TRtest
Test ve Değerlendirme A.Ş.

UÇ NOKTA TEHDİT TESPİT VE AKTİF MÜDAHALE ÜRÜN GRUBU KRİTERLERİ (EDR)

ÖNEMLİ NOT:
1- Kırmızı renkli başlık **ZORUNLU** ise altındaki bütün **zorunlu** maddeler karşılanmalı,
2- Kırmızı renkli başlık **OPSİYONEL** ise üretici başlık altındaki maddeleri karşılamak zorunda değildir,
fakat ilgili opsiyonel başlığı karşıladığını iddia eden üreticiler, başlıkların altında belirtilmiş olan tüm kriterleri sağlamalıdır.
Karşılanan opsiyonel başlıklar sertifikada belirtilecektir.

No	Başlık/Soru	ZORUNLU	OPSİYONEL
TOGFT	**1- Temel Özellikler ve Güvenlik Fonksiyon Testi**		
TOGFT_AE	**Anti-Exploit (Exploit Tespit ve Engelleme)**	Z	
TOGFT_AE_1	Hafıza tabanlı exploit ataklarına karşı anti-exploit tekniklerine dayalı davranışsal koruma sağlıyor mu?	Z	
TOGFT_AE_2	Kernel exploit tekniklerine yönelik anti-exploit (anti-istismar) ve tespit yetenekleri mevcut mu?		O
TOGFT_AE_3	Mantıksal exploit ataklarına karşı (Office Macro, Office DDE vb.) davranışsal koruma veya tespit sağlıyor mu?	Z	
TOGFT_AE_4	İstenen uygulamalar/processler için anti-exploit teknikleri aktif veya pasif edilebiliyor mu?	Z	
TOGFT_AE_5	DEP, ASLR korumalarını süreçler için zorunlu olarak aktif edebiliyor mu?		O
TOGFT_AE_6	Uzaktan network üzerinden DLL yüklenmesini (UNC) tespit edebiliyor mu?	Z	
TOGFT_AE_7	Alt Süreç kısıtlama (child process restriction) koruması mevcut mu? Belirli uygulamaların hangi alt süreçleri oluşturup oluşturamayacağı belirlenebiliyor mu?	Z	
TOGFT_AE_8	Saldırı yüzeyini azaltma koruması kapsamında belirlenen DLL ' lerin uygulama tarafından hafızaya yüklenmesini tespit edebiliyor mu?	Z	
TOGFT_ZYTE	**Zararlı Yazılım Tespit ve Engelleme**	Z	
TOGFT_ZYTE1	Bilinen zararlı yazılım örneklerini tespit edebiliyor mu? (VirusTotal vb. yerlerden indirilen)	Z	
TOGFT_ZYTE2	Bilinen zararlı yazılımlar packlenerek (mpress, upx vb.) mutasyona uğratılıp imzası değiştirildiğinde ve bilinmeyen hale geldiğinde tespit edebiliyor mu?	Z	
TOGFT_ZYTE3	Msfvenom ile yeni oluşturulmuş Meterpreter çalıştırılabilir dosyalarını tespit edebiliyor mu?	Z	
TOGFT_ZYTE4	Belirlenen dizinlerden süreç (process) çalıştırılması yasaklanabiliyor mu?	Z	
TOGFT_ZYTE5	Belirlenen dizinlerden kod imzasız süreç (process) çalıştırılması yasaklanabiliyor mu?	Z	
TOGFT_ZYTE6	Belirlenen dizinlerden dosya oluşturulma zamanına bakarak süreç (process) çalıştırılması yasaklanabiliyor mu?		O
TOGFT_ZYTE7	Network üzerinden, çıkartılabilir disklerden süreç (process) çalıştırılması yasaklanabiliyor mu?	Z	
TOGFT_ZYTE8	Powershell zararlı yazılımlarını tespit edebiliyor mu?	Z	
TOGFT_ZYTE9	Bitsadmin çalıştığında tespit edebiliyor mu?	Z	

TOGFT_PLM	**Persistence ve Lateral Movement (Kalıcılık ve Yayılma)**	Z	
TOGFT_PLM_1	Credential Dumping atağını davranışsal tespit edebiliyor mu? (Mimikatz çalıştırılabilir dosya olarak)	Z	
TOGFT_PLM_2	Credential Dumping atağını davranışsal tespit edebiliyor mu? (Mimikatz powershell script olarak)	Z	
TOGFT_PLM_3	Process (Süreç) Enjeksiyonu (CreateRemoteThread vb.) ataklarını tespit edebiliyor mu?	Z	
TOGFT_PLM_4	Sticky Keys ile sağlanan kalıcılık atağını tespit edebiliyor mu?	Z	
TOGFT_ISTAM	**İhlal Sonrası Tespit ve Aktif Müdahale**	Z	
TOGFT_ISTAM_1	Daha önceden enfekte / enjekte olmuş aktif süreçleri (process) tespit edebiliyor mu?		O
TOGFT_ISTAM_2	WMI Taraması ile WMI Events üzerinden sağlanan kalıcılık ve enfeksiyonları (WMI Persistence) tespit edebiliyor mu?		O
TOGFT_ISTAM_3	Aktif processlerin (süreçlerin) listesini alabiliyor mu?	Z	
TOGFT_ISTAM_4	Aktif processlerin (süreçlerin) makine öğrenimi ile güven skorlamasını yapabiliyor mu?	Z	
TOGFT_ISTAM_5	Aktif processlerin (süreçlerin) bulut istihbaratı ile güven skorlamasını yapabiliyor mu?	Z	
TOGFT_ISTAM_6	Aktif processlerin (süreçlerin) kod imzası ve güvenilirliğini gösterebiliyor mu?	Z	
TOGFT_ISTAM_7	Aktif processlerin (süreçlerin) uzaktan dosyasını ve hafıza dökümünü alabiliyor mu?	Z	
TOGFT_ISTAM_8	Aktif processlerin (süreçlerin) uzaktan bloklanmasını veya öldürülmesini sağlayabiliyor mu?	Z	
TOGFT_ISTAM_9	Aktif süreçler üzerinde hash bilgilerine göre arama gerçekleştirilebiliyor mu?	Z	
TOGFT_ISTAM_10	Aktif süreçler üzerinde süreç ismine (process name) göre arama gerçekleştirilebiliyor mu?	Z	
TOGFT_ISTAM_11	Disk üzerinde dosya adına ve hash bilgisine göre arama gerçekleştirebiliyor mu?	Z	
TOGFT_ISTAM_12	Registry üzerinde verilen değerleri (key vb.) arayabiliyor mu?	Z	
TOGFT_ISTAM_13	İşletim sistemi yeniden başladığında aktif olacak uygulamaları listesini alabiliyor mu? (Auto-run Persistence)	Z	
TOGFT_ISTAM_14	Sistemler üzerinde aktif mutex eventlerini ve objelerini arabiliyor mu?	Z	
TOGFT_ISTAM_15	Sistem üzerinde yüklü olan sürücülerin listesini uzaktan alabiliyor mu?	Z	
TOGFT_ISTAM_16	Sistem üzerindeki aktif TCP ve UDP bağlantılarını listeleyebiliyor mu?	Z	
TOGFT_ISTAM_17	Powershell geçmişini görüntüleyebiliyor mu?	Z	
TOGFT_ISTAM_18	Sistemde yüklü sürücü (driverlerin) listesini alabiliyor mu?	Z	
TOGFT_ISTAM_19	Sistemde yüklü uygulamaların listesini alabiliyor mu?	Z	
TOGFT_ISTAM_20	Sistemlerde verilen hash veya dosya isimleri aratılabiliyor mu?	Z	
TOGFT_ISTAM_21	Sistemlerden uzaktan PCAP network kaydı alınabiliyor mu?	Z	

TOGFT_ISTAM_22	IOC entegrasyonu veya IOC ile tarama gibi özellikler mevcut mu? (IOC tarama ve entegrasyonları farklılık gösterebilir. Ürüne göre desteklediği IOC formatları değişkenlik gösterebilir. Hash, dosya ismi, yara kuralı , open ioc vb. göstergeler IOC kabul edilebilir.)		O
TOGFT_ISTAM_23	Sistemlerde planlanmış görevler (scheduled tasks) alınabiliyor mu?	Z	
TOGFT_ISTAM_24	Sistemlerin ağ erişimlerini kapatılabiliyor mu? (Network İzolasyonu)	Z	
TOGFT_PT	**Performans Testleri**	Z	
TOGFT_PT_1	Ürüne ilişkin aşağıdaki testler yapılarak performans raporu alınmalıdır.	Z	
TOGFT_PT_2	Dosya kopyalama testi	Z	
TOGFT_PT_3	Arşivleme ve Arşivden çıkarma testi	Z	
TOGFT_PT_4	Uygulama yükleme ve kaldırma testi	Z	
TOGFT_PT_5	Uygulama başlatma testi	Z	
TOGFT_PT_6	Web erişimi testi	Z	
TOGFT_PT_7	Tarama sırasında veya uygulama yüklü olduğu durumlarda kaynak tüketimi	Z	
YPGFT	**2- Yönetim Paneli Güvenlik ve Fonksiyon Testleri**		
YPGFT_GT	**1. Güvenlik Testleri**	Z	
YPGFT_GT_WTYP	**1.1. Web Tabanlı Yönetim Paneli**	Z	
YPGFT_GT_WTYP_1	Oturum yönetiminde yetkilendirme kontrolü yapılıyor mu?	Z	
YPGFT_GT_WTYP_2	SQL Injection'a karşı güvende mi?	Z	
YPGFT_GT_WTYP_3	LDAP Injection'a karşı güvende mi?	Z	
YPGFT_GT_WTYP_4	Cross-Site Scripting'a karşı güvende mi?	Z	
YPGFT_GT_WTYP_5	Cross-Site Request Forgery'a karşı güvende mi?	Z	
YPGFT_GT_MTYP	**1.2. Masaüstü Tabanlı Yönetim Paneli**	Z	
YPGFT_GT_MTYP_1	Yönetim paneli eğer masaüstü uygulaması ise bireysel uygulama için gereken kontrolleri sağlıyor mu?	Z	
YPGFT_GT_YPHY	**1.3 Yönetim Paneli Hata Yönetimi**	Z	
YPGFT_GT_YPHY_1	Ürünün hata yönetimi/denetimi günlüklemeleri/loglamaları yapılıyor mu?	Z	
YPGFT_FT	**2. Fonksiyon Testleri**		O
YPGFT_FT_R	**2.1 Raporlama**		O
YPGFT_FT_R_1	Olayları raporlayabiliyor mu?	Z	
YPGFT_FT_R_2	Raporlar çeşitli zaman aralıklarına göre düzenlenebiliyor mu?	Z	

YPGFT_FT_R_3	Raporlar dosya olarak çıkartılabiliyor mu?	Z	
YPGFT_FT_R_4	Oluşturulan raporlar e-posta olarak gönderilebiliyor mu?	Z	
YPGFT_FT_Y	**2.2 Yedekleme**		O
YPGFT_FT_Y_1	Ürünün veri tabanı yedeklemesi yapılabiliyor mu?	Z	
YPGFT_FT_G	**2.3 Güncellemeler**		O
YPGFT_FT_G_1	Ürün versiyon güncellemeleri kontrol merkezinden dağıtılabiliyor mu?	Z	
YPGFT_FT_G_2	Çevrimdışı ortamlarda güncelleme desteği devam ediyor mu?	Z	
YPGFT_FT_AO	**2.4 Ağ Ortamları**		O
YPGFT_FT_AO_1	Kontrol merkezi internetten bağımsız olarak çevrimdışı ortamda hizmet sağlayabiliyor mu?	Z	
YPGFT_FT_YD	**2.5 Yük Dengeleme**		O
YPGFT_FT_YD_1	Yönetim merkezi ulaşılmaması durumunda eş zamanlı hizmet veren yedek yönetim merkezi sunucusu var mı?	Z	
YPGFT_FT_YD_2	Yedek yönetim merkezi sunucusu yönetim merkezinin bütün görevini yerine getirebiliyor mu?	Z	
YPGFT_FT_IS	**2.6 İşletim Sistemleri**		O
YPGFT_FT_IS_1	Yönetim panelinin Windows veya Linux desteği var mı?	Z	
YPGFT_FT_T	**2.7 Tarayıcılar**		O
YPGFT_FT_T_1	Güncel Microsoft tabanlı tarayıcı desteği var mı?	Z	
YPGFT_FT_T_2	Güncel Mozilla Firefox desteği var mı?	Z	
YPGFT_FT_T_3	Güncel Google Chrome desteği var mı?	Z	
YPGFT_FT_ADE	**2.8 Aktif Dizin Entegrasyonu**		O
YPGFT_FT_ADE_1	Merkezi yönetim konsolu AD bağlantısını sağlıyor mu?	Z	
YPGFT_FT_SE	**2.9 SIEM Entegrasyonu**		O
YPGFT_FT_SE_1	SIEM, Sylog gibi log toplama ve korelasyon sistemleri ile entegre olabiliyor mu?	Z	
YPGFT_FT_KBY	**2.10 Kural Bazlı Yönetim**		O
YPGFT_FT_KBY_1	Kurulan uygulamaların kural tabanları tek merkezden kontrol edilebiliyor mu?	Z	
YPGFT_FT_KBY_2	Gruplara atanan kurallar sonradan eklenen cihazlara uygulanabiliyor mu?	Z	
YPGFT_FT_KBY_3	Dinamik gruplara atanan kurallar her eklenen cihazı etkiliyor mu?	Z	
YPGFT_FT_KBY_4	Tarama planlaması, cihaz kontrolü, zararlı yazılım engellemesi ve istisnai tanımlamalar, blacklist/whitelist yapılabiliyor mu?	Z	
YPGFT_FT_UNGA	**2.11 Uç Nokta Görev Atama**		O

YPGFT_FT_UNGA_1	Görev ile ajan kaldırılabiliyor mu?	Z	
YPGFT_FT_UNGA_2	Görev ile yeniden başlatma veya kapatma işlevleri uygulanabiliyor mu?	Z	
YPGFT_FT_UNGA_3	Görev ile tarama başlatılabiliyor mu?	Z	
YPGFT_FT_UNGA_4	Görev ile kural atanabiliyor mu?	Z	
YPGFT_FT_UNGA_5	Görevler zamanlanmış bir şekilde atanabiliyor mu?	Z	
YPGFT_FT_Y	**2.12 Yetkilendirme**		O
YPGFT_FT_Y_1	Yönetici, raporlama yöneticisi, vb. yetki sınıflarına ayrılmış roller var mı?	Z	
YPGFT_FT_Y_2	Roller kapsamı dışında özelleştirilebiliyor mu?	Z	
YPGFT_FT_DK	**2.13 Denetim Kayıtları**		O
YPGFT_FT_DK_1	Oturum açma kapama kayıtları tutuluyor mu?	Z	
YPGFT_FT_DK_2	Kullanıcı yetki kayıtları tutuluyor mu?	Z	
YPGFT_FT_DK_3	Kural değişikliği, silme, atama kayıtları tutuluyor mu?	Z	
YPGFT_FT_DK_4	Uç nokta üzerinde yapılan değişiklik kayıtları tutuluyor mu?	Z	
YPGFT_FT_BU	**2.14 Bilgilendirme ve Uyarılar**		O
YPGFT_FT_BU_1	Ürün versiyon güncelleme bildirimleri gönderiliyor mu?	Z	
YPGFT_FT_BU_2	İmza veri tabanı versiyon kontrolleri yapılabiliyor mu?	Z	
YPGFT_FT_BU_3	Lisans kullanım süresi takip edilebiliyor mu?	Z	
YPGFT_FT_BU_4	Zararlı yazılım tespiti bildirimleri gönderiliyor mu veya kontrolleri yapılabiliyor mu?	Z	
YPGFT_FT_BU_5	Sürüm notları paylaşılıyor mu?	Z	
YPGFT_FT_L	**2.15 Lisanslama**		O
YPGFT_FT_L_1	Müşteri ihtiyaçlarına göre esnek mi?	Z	
YPGFT_FT_L_2	Çevrimiçi ve Çevrimdışı ortamlarda çalışabiliyor mu?	Z	
YPGFT_FT_A	**2.16 Ayarlar**		O
YPGFT_FT_A_1	Erişim adres bilgisi görüntülenebiliyor mu?	Z	
YPGFT_FT_A_2	Proxy ayarları var mı?	Z	
YPGFT_FT_A_3	E-posta hizmeti ayarları var mı?	Z	
YPGFT_FT_A_4	Lisans ile ilgili ayarlar var mı?	Z	
YPGFT_FT_UD	**Ürün Dökümantasyonu**		O

YPGFT_FT_UD_1	Ürün dökümantasyonu için Türkçe ve İngilizce dil desteği var mı? Diğer diller açıklama kısmına yazılmalı.		O
YPGFT_FT_UD_2	Hızlı kurulum, ürün özellikleri gösteren elektronik özet kitapçık ve yönetici el kitabı var mı?		O
YPGFT_FT_UD_3	Üreticinin ürüne ilişkin bilgi deposu ve çağrı sistemi v.b. web sayfaları var mı?		O