TRtest
Test ve Değerlendirme A.Ş.

SIEM ÜRÜN GRUBU KRİTERLERİ

No	Başlık/Soru
UG	**1- Ürün Güvenliği**
UG_YA	**Yönetim Arayüzleri**
UG_YA_WA	**Arayüz Zayıflık taraması**
UG_YA_WA_1	Zararlı girdi kontrolü yapılıyor mu?
UG_YA_WA_2	Kimlik Doğrulama kontrolü yapılıyor mu?
UG_YA_WA_3	Hata yönetimi ve loglama doğru bir şekilde yapılıyor mu?
UG_YA_WA_4	Güvenli iletişim kanalları destekleniyor mu?
UG_YA_WA_5	Veri tabanında hassas veriler güvenliği sağlanıyor mu?
UG_YA_WA_6	Oturum güvenliği kontrolü yapılıyor mu?
UG_YA_WA_7	Kriptografi uygulamalarında zayıflığı bilinen protokol kullanılmadığı teyit edildi mi?
UG_YA_WA_8	Parola yönetimi güvenliği ve parola karmaşıklığı sağlanıyor mu?
GFT	**2- Güvenlik Fonksiyon Testi**
GFT_YT	**Yetkilendirme Testleri**
GFT_YT_1	Yetkilendirme (authorization) mekanizması kapsamında kullanıcı ve rol bazlı yetkilendirme yapabiliyor mu?
GFT_YT_2	Log kaynağına göre yetkilendirme (authorization) mekanizmasına sahip mi?
GFT_YT_3	Log içeriğine göre yetkilendirme (authorization) mekanizmasına sahip mi?
TO	**3- Temel Özellikler**
TO_M	**Mimari**
TO_M_1	İstenildiği ölçüde yatay ve dikey genişleyebilme özelliğine sahip mi?
TO_M_2	Veri yedekliliği (redundancy) sağlanıyor mu?
TO_M_3	İlave log toplama kaynaklarını dahil edebilecek mimariye sahip mi?
TO_M_4	EPS hesaplaması yapıyor mu?
TO_M_5	Lisans değeri aşıldıktan sonra logları işlenmeye devam edebiliyor mu?

TO_M_6	Eş zamanlı toplama, korelasyon, saklama, sorgulama vb. desteği var mı?
TO_M_7	Tehdit istihbaratı verisi entegrasyonu sağlanabiliyor mu?
TO_M_8	Ürüne ilişkin yardım menüsü veya wiki sayfaları mevcut mu?
TO_M_9	Büyük veri mimarisi destekleniyor mu?
TO_SY	**Sistem Yönetimi/ Sistem İzleme**
TO_SY_1	Ajanları uzaktan kurabilme veya etkileşimsiz kurulabilecek kurulum paketi sağlıyor mu ? Güncelleme ve yönetebilme özelliği var mı?
TO_SY_2	Sistemin yapılandırma ayarları yedeklenebiliyor mu?
TO_SY_3	Coğrafi olarak dağıtık kurulumların merkezi olarak yönetimi yapılabiliyor mu?
TO_SY_4	Loglar üzerinde varlıkları, kullanıcıları, log kaynaklarını vb. mantıksal olarak gruplayabilme, kategorize edebilme yapabiliyor mu?
TO_SY_5	Ürünün üzerinde çalıştığı sistemin Disk, RAM, CPU kullanımı istatistikleri takip ediliyor mu
TO_SY_6	Merkezi olarak uzaktan bileşen yazılım güncellemeleri (kolektörler ve ajanlar vb.) yapılabiliyor mu?
TO_SY_7	Türkçe kullanıcı arayüzü var mı?
TO_SY_8	İngilizce kullanıcı arayüzü var mı?
TO_LT	**Log Toplama**
TO_LT_1	Özel log kaynakları ve tipleri için plugin geliştirebiliyor mu?
TO_LT_2	Diğer SIEM ürünlerinden dışa aktarılan loglar (CEF veya Json) içe aktarılabiliyor mu?
TO_LT_3	İşlenmiş loglarla birlikte ham loglar da saklanıyor mu?
TO_LT_4	Ajan vasıtasıyla log alınması durumunda ajan üzerinden istenen logların filtrelenerek gönderilmesi sağlanabiliyor mu?
TO_LT_5	Zafiyet araçları ile entegrasyon sağlanabiliyor mu? (Örnek UNITMON Acunetix Tenable Security Center Continuous View NetSparker vb)
TO_LT_6	Belirlenen zamanlarda toplayıcıdan yığın veri toplama yeteneği mevcut mu?
TO_LT_7	Log toparlama (aggregation) özelliği var mı?
TO_LT_8	Ajanlı ve ajansız log toplama yöntemleri (En az aşağıdakiler) destekleniyor mu? Syslog (TCP, UDP) OPSEC WMI SNMP Trap SMB FTP SSH Formatlı/ Düz Metin Dosyalarının Aktarımı RDBMS)

TO_LT_9	Log toplama yöntemi ve ortamında oluşacak hatalar dışında log kaynağında üretilen log sayısı ile SIEM tarafından toplanan logların sayısı aynı olmalıdır?
TO_LT_10	Log alınamadığı durumda alarm üretilebiliyor mu?
TO_LIN	**Log işleme ve Normalizasyon**
TO_LIN_1	Toplanan ham kayıtların; * Normalize edilmesi, * Sınıflandırılması, * Gerekiyorsa filtrelenebilmesi, * Önceliklendirilmesi, * Korelasyona Tabi Tutulması, Yapılabiliyor mu?
TO_LIN_2	Sınıflandırma tanımları güncellenebiliyor mu?
TO_KOR	**Korelasyon**
TO_KOR_1	Log kaynakları genelinde olayların gerçek zamanlı veya gerçek zamana yakın korele edilmesi gerçekleştiriliyor mu?
TO_KOR_2	Olay puanlama, derecelendirme için destek sağlanıyor mu?
TO_KOR_3	Geçmişe yönelik kayıtlar aracılığı ile korelasyon yapılabilme yeteneği var mı?
TO_KOR_4	Basit ve birleşik (zincir) kural tanımlayabilme yeteneği var mı?
TO_KOR_5	Düz metin (txt), csv ve Json tabanlı dosyaların girdi olarak alınabilmesi ve bu dosyalarda yer alan listelenmiş (look-up) tablolardan korelasyon kurallarında faydalanabilme yeteneği var mı?
TO_KOR_6	Kural ve betik tabanlı korelasyon yapabilme yeteneği var mı?
TO_KOR_7	Korelasyon sonucunda betik çalıştırma yeteneği var mı?
TO_KOR_8	Korelasyon çıktısı başka bir kuralı tetikleyebiliyor mu?
TO_KOR_9	Korelasyon sonucunda ayrıştırılan alanlardan seçilenleri, belirlenmiş aktif listeye ekleme özelliğine sahip mi?
TO_KOR_10	Kurallarda tehdit istihbaratı bilgileri kullanılabiliyor mu? (gelen olayları toplanan tehdit istihbaratı verisi ile eşleştirme, "kara liste" IP'leri, domainler vb.
TO_KOR_11	SOAR ürünü ile uyumlu çalışabiliyor mu?
TO_AOY	**Alarm ve Olay Yönetim**
TO_AOY_1	Uyarıların, alarmların (PDF, XLSX, DOCX, CSV, HTML - en az birinde) formatlarında dışarıya aktarabiliyor mu?
TO_AOY_2	Korelasyon sonucunda üretilen alarmları e-posta ve SMS ile sistem yöneticisine iletebiliyor mu?
TO_AOY_3	Log alma durumu anlık olarak grafik arayüz üzerinden gösterilebiliyor mu?
TO_AOY_4	Korelasyon sonucunda oluşan uyarıları özelleştirilebiliyor mu?
TO_AOY_5	Korelasyon sonucunda oluşan uyarıların kullanıcı veya grup özelinde iletme yeteneği var mı?

TO_AOY_6	SIEM'de oluşan uyarılar içerisinde arama yapılabiliyor mu?
TO_SR	**Sorgulama ve Raporlama**
TO_SR_1	Raporlama modülü bünyesinde ön tanımlı raporlar bulunuyor mu?
TO_SR_2	Tüm verilerin tüm alanları genelinde özel amaçlı, anahtar kelime araması yapılabiliyor mu?
TO_SR_3	İstatistiksel fonksiyonlar kullanılabiliyor mu?
TO_SR_4	Analiz ve sorgulama modülü ile loglar üzerinden istenilen sorguların, ayrıştırılan (normalize) veya orijinal (ham) log satırı üzerinde yapılabiliyor mu?
TO_SR_5	Sorgularda istenildiği kadar filtre (zaman aralığı, alan başlıkları, =,>,<,>=,<=) tanımlanabiliyor mu?
TO_SR_6	Yapılan sorguların sonuçlarını (pdf, docx, xlsx csv, html - en az birinde) formatında dışarı aktarılabiliyor mu?
TO_SR_7	Log kaynağı ve sınıflandırma bazlı raporları alınabiliyor mu?
TO_SR_8	Raporların görsel olarak tasarlanabilmesi ve kurumsal formata uydurulabilmesi için bir taslak düzenleyicisi var mı?
TO_SR_9	Raporlar periyodik çalıştırılabiliyor mu?
TO_SR_10	Raporları saklayabilme ve arşivleyebilme yeteneği var mı?
TO_SR_11	Gerçek zamanlı periyodik ve özelleştirilebilir kontrol panellerine sahip mi?
TO_G	**Güvenlik**
TO_G_1	Olay kaydı (audit log) tutma mekanizması var mı?
TO_G_2	Toplanan log kayıtlarının belirli zaman aralıklarında bütünlüğü ve inkar edilmezliği sağlanıyor mu?
TO_G_3	Endüstri tarafından kabul edilen standart bir Hash (özet) fonksiyon desteği var mı?
TO_VM	**Varlık Modeli**
TO_VM_1	Otomatik olarak ya da manuel olarak Varlık bilgilerinin oluşturulabilme yeteneği var mı?
TO_AS	**Arşivleme ve Sıkıştırma**
TO_AS_1	Log verilerinin saklama politikaları uygulanabiliyor mu? (Log Kaynağı, Log Türü, Zaman vb - En az birinde)
TO_AS_2	Toplanan loglar sıkıştırılarak saklanabiliyor mu?
TO_AS_3	Arşivleme ve sıkıştırma işlevlerinin çalışacağı saatler ve süre seçilebiliyor mu?
TO_AS_4	Farklı depolama alanlarına arşivleme yapılabiliyor mu?
PK	**4. Performans / Kapasite**
PK_1	Ürün üretici tarafından beyan edilen performans kriterlerini sağlıyor mu?

PK_2	Üretici tarafından test ortamı ve test edilecek ürünün modeli belirtilmiş mi?
PK_3	Veri üzerinde sorgu süreleri;
PK_4	Korelasyon performansının ölçülmesi; (Basit Korelasyon, 3 Kademeli Zincir Korelasyon)
PK_5	Rapor performansının ölçülmesi;
PK_6	Log işleme performansının ölçülmesi;