ÖLÇSAN 50
to measure is to know
50 years in the industry

T-STRAINER

SALDIRI TESPİT ve ÖNLEME SİSTEMİ (IDPS)

IDS*, ağ trafiğinizdeki kötü amaçlı etkinlikleri ve bağlantıları tespit etmek için kullanılan sistem adıdır. Saldırı Tespit Sistemlerinin kısaltması olarak kullanılmaktadır. IDS güvenlik sistemlerinin amacı, kötü niyetli faaliyetleri tespit etmek ve günlüğe kaydetmektir. **IPS****'ler, ağ trafiğinizdeki kötü amaçlı etkinlikleri ve bağlantıları tespit etmek ve önlemek için kullanılan güvenlik sistemleridir. Intrusion Prevention Systems kelimelerinin kısaltması olarak kullanılmaktadır. IPS sistemlerinin amacı, ağ trafiğindeki kötü amaçlı bağlantıları veya faaliyetleri engellemektir.

IDS, kötüye kullanım tespiti ve kötü niyetli etkinliklerin kontrolü için kullanılır. Kötü amaçlı faaliyetler, ağınızda oluşabilecek anormallikler (bilinen tehditler) tespit edilerek belirlenir. Ağ trafiğindeki paketler bilinen kurallara göre izlenir ve sınıflandırılır. IDS'den farklı olarak, IPS'ler kaynak ve hedef arasındaki doğrudan iletişim yoluna yerleştirilir, paketler aktif olarak analiz edilir ve izinsiz girişleri önlemek için otomatik eylemler gerçekleştirilir.

Topoloji 1

Bu modda **IDS ve IPS** beraber çalışır. Bu topoloji modeli saldırıları önlemek için kullanılır. Her ne kadar imza güncellemeleri için downtime*** süresine ihtiyaç duyulsa da **T-Strainer piyasadaki bütün rakip ürünlerden daha hızlıdır**.

Topoloji 2

Bu modda IDS tek başına çalışmaktadır. Bu konfigürasyon ile sadece tehditlerin tespiti sağlanabilir. Ağ içerisine yerleştirilmesi kolaydır ve downtime ihtiyacı yoktur.

Avantajlar & Teknik Üstünlükler

T-STRAINER daha az kaynak kullanarak kurumunuzu rakiplerine göre daha başarılı daha hızlı ve uygun maliyetle korur.

- Daha fazla protokolü ve bu protokollerin metakey bilgilerini destekler. Meta anahtar bilgilerini kullanarak daha geniş ve kapsamlı ağ güvenliği sunar.
- Kullanıcı, desteklenen metakey sayısı ile desteklenen imza kurallarının ötesine geçebilir. Kullanıcıların yeni özel kurallar oluşturmasına izin verir.
- Standart CIDSS**** imza biçimini kullanır. Bazı imza türlerinin başka sistemlere tam olarak çevrilmesi imkansızdır, ancak tüm imzalar CIDSS'ye çevrilebilir.
- Kullanıcının arayüzden kolayca yeni imzalar oluşturmasını sağlar. Oluşturulan imza kuralları otomatik olarak CIDSS formatına dönüştürülür.
- Ergonomik bir kullanıcı arayüzü ile birlikte gelir.

Kötü Amaçlı Faaliyetlerin Tespiti ve Önlenmesi

HIZLI
Tamamen ÖLÇSAN tarafından geliştirilen, gecikmesiz yüksek performanslı sistem.

VERİMLİ
Kullanıcıların saldırılara daha hızlı tepki vermesine olanak tanıyan yeni protokollere hızlı adaptasyon.

GÜVENLİ
Rakiplere göre daha hızlı ve daha derin analiz performansı. Ağ hızını yavaşlatmadan etkin çalışma.

KOLAY KULLANIM
Tamamen ÖLÇSAN tarafından geliştirilmiş, kullanıcı dostu arayüzü ile yönetimi kolay IDS/IPS.

AÇIK KAYNAK YOK
Ticari çözümlerin çoğu, kullanıcı arayüzlerini açık kaynak kütüphanesinden kullanırken T-STRAINER tamamen özgün olarak geliştirilmiştir.

+ T-STRAINER'in kendine özgü tehdit algılama yapısı oldukça hızlı ve etkilidir.

** IDS: Intrusion detection system ** IPS: Intrusion prevention system *** Downtime: Çalışan servis veya cihazların işlevlerini yerine getiremediği süredir **** CIDSS: Common Intrusion Detection Signatures Standard*

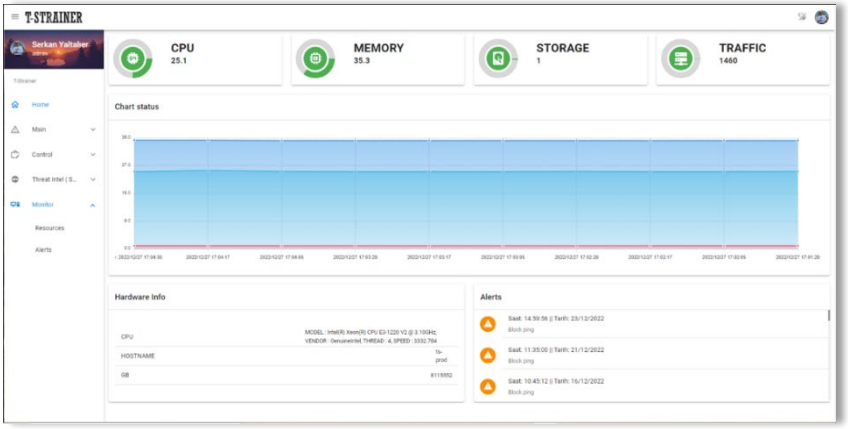
T- STRAINER Gelişmiş Özellikleri

Yüksek Kullanılabilirlik → Koruma altyapısının tamamını redundant* olarak çalıştırır.
SOC Entegrasyon → SOC/NOC sistemleri için çoklu entegrasyon olanakları sunar.
IP İtibarı → En güncel ve yanlış pozitiflerin hariç tutulduğu IP güvenli listeleri sağlar.
Optimize Edilmiş Hız → Yoğun ağlarda minimum gecikmeyle çalışacak şekilde tasarım.
Güncel İmzalar kullanır. → Bilinen tehditlere karşı güvenilir kaynaklardan en güncel imzaları
Otomatik Güncelleme → Ağ'a yönelik saldırılara karşı en güncel bilgiler ile koruma sağlar.
Metakey Bazlı Kurallar → Daha akıllı imzalar için metakey bazlı imza altyapısı sağlar.
Çoklu Kullanım → Çoklu çekirdek kullanımıyla yüksek performans ve verim sağlar

- IPS koruması kapsamında, HTTP, HTTPS, SMTP, DNS, POP ve IMAP gibi iyi bilinen protokollerinde kontrollerini yapar.
- Ticari ve açık kaynaklı ürünlerde hem trafiği yavaşlatmamak hem de paket kaybını önlemek için, donanım olarak pahalı işlemciler, hızlandırıcılar ve bellekler kullanılmak zorundayken T-STRAINER'de gerekli ve zorunlu değildir.

T-STRAINER, çoklu çekirdek kullanarak yüksek performans ve verimliliğe ulaşır. Donanım özelliklerine göre thread** sayısı belirlenebilir. 60.000 flow*** ile 60 thread için 120 Gbps canlı ağ trafik hızına paket kaybı olmadan ulaşılabilir.

T-STRAINER, ağınızı kötü amaçlı paketlerden korur ve güvenlik duvarı cihazlarınıza temiz bir trafik akışı sağlar.



Neden T-STRAINER daha gelişmiş?

- T-STRAINER'ı destekleyen Ağ ve Taşıma Katmanı Protokollerinin sayısı 75'in üzerindedir.
- Desteklenen Uygulama Katmanı Protokollerinin Sayısı 35'in üzerindedir.
- Muazzam miktarda denilebilecek 15.000'den fazla Veri anahtar kelimesi içerir. (metakeys)
- İmza format XML'dir
- Performans: 4 threads ile 15 flow'da 540 Mbps

Kullanım Örnekleri

DDoS Koruması- DDoS saldırılarına karşı normal trafiği kötü amaçlı trafikten ayırarak yoğunluk altında dahi doğru kararlar verir.

Ağ Güvenliği- Gelişmiş imzalar ve davranış analizi ile doğru hatadan arındırılmış kararlar verir.

WEB Uygulama Güvenliği- Web uygulamalarının yükselişe geçtiği günümüzde bu servislerin güvenliğini en iyi şekilde takip eder ve saldırıları engeller.

Veri tabanı Güvenliği- Veri tabanı sisteminden bağımsız olarak aradaki trafiği izler ve doğru imzalar ile doğru kararlar alır.

Ağ Görünürlüğü- Giderek karmaşıklaşan ağlar ve ortamlar, belirli izleri bulmayı zorlaştırır. Bu nedenle, ağ görünürlüğünüzü artırarak kayıplar azaltılır.

Trafik Loglama- Ağınızda olup bitenlerin hem mevcut hem de geçmiş durumunu gözden geçirmeniz gerekebilir. Belirttiğiniz imzalar ile bu kayıtlar kolayca yapabilirsiniz.

Yönetim Platformu- Kullanımı kolay ve basit arayüzü ile kullanıcıya ürünü yönetmesi ve izlemesi için bir platform sağlar. Ayrıca, farklı dil seçenekleri vardır.

Hızlı ve Kolay Kurulum- Mevcut ağ yapınızı değiştirmeden IDS veya IPS modunda kolayca kurulum yapılması sağlanır.

T-STRAINER, ELK gibi 3.parti uygulamalarla entegredir. Ticari ve açık kaynak uygulamalara da kolaylıkla entegre edilmektedir.

**Redundant: Farklı cihazlarda birden fazla T-STRAINER çalıştırarak donanımsal arızalar sonucu oluşabilecek kesintiler minimuma indirilir.*
***Thread: T-STRAINER aynı cihazda bir defadan fazla çalıştırılabilir. Bu sayede birden fazla çekirdek de işlem yaparak daha fazla yarar sağlanır.*
****Flow: Belirli parametrelere bakılarak oluşturulan trafik ayrımı olarak adlandırılır. Bu yöntemle trafik kanalize edilir.*