



UNITMON

UNIFIED IT MONITORING

- Web Tabanlı Ağ Güvenlik İzleme Aracı
- Zafiyet Yönetim Sistemi
- Siber Tehdit İstihbaratı
- Tümleşik BT Kontrolü
- Sunucu ve Uygulamaların Sürekli Takibi



UNITMON NEDİR ?

Güvenlik zafiyetlerinin tespiti, tehditlerle karşı karşıya olan her kuruluştaki BT sisteminin güvenliğinin etkin bir şekilde idamesinde en kritik rolü oynamaktadır. UNITMON, web tabanlı bir izleme aracı olup size sadece web sitenizin anında denetlemesi imkanını vermekle kalmayarak ağ zafiyetlerinizi araştırma ve bir arayüz üzerinden ağ bileşenlerinizin performansını kontrol etme olanaklarını da sağlar. Web içeriklerinizin, DNS ve IP sunucunuzun güvenliği hakkında istihbarat sağlayarak bakım maliyetlerini ve BT altyapısının kilit noktalarında kritik arıza risklerini de asgariye indirir.

Zafiyet izleme ve analiz özelliği, ağ cihazları, sunucular ve uygulamalarda zafiyetlerin taranması planlanabilmektedir. Zafiyetleri gidermek için çözümler sunan özelleştirilebilir değerlendirme raporları oluşturulabilmektedir. 10'dan fazla tarama aracı entegrasyonu sayesinde konsolide önleyici güvenlik çözümü sunmaktadır.

DNS zehirlenmesine karşı sürekli olarak DNS sorguları yaparak herhangi bir zehirlenme durumunda anında uyarı üretebilir.

Ortalama saldırılarına karşı sürekli olarak güncellenen domain veritabanından sorgular yaparak kurum domain adına benzer bir isimle domain alındığında uyarı üreterek, daha saldırı hazırlığı aşamasında önlem alabilmeyi sağlar.

UNITMON'un Siber İstihbarat Servisleri izleme özelliği; kurum IP lerinin, alan adlarının, kimliklerinin herhangi bir kara listeye girip girmediğini kontrol eder. Bu da kurum içerisinde ya da dışında kurum IP'leri ile herhangi bir illegal aktivite olup olmadığını gösterir.

TEMEL ÖZELLİKLER

- Yönetici Göstergeleri
- HTTP/S, SOAP, Web Servis İzleme
- Web Uygulama Takibi
- Sunucu Performans İzleme
- Website / Sunucu Güvenlik Açıklıkları Takibi
- SMS, E-Posta SNMP ile Bilgilendirme
- Dağıtık, Ölçeklenebilir Mimari
- Lokasyon Bazlı Kontroller
- Siber İstihbarat Servis Kontrolleri
- Ortalama Alanadı Kontrolleri
- Otomatize Zafiyet Tarama Planları
- Sızdırılmış Veri Analizi
- Paste Site Kontrolleri
- Sosyal Medya Takibi



TÜMLEŞİK İZLEME (UNIFIED IT MONITORING)

ERİŞİLEBİLİRLİK VE PERFORMANS İZLEME

UNITMON, yöneticilerin BT altyapısı üzerindeki neredeyse tüm ağ cihazlarını kullanımı kolay bir web tabanlı panel üzerinden izlemelerine, performanslarını ileri grafiklerle görselleştirmelerine imkan verir. Bulutta çalışan bu hızlı ve sezgisel arayüz ağ cihazlarınızın performansının sağlıklı olmasını temin etmekle kalmayarak etkin kaynak kullanımı ve maliyet ve risk minimizasyonunun sağlıklı işlemlerini sağlar.

UNITMON, CPU / RAM / DİSK kullanımını, eşik değeri aşma durumlarını ve performansını izler. TCP/UDP protokollerini, **SMTP, POP3, IMAP, HTTP(S), SSL, FTP, SSH, DNS, SNMP** ve bant genişliğini kontrol eder. Yine Form tabanlı kullanıcı girişi, HTTP veya JavaScript yeniden yönlendirmelerini izler. Form Post verilerini ve HTTP başlıklarını kaydederek işlem kayıt imkanı sağlar.

SİBER TEHDİT İZLEME

UNITMON, internet üzerinde oluşabilecek tehditlere karşı gerekli izlemeleri de yapmaktadır.

Sızdırılmış Veri Analizi ile bilinen hack olayları sonrasında yayımlanan veritabanlarında/dosyalarda kurumun belirlemiş olduğu; IP/domain, e-mail, kullanıcı adı, kredi kartı, kimlik numarası, anahtar kelimeler izlenmektedir.

Paste Siteleri İzleme ile **pastebin, github, pastie, nopaste, codepad, slexy** gibi birçok site üzerinden anlık olarak yapılan takiple kurumlar ile ilgili olabilecek herhangi bir veri sızıntısı anında tespit edilmektedir. Bunların yanı sıra sızdırılmış veri analizinde olduğu gibi IP/domain, e-mail, kullanıcı adı, kredi kartı, kimlik numarası, anahtar kelimeler de izlenmektedir.

Sosyal Media İzleme ile sürekli takip edilen sosyal medya sayfalarında (twitter, facebook, google+, github, reddit vs) meydana gelebilecek değişiklikler, takip edilen anahtar kelimeler ile olası bir veri sızıntısı tespit edilmeye çalışılır.

RAPORLAMA, UYARI VE BİLGİLENDİRMELER

Sunucuların ve web sayfalarının elverişlilik ve performansına ait geçmiş kayıtları, kusurların tespiti ve verim planlamasında önemli bir rol oynar. Bilgilendirme ve uyarılar, kullanıcıların tercihinine göre e-posta, SMS veya özel kodlarla gönderilebilir. UNITMON, güvenlik ve kontrolü amaçlayan BT yöneticilerinin tüm ihtiyaçlarının karşılanmasına yönelik geniş raporlama özelliklerine sahiptir.

OTOMATİK ZAFİYET TARAMA

UNITMON, ağınız içindeki sunucu, uygulama ve cihazlarınızın bilinen güvenlik açıklıklarını bilinen tarama araçları ile otomatik olarak tarayabilmektedir. **Nessus, Nexpose, Acunetix, Netsparker, OpenVas, W3af, Arachni, OWASP ZAP** tarama araçlarını API üzerinden yönetim veya sonuçlarını aktarma imkanı sağlar. Varlığın geçmişe yönelik zafiyet analizini takip edebilir, uyumluluk raporlarınızı çıkarabilirsiniz. Ağ, web, veritabanına özel politikalar ile periyodik planlar çıkarabilirsiniz. UNITMON tüm bu tarama araçlarını ana bir çatı altında toplar, CVE referanslarını ve çözüm önerilerini sunar.

İÇERİK İZLEME YÖNETİMİ

İçerik kontrol özelliği, web sitelerinin hacklemeye açık olan saldırı yüzey alanlarını izler. İçerik ve resimler dakikada bir kontrol edilerek herhangi değişiklik halinde uyarılar göndererek itibar kaybını asgariye indirir. Buna ilave olarak, hack-raporlama sitelerinin kayıtlarını kontrol ederek marka / hizmet itibarını korur.

UNITMON, karmaşık kalıp eşleşmelerini oluşturmak üzere düzenli ifadelerin kullanımını kolaylaştırarak sitenizin tüm özellik ve anahtar kelimelerini kontrol eder. Tüm içerik (resimler dahil) referanslar kullanılarak kontrol edilir. UNITMON, çevrimiçi alışveriş sepeti ve interaktif bankacılık gibi çoklu web işlemlerini de içerir. Uygulamalarda oluşabilecek bağlantı sorunlarını, içerik değişikliklerini veya sayfa yüklemeye kapanmayı tespit edebilir.

SİSTEM GEREKSİNİMLERİ

Sanal Makineler:

VMware Player, Workstation; VMware Server, ESX; Microsoft HyperV

İşletim Sistemi:

Windows 7,8,10, Windows Server 2008 R2, Windows Server 2012 R2 , Windows Server 2016

Donanım:

2 GHz CPU (4 Core), 8+ GB RAM, 120+ GB Disk Alanı

