TRtest
Test ve Değerlendirme A.Ş.

ZAFİYET YÖNETİMİ ÜRÜN GRUBU KRİTERLERİ

No	Başlık/Soru	B (Temel Seviye)	A (Üst Seviye)
UG	**1- Ürün Güvenliği**		
UG_DY	**Doğrulama ve Yetkilendirme**		
UG_DY_1	Oturum açmak için kimlik doğrulaması yapılıyor mu?	B	
UG_DY_2	Uzun süre etkileşim olmadığında oturum zaman aşımı özelliği var mı?	B	
UG_DY_3	Kullanıcı tanımlanabiliyor mu?	B	
UG_DY_4	Kullanıcı parolası tanımlarken kullanılan karakter ve uzunluk gibi zorluk kriterleri kontrol ediliyor mu?	B	
UG_DY_5	Kullanıcı doğrulaması için dizin servisleri (LDAP, Active Directory) ile entegrasyon yeteneği var mı?	B	
UG_DY_6	Kullanıcı hesapları pasif/geçici devre dışı bırakılabiliyor mu?	B	
UG_DY_7	Kullanıcılara rol ataması yapılabiliyor mu?	B	
UG_DY_8	Sistemdeki bilgileri görebilecek (readonly) yetkisine sahip kullanıcı tanımlanabiliyor mu?	B	
UG_DY_9	Rol bazlı erişim kısıtlamaları uygulanıyor mu?	B	
UG_WG	**Web Güvenliği**		
UG_WG_1	Güvenli iletişim kanalları destekleniyor mu? (HTTPS)	B	
UG_WG_2	Zararlı girdi kontrolü yapılıyor mu?	B	
UG_WG_3	Çıktı kodlama yapılıyor mu?	B	
UG_WG_4	OWASP Top 10 de belirtilmiş zafiyetlere karşı güvenli mi?	B	
UG_BG	**Bilgi Güvenliği**		
UG_BG_1	Veri tabanında hassas veriler şifrelenmiş tutuluyor mu?	B	
UG_BG_2	Veri tabanına erişim güvenli mi?	B	
UG_BG_3	Uygulama veri tabanı yedeklemesi yapıyor mu?		A
UG_EG	**Entegrasyon Güvenliği**		
UG_EG_1	Entegre olunan servisler ile güvenli iletişim kanalları üzerinden haberleşmeyi destekliyor mu?	B	
UG_EG_2	Ağ ve istemci/sunucu cihazlara bağlanmak için erişim parametresi (yöntem, kullanıcı adı, şifre) tanımlamaya imkân veriyor mu?	B	

UG_EG_3	Erişim parametrelerinin geçerliliği uygulama üzerinden test edilebiliyor mu?		A
TO	**2- Temel Özellikler**		
TO_GO	**Genel Özellikler**		
TO_GO_1	Web tabanlı mimari ve kullanıcı arayüzü sunuyor mu?	B	
TO_GO_2	Birden çok kullanıcının eş zamanlı olarak uygulamaya erişimini destekliyor mu?	B	
TO_GO_3	Kullanıcı ara yüzü Türkçe dilini destekliyor mu?	B	
TO_GO_4	Kullanıcı ara yüzünün yabancı dil desteği var mı?		A
TO_GO_5	Kullanıcı bazında kullanıcı ara yüzü dil seçim yeteneği var mı?		A
TO_GO_6	Zafiyet tanımları içerisinde Türkçe içerik mevcut mu?		A
TO_GO_7	Kullanıcı eposta bilgilendirmelerinde kullanılan formatlar özelleştirilebiliyor mu?		A
TO_GO_8	Uygulama, varlık grubu ya da özelliği bazında yetkilendirmeyi destekliyor mu? (Lokasyon, kategori, sahiplik gibi kriterlerden en az biri)		A
TO_GO_9	Uygulama, dizin servislerinden (LDAP, Active Directory) organizasyon, grup ve kullanıcı bilgilerini kimlik doğrulama için kullanabiliyor mu?		A
TO_GO_10	Hızlı kurulum yeteneği (bileşenleri otomatik kurma) mevcut mu?		A
TO_GO_11	Uygulama, birim/grup/departman bazında yetkilendirmeye izin veriyor mu?		A
TO_GO_12	Kullanıcı aktiviteleri kaydediliyor mu?	B	
TO_GO_13	Farklı ağlardan yapılan izlemelerin/taramaların verileri merkezi noktada görüntülenebiliyor mu?		A
TO_GO_14	Sistem üzerinden syslog aracılığıyla dışarıya veri gönderilebiliyor mu?		A
TO_GO_15	Geçmişe ait, belirli bir süreden önceki verileri otomatik silebilme özelliği var mı?		A
TO_NZY	**Network Zafiyet Yönetimi**		
TO_NZY_1	Ürün kendisi veya 3.parti network zafiyet tarama araçları üzerinden varlık - zafiyet tespiti yapabiliyor mu?	B	
TO_NZY_2	Varlıklar (istemci / sunucu cihazlar, yazılımlar) tespit edebiliyor mu?	B	
TO_NZY_3	Varlıklar üzerindeki açık portları tespit edebiliyor mu?	B	
TO_NZY_4	Varlıklar üzerindeki zafiyetleri tespit edebiliyor mu?	B	
TO_NZY_5	Varlık-zafiyet tarama görevleri programlanarak otomatik yapılabiliyor mu?	B	
TO_NZY_6	Geçmişteki varlık-zafiyet taramalarını ve sonuçlarını gösterebiliyor mu?	B	
TO_NZY_7	Geçmişteki varlık-zafiyet taramaları arasındaki bulgu farklılıklarını gösterebiliyor mu?		A
TO_NZY_8	Uygulama, periyodik taramaları geçici olarak pasif duruma çekebiliyor mu?	B	
TO_NZY_9	Varlık/Varlık grubu seçerek zafiyet tarama hedefi belirleme imkânı sunuyor mu? (Varlık grubu, subnet, IP aralığı vs.)	B	

TO_NZY_10	Uygulama, taramalarda hariç bırakılacak varlıkların (excluded IPs) tanımlanabilmesini sağlayabiliyor mu?		A
TO_NZY_11	Zafiyet tarama için ön tanımlı tarama politikalarını kullanıcının seçmesine imkân sağlıyor mu?	B	
TO_NZY_12	Tarama görevi, profil ve politika bazında özelleştirilebiliyor mu?		A
TO_NZY_13	▪ SSH oturumu açarak tarama yeteneği var mı?		A
TO_NZY_14	▪ Windows/SMB oturumu açarak tarama yeteneği var mı?		A
TO_VZY	**Varlık-Zafiyet Yönetimi**		
TO_VZY_1	Varlık-zafiyet tarama sonuçlarını kaynaştırarak organizasyondaki varlık ve zafiyetlerin son durumuna ilişkin bir görüntü sunabiliyor mu?	B	
TO_VZY_2	Varlıklar listelenebiliyor mu?	B	
TO_VZY_3	Uygulama, varlık listelerini dışarıya aktarabiliyor mu?	B	
TO_VZY_4	Uygulama, varlık listelerini içeri aktarabiliyor mu?		A
TO_VZY_5	Varlıkların istismar edilebilirlik durumunu gösterebiliyor mu?		A
TO_VZY_6	Seçili varlığın üzerindeki zafiyetleri gösterebiliyor mu?	B	
TO_VZY_7	Zafiyetler listelenebiliyor mu?	B	
TO_VZY_8	Uygulama, zafiyet listelerini dışarıya aktarabiliyor mu?	B	
TO_VZY_9	Seçili varlığın üzerindeki açık port ve servisleri gösterebiliyor mu?	B	
TO_VZY_10	Seçili varlığın güvenli hale getirilmesi için öneri sunuyor mu?	B	
TO_VZY_11	Varlığın silinmesini destekleniyor mu?	B	
TO_VZY_12	Tarama sonuçlarının sistem üzerinden silinmesi destekleniyor mu?		A
TO_VZY_13	Zafiyetlerin global referansları (CVE vb.) gösterilebiliyor mu?	B	
TO_VZY_14	Zafiyetlerin istismar edilebilirlik durumunu gösterebiliyor mu?		A
TO_VZY_15	Seçili zafiyetin hangi varlıklarda olduğunu gösterebiliyor mu?	B	
TO_VZY_16	Seçili zafiyetin hangi varlık grupları içinde olduğunu gösterebiliyor mu?		A
TO_VZY_17	Zafiyetleri belli kategorilerde gruplayarak gösterme imkânı var mı?		A
TO_VZY_18	Zafiyet tarama araçlarından alınan tarama sonuçları dosyadan sisteme yüklenebiliyor mu?		A
TO_VZY_19	Zamana bağlı varlık sayısı değişimi gösterilebiliyor mu?	B	
TO_VZY_20	Uygulama, varlık gruplama özelliğine sahip midir? Bir varlık birden çok gruba dahil edilebiliyor mu? Varlık grubu hiyerarşik olarak tanımlanabiliyor mu?		A
TO_VZY_21	Uygulamada zafiyet, varlık, ticket gibi nesneler üzerinde toplu işlem yapmayı destekliyor mu?		A

TO_VZY_22	Zafiyetlerin zamana bağlı sayısal değişimi gösterilebiliyor mu?	B	
TO_RH	**Risk Hesaplama**		
TO_RH_1	Varlık bazlı risk durumu gösterilebiliyor mu?	B	
TO_RH_2	Varlık gruplarının risk durumu gösterilebiliyor mu?		A
TO_RH_3	Sistem genel riski hesaplanabiliyor mu?	B	
TO_RH_4	Varlıkların kritiklik durumları risk değerlendirmesine dahil edebiliyor mu?		A
TO_RH_5	Uygulama, belirli zafiyet ve varlık parametreleri üzerinden zafiyet ve varlık önceliklendirme yapabiliyor mu?		A
TO_IBY	**İş ve Bildirim Yönetimi**		
TO_IBY_1	Tarama ile ilgili olarak ilgililere bildirim gönderebiliyor mu?	B	
TO_IBY_2	Bildirim için kriter kullanılabiliyor mu?		A
TO_IBY_3	Bildirimin yapılacağı hedef kullanıcı/grup belirlenebiliyor ya da seçimi yapılabiliyor mu?	B	
TO_IBY_4	Kullanıcı ara yüzü üzerinde bildirim yeteneğine sahip mi?	B	
TO_IBY_5	E-posta ile bildirim yapabiliyor mu?	B	
TO_IBY_6	Tarama sonucuna göre otomatik iş/olay/görev oluşturabiliyor mu?		A
TO_IBY_7	Kullanıcının manuel iş/görev tanımlamasına imkân sunuyor mu?		A
TO_IBY_8	Tanımlanan işler üzerinde atanan kişiyi/grubu ve işin durumunu değiştirme imkânı sunuyor mu?		A
TO_IBY_9	İş tanımlama ve düzenleme operasyonlarından bildirim yoluyla ilgilileri haberdar edebiliyor mu?		A
TO_IBY_10	İş üzerinde yapılan atama ve durum değişikliği gibi operasyonlara ilişkin geçmiş bilgisi gösterebiliyor mu?		A
TO_IBY_11	İşler üzerinde filtreleme imkânı sunuluyor mu?		A
TO_IBY_12	Tarama sonucuna göre otomatik iş/olay/görev kapatılabiliyor mu?		A
TO_IBY_13	Uygulama, varlık keşfi sonrası yeni tespit edilen sunucu veya servis olduğu durumda ilgili kullanıcılara bildirim yapabiliyor mu?		A
TO_IBY_14	İşlerin hedef çözüm süresi tanımlanabiliyor mu?		A
TO_IBY_15	Hedef çözüm süresi ve gerçekleşen çözüm süresi takip edilebiliyor mu?		A
TO_IBY_16	Uygulama, çözüm süreleri ile ilgili hatırlatma e-postaları göndermeyi destekliyor mu?		A
TO_IBY_17	Uygulama, tarama sonucunda iş/olay/görev yönetimine aktarılacak minimum risk seviyesinin seçilebilmesini destekliyor mu?		A
TO_IBY_18	Uygulama, zafiyet kapatırken belirlenen formatta kanıt dosyası ekleyebilmeyi sağlayabiliyor mu?		A
TO_AF	**Arama ve Filtreleme**		

TO_AF_1	Görüntülenen varlık ve zafiyetleri, kullanıcının gireceği arama kriterleri ile filtreleme imkânı sunuyor mu?	B	
TO_AF_2	Varlık seçilerek filtreleme yapılabiliyor mu?	B	
TO_AF_3	Varlık grupları seçilerek filtreleme yapılabiliyor mu?		A
TO_AF_4	Zafiyet seçilerek filtreleme yapılabiliyor mu?	B	
TO_AF_5	Zafiyetler belirli seçeneklere göre (Örnek: port, risk seviyesi, servis, yazılım vb.) seçilerek filtreleme yapılabiliyor mu?	B	
TO_AF_6	Zafiyet araması tam metin arama imkânı sunuyor mu?	B	
TO_R	**Raporlama**		
TO_R_1	Varlık-Zafiyet tarama sonuçlarını gösteren PDF formatında rapor üretebiliyor mu?	B	
TO_R_2	MS Word/Excel/CSV gibi alternatif formatlarda rapor üretebiliyor mu?		A
TO_R_3	Uygulama, teknik ve yönetici özet raporu oluşturabiliyor mu?	B	
TO_R_4	Kullanıcının gireceği kriterlere göre rapor içeriğini filtreleme/daraltma imkânı sunuyor mu?	B	
TO_R_5	Ürünlerden alınan raporlarda format özelleştirilebiliyor mu? (logo , isim gibi)		A
TO_UD	**Ürün Dokümantasyonu**		
TO_UD_1	Ürün dokümantasyonu var mıdır?(Yazılı materyal veya Tool Tip vb.)	B	
TO_UD_2	Üretici web sayfasında ürünle ilgili bilgilendirme mevcut mudur?	B	
EM	**3- EK Modüller** (Bu bölümün altında bulunan kırmızı başlıklardaki fonksiyonları sağladığını iddia eden üreticiler, altında belirtilmiş olan kriterleri sağlamalıdır.)		
EM_WZY	**Web Zafiyet Yönetimi**		
EM_WZY_1	Ürün kendisi veya 3.parti web uygulama zafiyet tarama araçları üzerinden varlık - zafiyet tespiti yapabiliyor mu?	B	
EM_WZY_2	Varlıklar üzerindeki zafiyetleri tespit edebiliyor mu?	B	
EM_WZY_3	Varlık-zafiyet tarama görevleri programlanarak otomatik yapılabiliyor mu?	B	
EM_WZY_4	Geçmişteki varlık-zafiyet taramalarını ve sonuçlarını gösterebiliyor mu?	B	
EM_WZY_5	Geçmişteki varlık-zafiyet taramaları arasındaki bulgu farklılıklarını gösterebiliyor mu?		A
EM_WZY_6	Uygulama, periyodik taramaları geçici olarak pasif duruma çekebiliyor mu?	B	
EM_WZY_7	Uygulama, taramalarda hariç bırakılacak varlıkların (excluded URL) tanımlanabilmesini sağlayabiliyor mu?		A
EM_WZY_8	Zafiyet tarama için ön tanımlı tarama politikalarını kullanıcının seçmesine imkân sağlıyor mu?	B	
EM_WZY_9	Uygulama, zafiyet listelerini dışarıya aktarabiliyor mu?	B	
EM_WZY_10	Tarama görevi, profil ve politika bazında özelleştirilebiliyor mu?		A
EM_ATY	**Ağ Topoloji Yönetimi**		

EM_ATY_1	Manuel olarak ağ cihazı tanımlama/düzenleme yeteneği var mı?	B	
EM_ATY_2	Ağ keşif yeteneği var mı?		A
EM_ATY_3	Ağ cihazı tanımlamadan tam otomatik olarak ağ keşfi yapabiliyor mu?		A
EM_ATY_4	Yönlendirici ve Firewall cihazlarının keşfini yapabiliyor mu?		A
EM_ATY_5	Ağ keşif görevleri programlanarak otomatik yapılabiliyor mu?		A
EM_ATY_6	Yönlendirici ve firewall cihazlarından yapılandırma çekebiliyor mu?		A
EM_ATY_7	Ağ cihazlarından SNMP(v2/v3) ve/veya SSH destekli bilgi toplama yeteneği var mı?		A
EM_ATY_8	Ağ keşif sonuçlarını kaynaştırarak topolojinin son durumuna ilişkin bir görüntü (topoloji haritası) sunabiliyor mu?	B	
EM_ATY_9	Topoloji haritasını bir ağ diyagramı üzerinde görselleştirme özelliği var mı?	B	
EM_ATY_10	Topoloji haritası kullanıcı etkileşimini (seçerek detay görüntüleme, çeşitli işlevleri tetikleme, vb.) destekliyor mu?	B	
EM_ATY_11	Topoloji üzerinden seçim yaparak varlık-zafiyet tarama hedefi belirleme imkânı sunuyor mu?	B	
EM_ATY_12	Varlık-zafiyet taramasında tespit edilen varlıklar bağlı oldukları alt ağlar altına otomatik yerleştirme yeteneği var mı?	B	
EM_ATY_13	Ağ cihazlarından çevrim dışı (dosyadan yükleme yoluyla) yapılandırma bilgisi alınarak kaynaştırılabiliyor mu?		A
EM_ATY_14	Topolojideki varlıkların değişimleri zamana bağlı sayısal olarak gösterebiliyor mu?		A
EM_SI	**Siber İstihbarat**		
EM_SI_1	Tehdit istihbaratı, alt alan adı (subdomain) verisini listeleyebiliyor mu?		A
EM_SI_2	Uygulama, kuruma ait hassas bilgi içeren veri sızıntısı (data leakage) kayıtlarını listeleyebiliyor mu?	B	
EM_SI_3	Uygulama, kuruma ait çalınmış e-posta hesaplarını (leaked accounts) listeleyebiliyor mu?	B	
EM_SI_4	Uygulama, kurum için saldırı olasılığına sahip oltalama (phishing) alan adlarını listeleyebiliyor mu?	B	
EM_SI_5	Oltalama takibi sağlanan alan adlarının web site içerik yayını kontrol edilebiliyor mu?		A
EM_SI_6	Uygulama, botnet IP, Url ve domain için kara liste kayıtlarını listeleyebiliyor mu?	B	
EM_SI_7	Uygulama, kurum adına phishing amacıyla kullanılabilecek sosyal medya hesaplarını listeleyebiliyor mu?		A
EM_SI_8	İstihbarat verileri kullanıcılara sunulmadan önce false-positive ayıklaması yapılabiliyor mu?		A
EM_SI_9	İstihbarat verileri, manuel olarak eklenip silinebiliyor mu?		A
EM_SI_10	Belirlenen kriterler doğrultusunda kullanıcılara bildirim yapılabiliyor mu?		A
EM_SI_11	İstihbarat verilerine göre otomatik iş/olay/görev oluşturulabiliyor mu?	B	

EM_SI_12	Coğrafi olarak Siber Tehdit haritası gösteriliyor mu?		A
EM_ZI	**Zafiyet İstihbaratı**		
EM_ZI_1	Tespit edilen zafiyetlere yönelik zafiyet istihbarat bilgisi gösterimi var mı?	B	
EM_ZI_2	Tespit edilen zafiyetlere yönelik zafiyet istihbarat risk puanı gösteriyor mu?	B	
EM_TA	**Tehdit Analizi**		
EM_TA_1	Kullanıcı tehdit kaynağı tanımlayabiliyor mu?	B	
EM_TA_2	Tehdit kaynaklarından başlayacak şekilde saldırı simülasyonu yapabiliyor mu?	B	
EM_TA_3	Simülasyon sonunda saldırı yolları gösterilebiliyor mu?	B	
EM_TA_4	Saldırı simülasyonu topoloji ve firewall kısıtlamalarını dikkate alıyor mu?		A
EM_TA_5	Saldırı simülasyonu tespit edilen zafiyetleri dikkate alıyor mu?	B	
EM_TA_6	Saldırı simülasyonu aynı makine üzerinde yetki yükseltimini simüle ediyor mu?	B	
EM_TA_7	Saldırı simülasyonunu dikkate alarak risk hesaplama özelliği var mı?		A
EM_TA_8	Kullanıcılar tarafından saldırılara karşı önlem senaryoları oluşturulabiliyor mu?		A
EM_TA_9	Koruyucu önlem senaryoları uygulanmak üzere ilgililere iş olarak atanabiliyor mu?		A
EM_KKA	**Kaynak Kod Analizi**		
EM_KKA_1	Uygulama, kod analiz araçlarıyla entegrasyon sağlayabiliyor mu?	B	
EM_KKA_2	Uygulama, belirli kriterler doğrultusunda otomatik olarak kaynak kod analiz araçları üzerinden kod analizi yapabiliyor mu?	B	
EM_KKA_3	Uygulama, kaynak kod analiz aracı çıktılarını otomatik ya da manuel olarak içeri aktarabiliyor mu?	B	
EM_KKA_4	Uygulama,versiyon kontrol araçlarından bilgi(commiter bilgisi vs.) çekebiliyor mu ?		A
EM_KKA_5	Uygulama, kaynak kod analiz sonuçlarını iş/olay/görev yönetimine aktarabiliyor mu ?		A
EM_KKA_6	Uygulama, periyodik tanımlanan taramalarda aynı iş/olay/görevin tekrar açılması engelleniyor mu?		A
EM_PT	**Pasif Tarama**		
EM_PT_1	Varlık Yönetim araçlarından varlık bilgilerini elde edebiliyor mu?	B	
EM_PT_2	Elde ettiği varlık bilgilerinden zafiyetleri çıkarabiliyor mu?		A
EM_EII	**Erişilebilirlik / İçerik İzleme**		
EM_EII_1	İzlemelere ilişkin (Web, SSL, Sunucu, port, DNS Kayıtları vb.) son durumları gösteren genel göstergeler var mı?	B	
EM_EII_2	Gösterge üzerinde uyarı durumları anlık gösterilebiliyor mu?	B	
EM_EII_3	Sanallaştırma platformlarını (VMware ESXi, Hyper-V vb.) izleyebiliyor mu?		A

EM_EII_4	▪Sanallaştırma platformları içerisindeki sanal sistemler otomatik keşfedilebiliyor mu?		A
EM_EII_5	▪Sanal sunucuların CPU, RAM, DISK gibi değerleri takip edilebiliyor mu?		A
EM_EII_6	HTTP/HTTPS, Web Servisler takip edilebiliyor mu?	B	
EM_EII_7	▪Web izlemelerindeki istekler (başlık, parametre, istek tipi vb.) özelleştirilebiliyor mu?		A
EM_EII_8	▪Web uygulamasının içerik değişimleri tespit edilebiliyor mu?	B	
EM_EII_9	▪Tespit edilen değişimler metin tabanlı olarak kullanıcıya sunulabiliyor mu?	B	
EM_EII_10	▪Tespit edilen değişimler görsel olarak kullanıcıya sunulabiliyor mu?		A
EM_EII_11	▪Web uygulamalarında sürekli değişen alanları izleme dışında tutma özelliği var mı?		A
EM_EII_12	DNS kayıtlarının sonuçlarını izleyebiliyor mu?	B	
EM_EII_13	▪DNS zehirlemeye karşın, yerel ve uzak DNS sunucularından sorgu sonuçlarını karşılaştırabiliyor mu?	B	
EM_EII_14	SSL Sertifikaları izlenebiliyor mu?	B	
EM_EII_15	▪Sertifika teknik özelliklerinde değişim olduğunda uyarı üretebiliyor mu?	B	
EM_EII_16	▪Sertifika geçerlilik süresine göre uyarı üretebiliyor mu?	B	
EM_EII_17	Alan adları Whois (Domain kayıt bilgileri) izlenebiliyor mu?	B	
EM_EII_18	▪Alan adının geçerlilik süresine göre uyarı üretebiliyor mu?	B	
EM_EII_19	▪Alan adının kayıt bilgilerine (isim, mail vb.) göre uyarı üretebiliyor mu?	B	
EM_EII_20	Varlıkların kaynak (CPU/RAM/DISK) izlemeleri yapılabiliyor mu?		A
EM_EII_21	▪Varlık kaynak izleme işlemleri gerçekleştirilebiliyor mu?		A
EM_EII_22	▪Varlık kaynak izleme işlemleri Windows ve Linux sistemlerde gerçekleştirilebiliyor mu?		A
EM_EII_23	▪Kaynak izlemede uyarı olması durumunda en çok kaynak tüketen uygulamalar listelenebiliyor mu?		A
EM_EII_24	Varlıkların Servis ve Süreç (Process) izlemeleri yapılabiliyor mu?		A
EM_EII_25	▪Varlık servis/süreç (Process) izleme işlemleri gerçekleştirilebiliyor mu?		A
EM_EII_26	▪Varlık kaynak izleme işlemleri Windows ve Linux sistemlerde gerçekleştirilebiliyor mu?		A
EM_EII_27	▪Sistem üzerindeki servisler otomatik olarak listelenebiliyor mu?		A
EM_EII_28	Varlıklar ping ile izlenebiliyor mu?	B	
EM_EII_29	▪Varlıklara erişilmediği durumlarda uyarı veriyor mu?	B	
EM_EII_30	▪Erişimler için paket kayıp yüzdesi eşik değeri belirtebiliyor mu?	B	
EM_EII_31	▪Otomatik keşif ile taranan ağ üzerinde bulunan varlıklar için çoklu ping izleme/ekleme özelliği destekleniyor mu?		A

EM_EII_32	Varlıklar SNMP (v2/v3) ile izlenebiliyor mu?	B	
EM_EII_33	Varlıkların port durumları (açık, kapalı) bazlı izlenebiliyor mu?	B	
EM_EII_34	Betik (script) kodlama ile izlemeler yapmaya izin veriyor mu?		A
EM_EII_35	Her izleme için bağlantı zaman aşımı süresi (timeout) seçilebiliyor mu?	B	
EM_EII_36	Her izleme için bağlantı yanıt süresi (response time) seçilebiliyor mu?	B	
EM_EII_37	Oluşan uyarılar için göz ardı et (çözüldü) seçeneği var mı?		A
EM_EII_38	Geçmişe dönük durum değişim, olay kayıtlarını gösterebiliyor mu?	B	
EM_EII_39	Geçmişe dönük değerler grafiksel olarak gösterilebiliyor mu?	B	
EM_EII_40	Belirli tarihler arasına yönelik olay/durum raporları (bilgi, trend, hata ve uyarı raporları vb.) verebiliyor mu?	B	
EM_EII_41	Periyodik olarak olay/durum raporları (bilgi, trend, hata ve uyarı raporları vb.) verebiliyor mu?		A