çıkartılarak üçüncü parti tehdit istibarat servisleri ile paylaşılabilmelidir

### Teklif edilecek çözüm yönetim arayüzüne erişim için LDAP ve RADIUS desteklenmelidir. Rol bazında kullanıcı yetkilendirme tanımlamaları yapılandırılabilmelidir

### Teklif edilecek çözüm, syslog ve cerf formatında kayıtların dışarı aktarılmasını desteklemelidir

### Aldatma platformu FortiGate, FortiNAC, FortiSIEM, FortiSOAR, FortiAnalyzer çözümlerine entegre olmalıdır. Fortigate web arayüzünde aldatma platformuna ait tuzak sistemler listelenebilmeli, sağlık durumları, ip erişim bilgilerine erişilebilmelidir

### Teklif edilecek çözüm, REST API desteklemelidir. Böylelikle Güvenlik Duvarı, NAC, SIEM gibi çözümlerle entegre çalışabilmelidir

### Teklif edilecek çözüm VMWare vSphere ESXi 5.1, 5.5,6.0,6.5 ve güncel versiyonları, KVM sanallaştırma platformları üzerinde çalışabilmelidir

### Aldatma platformu sahip olduğu CPU, Memory kaynakları doğrultusunda maksimum kaç adet tuzak VM konumlandırılabileceğini arayüzünde gösterebilmelidir

### Teklif edilen çözüm, sağlıklı çalışabilmesi için ihtiyaç duyduğu erişimlerin kontrolünü (internet bağlantısı, dns, ping speed, wget speed gibi) tek bir komut ile gerçekleştirebilmelidir

### Çözüm kurumun yapısına uygun olarak altyapı 1 için 3 adet, altyapı 2 için 2 adet VLAN da tuzak sistem konumlandırılacak şekilde 1 yıllık olarak teklif edilmelidir

* 1. **ÇOK FAKTÖRLÜ KİMLİK DOĞRULAMA YAZILIMI**

### Teklif edilen ürün 100 adet anlık local veya uzak kullanıcı desteğine sahip olmalıdır

### Teklif edilen ürün 50 adet CA (Certificate autority) desteğine sahip olmalıdır

### Teklif edilen ürün 100 adet kullanıcı sertifika desteğine sahip olmalıdır

### Teklif edilen ürün 100 adet kullanıcı grubu oluşturma desteğine sahip olmalıdır

### Teklif edilecek ürün donanım olarak veya sanal olarak VMware ESXi / ESX 3.5 / 4.0 / 4.1 / 5.0 / 5.5 / 6.0, Microsoft Hyper-V Server 2008 R2, 2012, and 2012 R2 ortamlarında çalışabilmelidir

### Teklif edilen üründe 4 adet interface desteği olmalıdır

### Teklif edilen ürün tek olarak lisanslanmalı ve gerektiğinde yedekli Active-Passive HA ve Config Sync HA desteğine sahip olmalıdır.

### Kimlik dogrulama özellikleri

### Teklif edilecek ürün SSO (single sign on) desteği olmalıdır ve aşagıdaki kaynaklardan beslenebilmelidir.

### AD (Active directory) sorgulama (AD polling) veya AD agent iletişimi

### TS (Terminal server) agent

### Kerberos

### REST API

### Radius Accounting

### FortiClient SSO client

### SSO Login Portal

### Syslog

### Teklif edilecek ürün Windows altyapılar için WMI sorgulama yöntemi ile aktif olmayan kullanıcıları SSO listesinden çıkartabilmelidir veya belli bir süre limiti ile SSO listesinden çıkartabilmelidir

### Teklif edilecek ürün kablosuz altyapılar için merkezi kimlik doğrulama sistemine sahip olmalıdır

### Teklif edilecek ürün kablosuz altyapılar için kullanıcılar için PEAP, EAP-TTLS desteği olmalıdır aynı zamanda sertifika tabanlı EAP-TLS BYOD (bring your own device) desteğine sahip olmalıdır

### Teklif edilecek ürün kablosuz altyapılar için mobil telefon doğrulamalı konuk yönetimi captive portal çözümüne sahip olmalıdır

### Teklif edilecek ürün kablosuz altyapılar için konuk captive portal çözümü admin onayı ile kullanıcı şifrelerini HTTP/HTTPS/mail-to-sms servislerine entegrasyonuna sahip olmalıdır

### Teklif edilecek ürün kablosuz altyapılar için konuk captive portal çözümü değiştirilebilir önyüz desteğine sahip olmalıdır

### Teklif edilecek ürün kablosuz altyapılar için SSO desteği ile Fortinet firewall’lara direk entegre olabilmelidir

### Teklif edilecek ürün kablosuz altyapılar için konuk yönetimi captive portal çözümü facebook, twitter, Google vb. Kimlik bilgileri ile giriş desteğine sahip olmalıdır

### Teklif edilecek ürün kablosuz altyapılar için konuk yönetimi belli bir sürede ilgili kullanıcıların resetlenmesini ve sistemden silinmesini desteklemelidir

### Teklif edilen ürün sertifika yönetimi yapabilmelidir

### Teklif edilecek ürün kullanıcı sertifika yönetimi aşagıdaki bağlantılar için oluşturup doğrulayabilmelidir

### VPN

### Kablosuz 802.1X(PEAP,EAP)

### Windows desktop authentication

### FTK300 USB PKI Certificate Store uyumluluğu

### KAblo NAC destegi 802.1X (PEAP, EAP-TTLS, EAP-TLS, EAP-GTC)

### Teklif edilen ürün Radius Accounting Proxy desteği olmalıdır

### Teklif edilen üründe MAC cihaz kimlik doğrulama desteği olmalıdır

### Teklif edilen ürün harici AD, LDAP, Radius desteği olmalıdır

### Teklif edilen ürün LDAP server olarak kullanılabilmelidir

### Teklif edilen ürün Radius ürün olarak kullanılabilmelidir

### Teklif edilen ürün Token yönetimi yapabilmelidir. Lisans kadar soft veya hardware token register edilebilmelidir

### Teklif edilen ürün üzerinden adil kullanım kotası amaçlı kota temelli bant genişliği yönetimi yapılabilmelidir

### Teklif edilen ürün HTTPS üzerinden yönetilebilmelidir.

### Teklif edilen ürün kullanıcı girişlerini kayıt altına alabilmeli ve harici loglama sistemlerine aktarabilmelidir.

### Teklif edilen ürün CPU ve memory kullanımlarını, kullanıcı adet istatistiklerini önyüz üzerinden gösterebilmelidir.

### Teklif edilen ürün otomatik backup alarak belirlenen zamanda harici ftp sitesine gönderebilmelidir.

### Teklif edilen ürün SNMP v1/v2c ve v3 destegi olmalıdır. MIB bilgileri üzerinden soğulama yapılabilmelidir.

### Teklif edilen ürün admin kullanıcılarına yetkilendirme yapılabilmelidir.

### Teklif edilen ürün log kayıtları HTTPS arayüz üzerinden filitrelenebilir şekilde sorgulanabilmelidir.

### Teklif edilen ürün log kayıtlarını harici syslog server’lara gönderebilmelidir.

### Teklif edilen ürün bir yıllık yazılım destek paketi ile verilmelidir.

* 1. **UÇ NOKTA TEHDİT ALGILAMA VE YANIT YAZILIMI**

### Önerilecek sistem merkezi olarak istemciler üzerinde sorguların çalıştırılmasına izin vermeli, sorgu ve cevaplar en kısa sürelerde gerçekleşmelidir.

### Çözüm sahip olduğu bütün fonksiyonları aynı yönetim konsolu üzerinde gerçekleştirebilmelidir. Farklı araç ya da konsollara ihtiyaç duymamalıdır.

### Teklif verecek firmanın teklif edeceği ürün için Platinium partnerlık seviyesine sahip olmalıdır.

### Bunun icin kullanılacak ajanlar en az Windows, MacOS ve Linux işletim sistemlerini desteklemelidir. Desteklenecek işletim sistemleri aşağıdaki gibi olmalıdır;

### Windows 7 32 ve 64 bit

### Windows 8 ve 8.1 32 ve 64 bit

### Windows 10 32 ve 64 bit

### Windows Server 2008 R2 Standart, Enterprise

### Windows Server 2012

### Windows Server 2016

### CentOS/ RedHat 64 Bit ver 6.6’dan 7.5’e kadar

### Suse 11-12

### MacOS Mojave 10.14

### MacOS High Sierra 10.13

### MacOS Sierra 10.12

### MacOS El Capitan 10.11

### Ajanların dağıtımı ve yönetimi için son kullanıcı güvenlik sisteminin merkezi yönetim yazılımı kullanılmalıdır

### Merkezi yönetim yazılımı web tabanlı olmalıdır.

### Sistem zengin (en az 25 adet) ön tanımlı sorgu imkanları sunmanın dışında el ile bu sorguları yapılmasını sağlayacak fonksiyonların (collector) yenilerinin tanımlanmasına imkân sağlamalıdır. Böylelikle kurum ihtiyaçlarına uygun olarak geliştirmeler yapabilmelidir. Bu fonksyionlar yazılırken OS komutları dısında, vmi, bash script, VB script ve Phython kullanılabilmelidir.

### Ön tanımlı collector lerin internet uzerinden ureticinin sagladıgı alt yapıyla otomatik olarak güncellenmesi mümkün olmalıdır.

### İlgili ajanlar son kullanıcı sistemlerindeki network flowlarını ve file sistem ve kayıt günlüğü üzerindeki değişiklikleri anlık takip edebilmelidir

### Sorgular belli tarih aralıkları için gerçekleştirilebilmelidir. Örneğin belli bir tarih sonrası belli bir kullanıcıda oluşan network bağlantılarının tespiti ve bu tarih sonrasında o istemcide oluşan belli bir dosya tipinin sorgulanması gibi

### Hash temelinde tüm ağ üzerinde veya belli istemciler üzerinde taramalar yapılabilmelidir

### Flow verileri içinde en az aşağıdaki parametlere tarama yapmaya imkan sağlamalıdır.

### Lokal IP

### Source IP ve Port

### Destination IP ve Port

### Remote Port

### ProcessID

### User

### Protocol

### Hash (md5, sha-1)

### Dosyalar için ön tanımlı collectorler en az aşağıdaki parametrelere sahip olmalıdır

### File Name

### Directory

### Full Name

### Size

### Last Write

### Hash (md5, Sha-1)

### Created at

### Deleted at

### Status

### Host collector en az aşağıdaki parametrelere sahip olmalıdır.

### Hostname

### IP Address

### Operating System

### Update edilen hotfixler için en az aşağıdaki parametlere sahip olmalıdır.

### Description

### Hotfix ID

### Installed Date

### Installed by

### Processler için kullanılacak collector en az aşağıdaki parametrelere sahip olmalıdır.

### Name

### ID

### ThreatCount

### Parent ID

### Size

### Hash

### Cmdline

### Image Path

### Kernel Time

### Uptime

### User

### Kullanıcı Profil collector’u en az aşağıdaki parametrelere sahip olmalıdır.

### Account Disabled

### Domain

### Fullname

### Install Date

### Local Account

### Locked Account

### SID

### Password Expires

### Group

### Windows Registry collectoru en az asagıdaki parametrelere sahip olmalıdır.

### Key Path

### Key Value

### Value Data

### Value Type

### Olayları yakalamak ve otomatik reaksiyon uretmek icin en az asagıdaki olay tipleri desteklemelidir

### File Created

### File Modified

### File Deleted

### Network Connection Open

### Network Connection Close

### Port Opened

### Port Closed

### Process Created

### Process Terminated

### Sorgular oluşturulurken sistem ara yüzü sorgunun doğru ya da yanlış olduğunu işaret eden uyarı alt yapısına sahip olmalıdır.

### Konsol sorgularını kaydedilmesini sağlayabilmelidir. Böylelikle kullanıcı en çok ihtiyaç duyduğu sorguları tekrar tekrar yazmak durumda kalmamalıdır.

### Çözüm, yönetilen sistemler üzerinde canlı arama yapabilmelidir, arama yönetim konsolu üzerine gelen tarihsel veri üzerinde olmamalıdır.

### Ürün tespit edilen tehditleri bir arayüz üzerinde riskine göre görüntüleyebilmelidir. Bu ekran zararlı ismi, zararlının hash değeri, hangi bilgisayarda rastlanıldığı gibi bilgileri verebilmelidir.

### Aynı arayüz üzerinde zararlının sistem üzerinde yaptığı değişiklikler (yaratılan processler, ağ bağlantıları, registry kayıtları, yaratılan dosyalar gibi) birbirleriyle ilişkilendirilerek görüntüleyebilmelidir.

### Bu arayüz üzerinden yapılan incelemerde istenildiği takdirde olayla ilgili bilgisayarlar üzerinde araştırmanın yapılması sağlanabilmelidir. Örneğin zararlının yarattığı bir dosyanın ağ üzerindeki varlığının sorgulanmasını sağlayacak dizi otomatik oluşturulup aramanın yapılması sağlanabilmelidir.

### Aynı arayüz üzerinden merkezi olarak ilgili zararlı için sadece zararlının çalıştığı bilgisayar ya da tüm bilgisayarlar için silme, durdurma, karantina gibi aksiyonlar alınabilmelidir. Tek tek zararlının olduğu her bir sistem üzerinde ayrı ayrı aksiyon almak gerekmemelidir.

### Çözüm memorydump almaya olanak sağlamalıdır.

### Çözüm 1400 kullanıcıyı içerecek şekilde 1 yıllık olarak lisanslanmalıdır.

* 1. **BİLGİ GÜVENLİĞİ ÜRÜNLERİ TEKNİK OPERASYON SÜREÇ KAPSAMI**

### Yenileme projesi kapsamında yer alan tüm güvenlik çözümlerinin teknik anlamda operasyonel süreçlerini tek bir yüklenici üstlenecektir.

### Yenileme projesi kapsamında yer alan tüm güvenlik çözümlerinin kurulum öncesi, kurulum süreci ve kurulum sonrası test aşamalarında yüklenici firma ile birlikte başka bir ikincil (taşeron) firma kesinlikle bu süreçte bulunmamalıdır.

### Yenileme projesi kapsamında hali hazırda yapıda çalışan tüm güvenlik cihazlarının lisans bitim tarihinden öncesinde süreç planlanmalıdır.

### Yenileme projesi kapsamında yer alan tüm güvenlik çözümlerinin lisans geçişleri noktasında yeni lisansları sisteme tanımlanırken mutlaka sistemler üzerinden yer alan konfigürasyon ve politika yedeklerinin alınması zorunlu bir durumdur.

### Yenileme projesi kapsamında lisans geçişleri sağlanırken olası bir kesintiye karşı yedek bir yapı oluşturulmalı veya sistemin sürekliliğini riske atmayacak bir kurguda süreç yönetilmelidir.

### Yenileme projesi kapsamında sistemlere tanımlanacak yeni lisanslar ile birlikte sistemlerin o anki güncel sürümlerinden daha üstte bir sürüm üreticilerin sitesinde duyuruldu ise en üst sürümlere geçiş sağlanmalıdır. Bazı durumlarda en üst sürümlere geçmek ürünlerin kararlı çalışması noktasında sıkıntılara yol açıyorsa bu geçiş yapılmadan önce kurum yetkin mühendisler tarafından öncesinde bilgilendirilmelidir.

### Yenileme projesi kapsamında sistemlere tanımlanacak yeni lisanslar, sorunsuz bir şekilde geçişi yapıldıktan sonra sistemlerin kesintisiz çalıştığının taahhütü verilmelidir.

* 1. **BİLGİ GÜVENİĞİ, YÜKLENİCİNİN PERSONEL YETKİNLİKLERİ KAPSAMI**

### Bilgi güvenliği ürünleri lisans yenilenmesi kapsamında yer alan, tüm güvenlik çözümlerinin kurulum sürecini yüklenici firma bünyesinde yer alan teknik uzmanlar tarafından yapılması zorunludur.

### Bilgi güvenliği ürünleri lisans yenilenmesi kapsamında yer alacak olan teknik uzmanlar minimum kendi alanlarında 4 yıl tecrübe ve ilgili çözümler noktasında üreticinin teknik sertifikasyonlarına sahip olmalıdır. Üreticinin teknik sertifikası olmayan teknik uzmanlar kesinlikle kurulum ve geçiş operasyonunda yer almamalıdır.

### Bilgi güvenliği ürünleri lisans yenilenmesi kapsamında yüklenici firma bünyesinde çalışan teknik uzmanlardan en az 4 farklı kişide Fortinet NSE5, en az 1 kişide Fortinet NSE 7, en az 3 farklı kişide Trellix Network Security Technical Specialist ve son olarak en az 2 kişi Trellix teknik sertifikaları bulunması zorunludur.

# **MICROSOFT VE ADOBE LİSANSLARI TEKNİK ŞARTNAMESİ**

* 1. **MICROSOFT LİSANS YENİLEMELERİ VE YENİ LİSANS ALIMLARI**

### Teklif edilecek olan Windows sunucu lisansı host bazında sınırsız sanal sunucu kurma hakkını barındırmalıdır.

### Temin edilecek Windows Sunucu lisansı Hibrit entegrasyon, korumalı sanal makineler, yazılımla tanımlanmış ağ ve yazılımla tanımlanmış depolama özelliğini içermelidir.

### Teklif edilecek lisansların Yazılım Güvencesi (Software Assurance) içermesi gerekmektedir.

### Anlaşma kurum adına 3 yıllık açılacak olup her yıl yenilenecektir.3 yılın sonunda tekrardan anlaşma yapılacaktır.

### Yeni alım ve yenileme kapsamında temin edilecek tüm lisanslar belirtilen e-mail adresine tanımlanacaktır ve Volume Licensing Service Center üzerinden ürün anahtarları görüntülenebilir ve kurulum ISO’ları indirilebilir olmalıdır.

### Microsoft lisanslarını temin edecek firmanın MPN (Microsoft Partner Network) sistemine kayıtlı olmalı ve en az aşağıda belirtilen sertifikalara sahip olmalıdır. Teklif verilebilmesi için Microsoft Licensing Solution Providers (LSP) yetki belgesi alınmalıdır.

### Gold Cloud Productivity

### Gold Application Development

### Gold Datacenter

### Gold Small and Midmarket Cloud Solutions

### Gold Collaboration and Content

### Lisansları temin edecek kuruluşun yukarıda belirtilen yetkinlikleri yanı sıra kurumsal segmentte SAM (Software Asset Management) çalışması yapma yetkisinin olması tercih sebebidir.

|  |  |  |
| --- | --- | --- |
| **Ürün Kodu** | **Ürün Adı** | **Adet** |
| AAA-73004 | M365 A3 Original Edu Sub Per User | 1400 |
| PYQ-00001 | M365 A5 Security Edu Sub Per User | 1400 |
| LK7-00001 | Teams Phone Standard Edu Sub Per User | 25 |
| 9EA-00039 | Win Server DC Core ALng LSA 2L | 232 |
| 395-02412 | Exchange Server Ent ALng LSA | 2 |
| 7JQ-00341 | SQL Server Enterprise Core ALng LSA 2L | 22 |
| 7NQ-00302 | SQL Server Standard Core ALng LSA 2L | 4 |
| R39-00374 | Win Server External Connector ALng LSA | 2 |
| 4ZF-00019 | Win VDA Device ALng Sub Per Device | 60 |
| 6VC-01251 | Win Remote Desktop Services CAL ALng LSA DCAL | 50 |
| 9EM-00562 | Win Server Standard Core ALng LSA 2L | 10 |

* 1. **ADOBE LİSANS YENİLEMELERİ**

### Mevcutta kullanılan Adobe Creative Cloud, Photoshop, InDesign, Acrobat Pro, ve InCopy lisanslarının 1 yıllık lisans yenilemesi alımı yapılacaktır. Yazılımların en son versiyonları sağlanmalıdır.

### Lisanslar 135B298766E49B509CBA VIP numarasına tanımlanacaktır.

### Adobe Creative Cloud; video, tasarım, fotoğraf ve web için dünyanın en iyi uygulamalarını ve hizmetlerini sunar. Lisans adet listesi aşağıdaki gibidir.

|  |  |
| --- | --- |
| **AÇIKLAMA** | **ADET** |
| Creative Cloud for enterprise All Apps/HED Shared Lab & Classroom | 151 |
| Creative Cloud for teams All Apps | 11 |
| Acrobat Pro DC | 1 |
| InDesign for teams | 2 |
| Photoshop for teams | 3 |
| InCopy for teams | 12 |

# **SOLIDWORKS LİSANS YENİLEMELERİ**

### Kurum bünyesinde mevcutta kullanılan 60 kullanıcılı Solidworks lisansının yenileme alımı yapılacaktır.

# **DEEPFREEZE LİSANS YENİLEMELERİ**

### Kurum bünyesinde mevcutta kullanılan 577 kullanıcılı Deep Freeze Enterprise Maintenance lisansının ve 85 kullanıcılı Deep Freeze Mac Maintenance lisansının yenileme alımı yapılacaktır.

### Mevcut lisanslara ek olarak 100 kullanıcılı Deep Freeze Enterprise Maintenance lisans alımı yapılacaktır.

# **EXCLAIMER LİSANS YENİLEMELERİ**

### Mevcutta bulunan 1400 kullanıcılı Exclaimer Mail İmzaları Yönetimi lisansının yenileme alımı yapılacaktır.

# **XMEDIUS FAX SERVER BAKIM YENİLEMELERİ**

### Kurum bünyesinde bulunan Xmedius Fax Serverın 1 yıl boyunca 5x8 bakım desteğini kapsamaktadır.

### Bakım 1 yıl boyunca sınırsız telefon ve email desteği ve 1 yıl içerisinde çıkacak olan yeni versiyonları ücretsiz yükleme hakkı sağlar.

# **TEKNİK VE YÖNETİLEN HİZMETLER TEKNİK ŞARTNAMESİ**

* 1. **YÖNETİLEN HİZMETLER**

### Yönetilen Hizmetler Proje Yöneticisi ile Proje yönetimi

### Proje planının hazırlanması, haftalık proje takibi ve bilgilendirmesi, projenin genel koordinasyonu ve takibi

### Yılda 1 kere Healthcheck

### Yönetilen Güvenlik Uzmanı (Paylaşımlı Uzaktan)

### Müşterinin kullanacağı McAfee ürünlerine konfigürasyon, bakım destek ve yönetimini gerçekleştiren birinci kontaktır. BBS L2 güvenlik ekibi birlikte koordineli olarak çalışır.

### McAfee Endpoint, DLP ve EDR konfigürasyon ve yönetimi.

### McAfee EndPoint, McAfee DLP ve EDR, SIEM DAM ürünlerine yönelik verilecek olan bakım & destek ve yönetim hizmeti.

### Üsküdar Üniversitesi envanterinde bulunan McAfee SIEM 5000 EPS ürününün;

### LOG kaynaklarının belirlenmesi

### SIEM ürününün bakım & destek ve Yönetim Hizmeti

### Korelasyonların yazılması

### False positive’lerin ayıklanması

### 7x24 SIEM izleme

### Proje boyunca Korelasyonların güncellenmesi ve yeni korelasyonların eklenmesi

### Korelasyonlar yardımıyla atakların fark edilmesi durumunda Paloalto Firewall ve McAfee IPS aracılığı ile müdahale

### 7x24 EDR izleme.

### Atakların farkedilmesi durumunda müdahale.

### Güvenlik Danışmanlığı

### Aylık raporlama

### 3 ayda bir değerlendirme ve iyileştirme toplantısı

* 1. **SİSTEM BAKIM DESTEK ANLAŞMASI**

### Mutabık olunan envanter dokümanında yer alan ürünlere, müşteri tarafından açılacak çağrı ile başlayan bakım destek hizmeti. Maksimum 2 saat içerisinde uzaktan, gerekli durumlarda İstanbul Lokasyonunda maksimum 4 saat içerisinde yerinde müdahale hizmetini kapsamaktadır.

### •Belirlenen Hizmet süresi 1 yıl için geçerlidir.

### •Hizmet 7x24 esasına göre verilecektir.