TRtest
Test ve Değerlendirme A.Ş.

# CTI - SİBER TEHDİT İSTİHBARATI 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 | Web Arayüzü bulunuyor mu? | C | | |
| UG_YA_WA_2 | Son Kullanıcının erişebileceği bir arayüz bulunuyor mu? | C | | |
| UG_YA_WA_3 | Arayüzde geçmişe ait sorgular yapılabiliyor mu? | C | | |
| UG_YA_WA_4 | Arama kriterleri saklanabiliyor mu? | C | | |
| UG_YA_WA_5 | Anahtar kelime ile arama yapılabiliyor mu? | C | | |
| UG_YA_WA_6 | Dashboard arayüzüne herhangi bir program/kurulum ihtiyacı olmaksızın web browser vb toollar ile erişilebiliyor mu? | C | | |
| UG_YA_WA_7 | Dashboard ekranında istihbaratlarla alakalı istatistiksel veri paylaşılıyor mu? | C | | |
| UG_YA_WA_8 | Zararlı girdi kontrolü yapılıyor mu? | C | | |
| UG_YA_WA_9 | Çıktı Kodlama yapılıyor mu? (Output encoding) | C | | |
| UG_YA_WA_10 | Kimlik Doğrulama kontrolü yapılıyor mu? | C | | |
| UG_YA_WA_11 | MultiFactor Authentication desteği var mı? | | B | |
| UG_YA_WA_12 | Karmaşıklık, Max uzunluk ve son kullanma süre periyodunun belirlenebileceği bir parola yönetim arayüzü var mı? | | B | |
| UG_YA_WA_13 | Kullanıcı erişim yönetimi ve yetkilendirme yapılıyor mu? | C | | |
| UG_YA_WA_14 | Kriptografi uygulamalarında zayıflığı bilinen algoritma kullanılmadığı teyit edildi mi? | C | | |
| UG_YA_WA_15 | Güvenli iletişim kanalları destekleniyor mu? | C | | |
| UG_YA_WA_16 | Veri tabanında hassas verilerin güvenliği sağlanıyor mu? | | B | |
| UG_YA_WA_17 | Oturum yönetiminde yetki kontrolü yapılıyor mu? | C | | |
| UG_YA_WA_18 | Genel kod (API) uygulamalarında güvenli girdi çıktı kontrolü yapılıyor mu? | 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** | Kullanıcı erişim yönetimi ve yetkilendirme yapılıyor mu? | C | | |
| **UG_YA_D_5** | Güvenli iletişim kanalları destekleniyor mu? | C | | |
| **UG_YA_D_6** | Sistem yapılandırması doğru, güncel ve güvenli mi? | C | | |
| **UG_YA_D_7** | Oturum yönetiminde yetki kontrolü yapılıyor mu? | C | | |
| **UG_ISS** | **İşletim Sistemi ve Servisler** (On-Premise Çözüm Mevcutsa) | | | |
| **UG_ISS_1** | Önyüz sunucuları için bilinen zayıflıklara karşı güvenlik önlemleri var mı? | C | | |
| **UG_ISS_2** | Kimlik Doğrulama kontrolü yapılıyor mu? | C | | |
| **UG_ISS_3** | Parola yönetimi güvenliği sağlanıyor mu? | C | | |
| **UG_ISS_4** | Sistem yapılandırması doğru, güncel ve güvenli mi?<br>(Uzaktan karakutu olacak şekilde) | C | | |
| **UG_ISS_5** | Yetki kontrolü yapılıyor mu? | C | | |
| **GFT** | **2- Güvenlik Fonksiyon Testi** (Bu bölümün altında bulunan kırmızı başlıklardaki fonksiyonları sağladığını iddia eden üreticiler, kırmızı başlıkların altında belirtilmiş olan kriterleri sağlamalıdır.) | | | |
| **GFT_OT** | **Oltalama Tespiti** | | | |
| **GFT_OT_1** | Temel Özelliklerde belirtilen oltalama tespitini ilgilendiren kriterler çerçevesinde oltalama tespiti yapabiliyor mu? | C | | |
| **GFT_OT_2** | Oltalama Tespiti için kendine ait risk metodolijileri var mı? | | | A |
| **GFT_ZO** | **Zaafiyet Önceliklendirme** | | | |
| **GFT_ZO_1** | Temel Özelliklerde belirtilen zafiyetleri ilgilendiren kriterler çerçevesinde zaafiyet önceliklendirme yapabiliyor mu? | C | | |
| **GFT_ZO_2** | CVSS e göre önceliklendirme yapılıyor mu? | C | | |
| **GFT_ZO_3** | Kurum varlık envanteri ile entegrasyonu var mı? | | B | |
| **GFT_ZO_4** | Çözüm önerisi sunuyor mu? | | B | |
| **GFT_SMI** | **Sosyal Medya İzleme** | | | |
| **GFT_SMI_1** | Markaya ilişkin kötü propaganda takibi, tespiti yapılabiliyor mu? | C | | |
| **GFT_SMI_2** | Markaya ilişkin saldırı hazırlığının tespiti yapılabiliyor mu? | C | | |
| **GFT_DWI** | **Deep / Dark Web İzleme** | | | |
| **GFT_DWI_1** | Markaya ilişkin kötü propaganda takibi, tespiti yapılabiliyor mu? | C | | |
| **GFT_DWI_2** | Markaya ilişkin saldırı hazırlığının takibi yapılabiliyor mu? | | B | |
| **GFT_DWI_3** | Markaya ilişkin veri sızıntısını tespit edilebiliyor mu? | C | | |
| **GFT_MI** | **Marka İzleme** | | | |
| **GFT_MI_1** | Markaya ilişkin kötü propoganda takibi, tespiti yapılabiliyor mu? | C | | |
| **GFT_MI_2** | Sahte alan adı kapatma hizmeti veriliyor mu? | | | A |
| **GFT_MI_3** | Markaya ilişkin saldırı hazırlığının takibi yapılabiliyor mu? | C | | |

| | | | | |
|---|---|---|---|---|
| GFT_MI_4 | Markaları taklit eden sahte alan adları takibi yapılabiliyor mu? | C | | |
| GFT_MI_5 | Sahte sosyal medya hesaplarının kapatılması ve sahte mobil hesapların kaldırılması yapılabiliyor mu? | | B | |
| GFT_DI | **Dolandırıcılık (Fraud) İzleme** | | | |
| GFT_DI_1 | Kredi Kartı takibi ve tespiti yapılabiliyor mu? | C | | |
| GFT_DI_2 | Kredi Kartı bilgisi çalmaya yönelik oltalama sitelerin takibi yapılıyor mu? | C | | |
| GFT_DI_3 | Sosyal medya üzerindeki oltalama reklamlarının anahtar kelime (keyword) ve görsel bazlı taramaları gerçekleştirilerek takibi ve tespiti yapılabiliyor mu? | | | A |
| GFT_DI_4 | Kötücül alan adına ait SSL sertifika kontrol ediliyor mu? | C | | |
| GFT_DI_5 | Who is ve IP bilgileri sorgulanabiliyor mu? | C | | |
| GFT_DI_6 | Sahte mobil uygulama tespiti yapılabiliyor mu? | C | | |
| GFT_DI_7 | Zararlı alan adı tespitinde International Domain Name (IDN) desteği sağlıyor mu? | | B | |
| GFT_TI | **TI Paylaşım Platformu** | | | |
| GFT_TI_1 | Farklı Tehdit İstihbarat üreten ve paylaşan platformla veri paylaşımı yapabiliyor mu? | C | | |
| GFT_TA | **Tehdit Aktörü Takibi** | | | |
| GFT_TA_1 | Tehdit Aktörlerinin TTP, Kampanya, Indicator analizini yapabiliyor ve raporlayabiliyor mu? | | | A |
| GFT_CTI | **CTI Analisti İnceleme Araçları** | | | |
| GFT_CTI_1 | CTI Analisti için inceleme ve araştırma yapabileceği araçlar mevcut mudur? | C | | |
| GFT_YZ | **Yapay Zeka** | | | |
| GFTT_YZ_1 | İki bileşenli olay analizi yapabiliyor mu? | C | | |
| GFTT_YZ_2 | İki olay arasında benzerlikleri otomatik olarak kurabiliyor mu? | C | | |
| GFTT_YZ_3 | Metadata sağlayabiliyor mu? | C | | |
| GFTT_YZ_4 | Korelasyon sağlayabiliyor mu? | C | | |
| TO | **3- Temel Özellikler** | | | |
| TO_1 | Açık kaynak istihbarat servislerinden (OSINT) tarama yapabiliyor mu? | C | | |
| TO_2 | Arayüzde anlık bilgilendirme yapılıyor mu? | C | | |
| TO_3 | Eposta veya sms ile bilgilendirme yapılıyor mu? | C | | |
| TO_4 | Sektörel ya da bölgesel bazlı takip gerçekleştirilebiliyor mu? | | B | |
| TO_5 | STIX/TAXII/API entegrasyonları var mı? | C | | |
| TO_6 | Kural ekleme, silme ve tekrarlı verilerin tekilleştirilmesi özellikleri var mı? | | B | |
| TO_7 | Diğer güvenlik ürünleri ile entegre edilebilir mi? | | B | |
| TO_8 | Geçmiş tehdit istihbaratı verileri saklanıp analiz edilebiliyor mu? | C | | |

| | | | | |
|---|---|---|---|---|
| **TO_9** | İnternet ortamına açık SSL hizmeti veren servislerin SSL sertifika durumları, bu sertifikaların zafiyet kontrolleri ve son kullanım süreleri raporlanabiliyor mu? | C | | |
| **TO_10** | Yönetim arabirimi Türkçe ve İngilizce olmak üzere en az iki dil desteğini sağlıyor mu? | C | | |
| **TO_11** | Kullanıcıların yapmış olduğu işlemler özelinde detaylı log tutabiliyor mu? (Yetkisi olmayan modüle erişim girişimi, atak denemesi, ilgili kişi ip adresi tarih ve saat vb.) | C | | |
| **TO_12** | Tehdit istihbarat verilerine ilişkin skor değeri ve raporlanma nedenini sunuyor mu? | | | A |
| **TO_13** | White list özelliği var mı? | | B | |
| **TO_14** | Oluşan false positive ve ihbarlara istinaden müşteri tarafından geri besleme mekanizması var mı? | | B | |
| **TO_15** | Parola güvenliği sağlanıyor mu? | C | | |
| **TO_16** | Yetkilendirme (authorization) mekanizması kapsamında kullanıcı ve rol bazlı yetkilendirme yapabiliyor mu? | C | | |
| **TO_17** | Aktif-Pasif yedekli çalışmayı destekliyor mu? ( On premise ürünler için gereklidir.) | | B | |
| **TO_RO** | **Raporlama Özellikleri** | | | |
| **TO_RO_1** | Raporlama format desteği bulunuyor mu? (txt, pdf, html, csv, xlsx) | C | | |
| **TO_RO_2** | Raporlama arayüzüne herhangi bir program/kurulum ihtiyacı olmaksızın web browser vb. toollar ile erişilebiliyor mu? | C | | |
| **TO_RO_3** | Raporlama arayüzünde saldırı veya malware raporları bulunuyor mu? | C | | |
| **TO_RO_4** | Raporlama arayüzünde anahtar kelime araması yapılabiliyor mu? | C | | |
| **TO_RO_5** | Arayüzden erişilen bilgiler (örnek:istihbari bilgiler) raporlanabiliyor mu? | C | | |
| **TO_RO_6** | Arayüzden erişilen bilgiler filtrelenebiliyor mu? | C | | |
| **TO_AO** | **API Özellikleri** | | | |
| **TO_AO_1** | API üzerinden paylaşılan veri formatı JSON, CSV, STIX veya OpenIOC' lerden en az birini destekliyor mu? | C | | |
| **TO_AO_2** | API üzerinden gelişmiş istek atılıyor mu?(Son 24 saatte gelen istihbaratlar, şu ID den sonra gelen istihbaratlar vs.) | C | | |
| **TO_UD** | **Ürün Dokümantasyonu** | | | |
| **TO_UD_1** | Ürün dokümantasyonu var mıdır?(Yazılı materyal veya Tool Tip vb.) | C | | |
| **RU** | **4- REGÜLASYONLARA UYUM** | | | |
| **RU_KVKK** | **KVKK** | | | |
| **RU-KVKK_1** | Ürün, Kişisel Verilerin işlenmesi ile ilgili kanun kapsamında müşterisi ile sözleşme, bilgilendirme ve onay alma sistemini destekliyor mu? | C | | |