TRtest
Test ve Değerlendirme A.Ş.

DLP ÜRÜN GRUBU KRİTERLERİ

No	Başlık/Soru	C (Giriş Seviye)	B (Orta Seviye)	A (Üst Seviye)
UG	**1- Ürün Güvenliği**			
UG_YA	**Yönetim Arayüzleri**			
UG_YA_WA	**1.1 Web Arayüzleri Zayıflık taraması**			
UG_YA_WA_1	Zararlı girdi kontrolü yapılıyor mu?	C		
UG_YA_WA_2	Çıktı Kodlama yapılıyor mu?	C		
UG_YA_WA_3	Kimlik Doğrulama kontrolü yapılıyor mu?	C		
UG_YA_WA_4	Parola yönetimi güvenliği sağlanıyor mu?	C		
UG_YA_WA_5	Erişim yönetimi ve yetkilendirme yapılıyor mu?	C		
UG_YA_WA_6	Hata yönetimi ve loglama doğru bir şekilde yapılıyor mu?	C		
UG_YA_WA_7	Güvenli iletişim kanalları destekleniyor mu?	C		
UG_YA_WA_8	Sistem yapılandırması doğru, güncel ve güvenli mi?	C		
UG_YA_WA_9	Veri tabanı güvenliği sağlanıyor mu? (Erişim ve İçerik Güvenliği)		B	
UG_YA_WA_10	Dosya yönetiminde yetkilendirme ve güvenlik sağlanıyor mu?	C		
UG_YA_WA_11	Bellek yönetimi güvenliği var mı?	C		
UG_YA_WA_12	Oturum yönetiminde yetki kontrolü yapılıyor mu?	C		
UG_YA_WA_13	Genel kod (API) uygulamalarında kod güvenliği test ediliyor mu?	C		
UG_YA_WA_14	Kriptografi uygulamalarında zayıflığı bilinen protokol kullanılmadığı teyit edildi mi?	C		
UG_YA_D	**1.2. Diğer (Uygulama/Web API vb. Kullanarak Yönetim)**			
UG_YA_D_1	Zararlı girdi kontrolü yapılıyor mu?	C		
UG_YA_D_2	Kimlik Doğrulama, parola kaba kuvvet kontrolü yapılıyor mu?	C		
UG_YA_D_3	Parola yönetimi güvenliği sağlanıyor mu?	C		
UG_YA_D_4	Erişim yönetimi ve yetkilendirme yapılıyor mu?	C		
UG_YA_D_5	Hata yönetimi ve loglama doğru bir şekilde yapılıyor mu?	C		
UG_YA_D_6	Güvenli iletişim kanalları destekleniyor mu?	C		
UG_YA_D_7	Güvenli iletişim kanallarında zaafiyet var mı?	C		
UG_YA_D_8	Sistem yapılandırması doğru, güncel ve güvenli mi?	C		
UG_YA_D_9	Oturum yönetiminde yetki kontrolü yapılıyor mu?	C		

UG_YA_D_10	Genel kod uygulamalarında kod güvenliği test ediliyor mu?	C		
UG_ISS	**İşletim Sistemi ve Servisler**			
UG_ISS.1	Ajanın dosyalarının bulunduğu (kurulum dosyaları, yapılandırma, log, script vb.) dizinlerinin kullanıcının erişimine kapatılıyor / kısıtlanıyor mu?	C		
UG_MT	**Masumiyet Testi**			
UG_MT_1	Herhangi bir dış noktaya şüpheli veri göndermiyor, içeride görevi dışında bir sisteme erişiyor mu?	C		
UG_MT_2	Windows/Linux kernel seviyesinde entegre edilen sürücülerin (driver) sistemi bozabilecek herhangi başka manipülasyona sebep oluyor mu?	C		
GFT	**2- Güvenlik Fonksiyon Testi**			
GFT_YT	**Yetkilendirme Testleri**			
GFT_YT_1	LDAP protokolünü kullanan dizin uygulamaları yetkilendirme/entegrasyon yöntemlerini destekliyor mu?	C		
GFT_WF	**Web Filtreleme (Http, Https) ve Mail Kotrolü (Network DLP)**			
GFT_WF_1	Kullanıcı/Grup/Zaman bazlı kural yazımını destekliyor mu?	C		
GFT_WF_2	URL, Alan adı, içerik, içerik tipi, eklenti, kelime, düzenli ifade(regex) engellemeyi destekliyor mu?	C		
GFT_WF_3	Kategori bazlı filtrelemeyi destekliyor mu?	C		
GFT_WF_4	Hassas verilerin e-posta yoluyla gönderilmesi engellenebiliyor mu?	C		
TO	**3- Temel Özellikler**			
TO_1	Ürün web uygulaması ile yönetilebiliyor mu?	C		
TO_2	Yönetim arabiriminin Türkçe ve İngilizce olmak üzere en az iki dil desteği var mıdır?		B	
TO_3	Modüler yapıda ve ürün bileşenleri ayrı ayrı güncellenebiliyor mu?			A
TO_4	Tüm web ekranlarında form alanlarının doğrulanması (Geçerli veri, Zorunluluk) sağlanabiliyor mu?	C		
TO_5	İstemci uygulamasında çoklu platform desteği sağlanıyor mu?	C		
TO_SY	**Sistem Yönetimi**			
TO_SY_1	Kullanıcı ve rol temelli yetkilendirme modelini destekliyor mu?	C		
TO_SY_2	Farklı kimlik doğrulama yöntemlerini destekliyor mu?		B	
TO_SY_3	Şifre güvenlik seviyesi kontrolleri yapılabiliyor mu?	C		
TO_SY_4	Sistem modüllerinin konfigürasyonu yapılabiliyor mu?	C		
TO_SY_5	Ajanın yapacağı işlemler, politika ile belirlenebiliyor mu?	C		
TO_SY_6	Tanımlanan bir varlık güncellendiğinde, aynı varlık ile ilgili daha önceden tanımlanan politikaların yeniden uygulanması (sürekliliği) sağlanıyor mu?	C		
TO_SY_7	Herhangi bir politika tarafından kullanılmakta olan varlıkların silinmesi engelleniyor mu?	C		
TO_SY_8	Bir politika farklı varlıkların kombinasyonuna yönelik tanımlanabiliyor mu?	C		
TO_SY_9	Bir politikaya uygun engelleme oluştuğunda, bu olaya ilişkin uyarıların belirlenen bir adrese otomatik olarak bilgilendirme mesajları e-posta/sms vb. ile gönderilmesi sağlanabiliyor mu?	C		

TO_SY_10	Bileşen bazında, detaylı log yönetimi (Akış bilgisi, Exception) yapılıyor mu?	C		
TO_SY_11	Önemli veritabanı kayıtlarının aktiflik durumları (DLP logları vb.) veya silinmiş kullanıcıların geçmişe yönelik loglarının yönetimi yapılabiliyor mu?	C		
TO_AJ	**Ajan İşlemleri**			
TO_AJ_1	Son kullanıcı bilgisayarına yüklenmiş olan ajan, administrator' un kontrolünde ve bilgisinde kolay bir şekilde uzaktan bypass edilebiliyor mu?		B	
TO_AJ_2	Ajanlar merkezi olarak yönetilebiliyor mu ? (kurulum, güncelleme)		B	
TO_AJ_3	Son kullanıcı bilgisayarına yüklenmiş olan ajanın, Güvenli Mod veya üçüncü parti bir tool yardımıyla veya registry ayarları oynanarak uninstall edilmesi engellenebiliyor mu?		B	
TO_AJ_4	Son kullanıcı bilgisayarına yüklenmiş olan ajanın dosya ve klasörlerinin gizlenmesi & Task Manager'daki process' inin gizlenmesi sağlanabiliyor mu?			A
TO_AJ_5	Son kullanıcı bilgisayarına yüklenmiş olan ajan, "Storage Media" olarak algılanan cihazlara ek olarak, fotoğraf makinesi / mp3 çalar / telefon gibi cihazlara yapılan dosya transferini de monitor edebiliyor mu?		B	
TO_AJ_6	Son kullanıcının kendisi, Endpoint' in log' larından, hangi politikadan veya hangi filtreden veya hangi kuraldan dolayı engellendiğine ait bir bilgilendirme görebiliyor mu?	C		
TO_AJ_7	**Ajan tarafından aşağıdaki olaylar izleniyor mu? Olay bilgileri sunucuya gönderiliyor mu?**	C		
TO_AJ_7_1	**Sistem konfigürasyon**			
TO_AJ_7_1_1	Bilgisayar isim değişikliği	C		
TO_AJ_7_1_2	Registry (Windows) anahtar bilgisi değişikliği			A
TO_AJ_7_1_3	İzlenecek anahtar bilgisi (Windows registry key) belirleme			A
TO_AJ_7_2	**Kullanıcı ile ilgili olaylar**			
TO_AJ_7_2_1	Kullanıcı ile ilgili olaylar			A
TO_AJ_7_2_2	Sisteme giriş (Login)			A
TO_AJ_7_2_3	Sisteme başarısız giriş (Login failure)			A
TO_AJ_7_2_4	Ekran görüntüsü alma	C		
TO_AJ_7_2_5	Pano (Clipboard) kopyalama	C		
TO_AJ_7_3	**Kullanıcı yönetimi ile ilgili olaylar**			
TO_AJ_7_3_1	Yeni Admin kullanıcısı eklenmesi	C		
TO_AJ_7_3_2	Admin kullanıcısının silinmesi	C		
TO_AJ_7_3_3	Admin kullanıcısının şifre değişikliği	C		
TO_AJ_7_3_4	Domain kullanıcısı eklenmesi	C		
TO_AJ_7_3_5	Erişilebilir makinelerin MAC adresleri Yönetim Arayüzü üzerinden görülebiliyor mu?	C		
TO_AJ_7_3_6	Erişilebilir makinelerin IP adresleri Yönetim Arayüzü üzerinden görülebiliyor mu?	C		
TO_AJ_7_3_7	Erişilebilir istemcilerin yüklü olduğu makinelerin zaman bilgileri otomatik kontrol ediliyor mu?	C		
TO_AJ_7_3_8	Domain kullanıcısı silinmesi	C		

TO_AJ_7_4	**Donanım değişiklikleri ile ilgili olaylar**			
TO_AJ_7_4_1	Yeni donanım eklenmesinin engellenmesi ve çıkarılmasının bilgilendirilmesi (SoundDevice, PhysicalMemory, NetworkAdapter, DiskDrive, CDROMDrive, VideoController)	C		
TO_AJ_7_5	**Sistem kullanımı ile ilgili olaylar**			
TO_AJ_7_5_1	Yeni proses başlatılması		B	
TO_AJ_7_5_2	Prosesin durdurulması		B	
TO_AJ_7_5_3	Servis başlatılması		B	
TO_AJ_7_5_4	Servis durdurulması		B	
TO_AJ_7_5_5	Program kurulması		B	
TO_AJ_7_5_6	Program kaldırılması		B	
TO_AJ_8	**Dizinler ve tercihe bağlı alt dizinler takibe alınabiliyor mu?**		B	
TO_AJ_8_1	**Dosya Olayları (Takip edilen dizinler ile ilgili)**			
TO_AJ_8_1_2	Dosya oluşturulması		B	
TO_AJ_8_1_3	Dosya silinmesi		B	
TO_AJ_8_1_4	Dosya isim değişikliği		B	
TO_AJ_8_1_5	Dosya içeriğinin değiştirilmesi		B	
TO_AJ_8_2	**Paylaşıma açık dizinler**			
TO_AJ_8_2_1	Paylaşılan dosyanın açılması		B	
TO_AJ_8_2_2	Paylaşılan dosyanın kapanması		B	
TO_AJ_8_2_3	Ağ üzerinden paylaşılan dizine erişim yapılması		B	
TO_AJ_8_3	**USB Bellek Olayları**			
TO_AJ_8_3_1	USB takılması	C		
TO_AJ_8_3_2	İzin verilen USB'ye kontrol altındaki dokümanın kullanıcı tercihine bırakılmadan şifreli atılması		B	
TO_AJ_8_3_3	USB içindeki dosyaların (verilen yol bilgisi) izlenmesi (Yeni dosya, İsim değişikliği, Dosya silinmesi)			A
TO_AJ_8_3_4	Sadece izin verilen USB cihazların kullanımına izin veriliyor mu?	C		
TO_AJ_8_3_5	Gizli bilgilerin USB Bellek içerisine şifrelenerek kopyalanması sağlanabiliyor mu?			A
TO_AJ_8_4	**Yazıcı olayları**			
TO_AJ_8_4_1	Yeni yazıcı (sürücüsü) eklenmesinin engellenmesi			A
TO_AJ_8_4_2	Yazıcının (sürücüsü) silinmesinin engellenmesi			A
TO_AJ_8_4_3	Doküman yazdırmanın engellenmesi			A

TO_AJ_9	**Ajan tarafından, içerik sınıflandırmasına bağlı olarak, aşağıdaki engellemeler gerçekleştiriliyor mu?**	C		
TO_AJ_9_1	**Proses Engelleme**			
TO_AJ_9_1_1	Ajanın çalıştığı processin durdurulmasının engellenmesi	C		
TO_AJ_9_1_2	İzin verilmeyen prosesler (BlackList) çalışıyorsa durdurulması ve tekrar çalışmasının engellenmesi		B	
TO_AJ_9_2	**Doküman Engellemeleri**			
TO_AJ_9_2_1	Dosya kopyalamanın engellenmesi	C		
TO_AJ_9_2_2	Dosyaların silinmesinin, isim değişikliğinin ve içerik değişiminin engellenmesi	C		
TO_AJ_9_2_3	Dosyaların çalıştırılmaların engellenmesi (executable)	C		
TO_AJ_9_2_4	Dosyaların “Farklı Kaydet” engellenmesi	C		
TO_AJ_9_2_5	Dosyaların kısayol oluşturulmasının engellenmesi		B	
TO_AJ_9_2_6	Dosyaların güvenlik özelliklerinin değiştirilmesinin engellenmesi	C		
TO_AJ_9_2_7	Kurala uyan dosyaların gizlenebilmesi		B	
TO_AJ_9_3	**Diğer Engellemeler**			
TO_AJ_9_3_1	OCR kullanarak ekran görüntüsü almanın engellenmesi	C		
TO_AJ_9_3_2	USB ID ile izin verilen USB’lerin görüntülenmesi ve izin verilmeyenlerin engellenmesi	C		
TO_AJ_9_4	**Keşif Olayları**			
TO_AJ_9_4_1	Sistem, keşif politikaları yoluyla istemci makinelerde bulunan dosyaların içeriklerine göre etiketlenmesini sağlayabiliyor mu?	C		
TO_AJ_9_4_2	Kritik bilgilerin sisteme öğretilebilmesi için, sistem kritik bilgilerin bulunduğu dosyaların parmak izini alabiliyor mu?	C		
TO_AJ_9_4_3	Sistem, parmak izi politikaları yoluyla istemci makinelerde bulunan dosyaların içeriklerine göre kontrol edilebilmesini sağlayabiliyor mu?	C		
TO_AJ_9_4_4	Sistem, parmak izi vasıtası ile belirtilen önemli dosyaların takip edilmesini sağlayabiliyor mu, böylece bu dosyalar içerisinden alınabilecek kısmi veri bloklarının kurum dışına çıkarılmasına engel olabiliyor mu?	C		
TO_AJ_10	**Ajan tarafından belirli periyotlarda aşağıdaki bilgiler toplanıyor ve sunucuya gönderiliyor mu?**		B	
TO_AJ_10_1	Anlık disk durumu		B	
TO_AJ_10_2	Anlık bellek kullanımı		B	
TO_AJ_10_3	Proses listesi		B	
TO_AJ_10_4	Proseslerin bellek ve CPU kullanımı		B	
TO_SN	**Sınıflandırma**			
TO_SN_1	**Aşağıdaki sınıflandırma yaklaşımları destekleniyor mu?**			
TO_SN_1_1	İçerik Analizi (Makine öğrenmesi yaklaşımı)	C		
TO_SN_1_2	Dosyanın Özellikleri (Dosya Boyutu gibi)		B	
TO_SN_1_3	Örüntü Tarama (Regex)	C		

TO_SN_1_4	Yaygın olarak kullanılan (Office, Pdf) dokümanların sınıflandırması gerçekleştirilebiliyor mu?	C		
TO_SN_1_5	Sınıflandırma hizmetinde, farklı öğrenme algoritmaların entegrasyon imkânı var mıdır?			A
TO_SN_1_6	Resim içerikler için, Optik Karakter Tanıma (OCR) entegrasyonu gerçekleştiriliyor mu?	C		
TO_SN_1_7	Resim içerikler için, Akıllı Karakter tanıma (ICR) entegrasyonu gerçekleştiriliyor mu?		B	
TO_SN_1_8	Manual yöntem ile sınıflandırma yapılabiliyor mu?	C		
TO_SN_1_9	Dosyanın keşif taramasından sonra otomatik sınıflandırması yapılabiliyor mu?	C		
TO_OKY	**Olay Kayıt Yönetimi**			
TO_OKY_1	**Ajanlar tarafından tespit edilen olaylar için aşağıdaki ortak özellikler sağlanıyor mu?**	C		
TO_OKY_1_1	Olay kaynak bilgileri (MakineAdı,IP)	C		
TO_OKY_1_2	Kritiklik seviyesi	C		
TO_OKY_1_3	Olay zamanı	C		
TO_OKY_2	Olay hakkında özel bilgiler toplanıyor mu? (Olay çeşidine bağlı)	C		
TO_OKY_3	Olay kayıtları, minimum ortak alanlara göre indeksleniyor mu?	C		
TO_OKY_4	Olay kayıtları, belirlenen zaman dilimine göre, arşivlenebiliyor mu? (Eski olay kayıtları)	C		
TO_OKY_5	Oluşan log kayıtları geriye doğru incelenebiliyor mu?	C		
TO_RY	**Raporlama ve Yönetim**			
TO_RY_1	Sisteme güvenli giriş yapılabiliyor mu? (Login)	C		
TO_RY_2	Kullanıcıya sadece yetkili olduğu işlemler sunulabiliyor mu? (Kullanıcı-Rol bazlı model)	C		
TO_RY_3	Kullanıcı ve Rol tanımlanabiliyor mu?	C		
TO_RY_4	Kullanıcının profilini güncelleme imkanı var mı? (Kullanıcı parametreleri, Kullanıcı bilgileri)	C		
TO_RY_5	Varlıklarlar yönetilebiliyor mu? (Assets)	C		
TO_RY_6	Kullanıcı ve varlık ilişkilendirilmesi yapılabiliyor mu?	C		
TO_RY_7	Kurulu olan ajan sayısı ve anlık çalışma durumları görüntülenebiliyor mu? (Dashboard)	C		
TO_RY_8	Ajan kurma, kaldırma, başlatma, durdurma işlemleri gerçekleştirilebiliyor mu?		B	
TO_RY_9	Politika oluşturma, uygulama ve uygulanan politikaları görüntüleme yapılabiliyor mu?	C		
TO_RY_10	**Olay görünümü grafik (Dashboard) olarak izlenebiliyor mu? Grafik üzerinden detay bilgilere erişim sağlanabiliyor mu?**	C		
TO_RY_10_1	Ajana ait tüm olaylar	C		
TO_RY_10_2	Zamana bağlı oluşan engelleme olayları	C		
TO_RY_11	Varlık Görünümü (Dashboard) izlenebiliyor mu?	C		

TO_RY_12	**Varlıkların Kaynak tüketim analizi izlenebiliyor mu?**		B	
TO_RY_12_1	Tüm Kaynaklar		B	
TO_RY_12_2	Kaynak bazında		B	
TO_RY_12_3	Alınan raporlar dosya olarak yerel diske kaydedilebiliyor mu?		B	
TO_RY_13	Varlıklarda en çok kaynak (Bellek,CPU) tüketen işlemler listesi (TOP X) alınabiliyor mu?		B	
TO_RY_14	Keşif kayıtlarının oluşturulmasına ilişkin istatistiki bilgiler görüntülenebiliyor mu?	C		
TO_RY_15	İlk başta izleme modunda kurup, bir süre boyunca bilgisayarın normal kaynak tüketimini profilleyip, daha sonra koruma moduna alındığında, hangi process' lerin fail ettiğini veya profilin dışında anormal kaynak tükettiğini raporlayabilir mi?			A
TO_UD	**Ürün Dokümantasyonu**			
TO_UD_1	Ürün dokümanları Türkçe dil desteğine sahip mi?	C		
TO_UD_2	Ürün dokümanları İngilizce dil desteğine sahip mi?		B	
TO_UD_3	Ürüne ilişkin dokümantasyon (yazılı materyal ve tool tip) var mıdır?	C		
TO_UD_4	Üreticinin ürüne ilişkin forum, bilgi deposu ve çağrı sistemi vb. web sayfaları var mı?		B	
TO_UD_5	Ürünün temel özellikleri ile ilgili nasıl yapılır videoları veya makaleleri var mı?		B	
TO_UD_6	Ürünün üretici tarafından yayınlanan güncellemelerine ilişkin sürüm notları ile mevcut mudur?	C		
PK	**4. Performans / Kapasite**			
PK_1	**Ürüne ilişkin aşağıdaki testler yapılarak performans raporu alınmalıdır.**	C		
PK_1_1	**Dosyalardan Metin ve Özellik Çıkarımı Performansı**			
PK_1_1_1	Metin türündeki (MSOffice/OpenOffice/TXT vb.) metin dosyalarından içerik çıkarım hızı	C		
PK_1_1_2	PDF/RTF/HTML/XML türünden dosyalardan metin çıkarım hızı		B	
PK_1_1_3	Farklı türden dosya tipi içeren sıkıştırılmış dosyalardan metin çıkarımı hızı	C		
PK_1_1_4	Resim türündeki (JPG/PNG/Bitmap vb.) dokümanlardan OCR ile metin çıkarım hızı	C		
PK_1_1_5	El yazısı içeren dokümanlardan ICR ile metin çıkarım hızı		B	
PK_1_1_6	E-mail içeriklerinin metin çıkarımı hızı	C		
PK_1_1_7	E-mail' e ek olarak eklenen dosyaların yakalanıp metin çıkarımı hızı	C		
PK_1_1_8	Sınıflandırılan dokümanlara metadata bilgisi ekleme hızı		B	
PK_1_1_9	Sınıflandırılan dokümanlardan metadata bilgisi çıkarım hızı		B	
PK_1_1_10	Dosyanın sahibi, boyutu, uzantısı vb. gibi özelliklerinin çıkarım hızı		B	
PK_1_1_11	Şifrelenmiş dosyaların yeniden açılmasının hızı	C		
PK_1_1_12	Çok büyük boyuttaki (3-5 GB) dosyalardan metin çıkarımı hızı	C		

PK_1_2	**Sınıflandırma Performansı**			
PK_1_2_1	Doküman içeriğine göre sınıflandırma hızı	C		
PK_1_2_2	Doküman özelliklerine göre sınıflandırma hızı		B	
PK_1_2_3	Dokümanın içeriğindeki ifadelere göre sınıflandırma (Regex ve ön tanımlı listeler) hızı	C		
PK_1_2_4	Birden fazla gruba göre değerlendirerek sınıflandırma hızı			A
PK_1_2_5	Arka planda çalışan lokal sınıflandırma ve etiketleme işlemi performansı (crawling) hızı	C		
PK_1_3	**Engelleme Performansı**			
PK_1_3_1	Web browsing engelleme (IP ve/veya Port ile) hızı	C		
PK_1_3_2	Network üzerinden dosya transferi engelleme (HTTP/HTTPS/FTP) hızı	C		
PK_1_3_3	Yazıcı ve fax cihazlarına gönderilen dosyaların engellenme hızı		B	
PK_1_3_4	Kopyalama panosu ve ekran görüntüsü almanın engellenme hızı	C		
PK_1_3_5	İzinsiz takılan harici cihazları engelleme (Printer/Fax/USB vb.) hızı	C		
PK_1_3_6	Blacklist prosesleri durdurma ve engelleme hızı	C		
PK_1_3_7	Harici ortamlara ve harici ortamlardan yapılan veri kopyalama işlemlerinin engellenmesi hızı	C		
PK_1_3_8	E-mail gönderimi engelleme hızı	C		
PK_1_4	**Ajan Yönetimi Performansı**			
PK_1_4_1	Web arayüzü kullanarak ajanın kurulum hızı	C		
PK_1_4_2	Web arayüzü kullanarak ajanın başlatılma ve durdurulması hızı	C		
PK_1_4_3	İstemci makine yeniden başlatıldığında ajanın otomatik başlaması hızı	C		
PK_1_4_4	Ajanın politikalarının güncellenmesi hızı	C		
PK_1_4_5	Ajan olaylarının ağırlıklarının (severity) güncellenmesi hızı	C		
PK_1_4_6	Ajanın sınıflandırma kurallarının güncellenmesi hızı	C		
PK_1_5	**Çalışma Performansı**			
PK_1_5_1	Ürünün RAM, Disk, CPU, Ağ ve Güç tüketim miktarı	C		
PK_1_5_2	Birden fazla politika veya iş aldığında çalışma performansı	C		
PK_1_5_3	Aynı anda çoklu dosya kopyalama olayı karşısındaki performans	C		
PK_1_5_4	Olay döngü performans (yakalama-> yayınlama->alarm üretme) hızı	C		
PK_1_6	**SQL veritabanı performansı**			
PK_1_6_1	Veritabanında ilişkisel olarak saklanan verilerin (konfigürasyon, güvenlik, varlık vb.) sorgulama performansı hızı	C		
PK_1_6_2	Yazma ve güncelleme performansı hızı	C		
PK_1_6_3	Veritabanı işlemlerinde indeks kullanım değerlendirmesi hızı		B	

PK_1_7	**Kapasite**			
PK_1_7_1	Sistem büyüklüğüne ait özellikler: Kullanıcı sayısı, Ajan sayısı, Birim zamanda doküman işleme hızı	C		
PK_1_7_2	Minimum değerler: RAM, Disk, CPU, Ağ, Güç tüketim miktarı	C		
PK_1_7_3	Minimum İşletim Sistemi: Windows 8 (32/64) bit, Ubuntu 16.04 ve Pardus 17	C		
	5- REGÜLASYONLARA UYUM			
RU_1	Ulusal çerçeveler içerisinde bağlayıcı kanun hükümlerine uyumluluk sağlıyor mu? (KVKK vb.)	C		
RU_2	Uluslararası anlaşmalar dahilinde uyulması gereken standartlar karşılanıyor mu? (GDPR vb.)			A
	6- DİĞER HUSUSLAR			
DH_1	SIEM sistemlerine olay bilgilerinin aktarılması için log dosyası üretilebiliyor mu? (DLP Log dosyası)		B	
DH_2	Yüksek seviye performans ve sistem sürekliliği gerektiren kurulumlar için, yatay ve dikeyde ölçeklendirilebilir mimariye sahip mi? Örnek (cluster mimarisi)		B	