IBM İletişim Kuralı Analiz Modülü

IBM Security İzinsiz Giriş Önleme Sistemi teknolojilerinin temelindeki koruma motoru.

Öne Çıkanlar

- Ağınızı ve ağınızdaki sunucular, masaüstleri ve ağ altyapısı gibi varlıkları etkilemeden önce tehditleri durdurur.
- Son kullanıcıları her gün kullanılan belge biçimleri, elektronik tablolar, sunumlar, çoklu ortam dosyaları ve web tarayıcıları gibi uygulamalarda gizlenen izinsiz yetki kazanma programlarına karşı korur.
- Tehditler geliştikçe yeni güvenlik teknolojilerinin ve işlevselliklerin eklenmesine olanak sağlayan modüler, genişletilebilir çerçeve.

Tehdidin bir adım önünde olmak - İnternet tehditlerinin işinizi etkilemeden durdurulması.

IBM Security İzinsiz Giriş Önleme Sistemi teknolojileri, İnternet tehditlerini işinizi etkilemeden önce durdurur. Özgün güvenlik yapımızın temelinde, IBM İletişim Kuralı Analiz Modülü (Protocol Analysis Module - PAM) adı verilen ve pek çok farklı İnternet tehdidine karşı önleyici koruma sağlayan motorumuz bulunmaktadır. PAM, IBM X-Force® araştırma ve geliştirme ekibi tarafından yıllar boyunca toplanan güvenlik bilgileri temel alınarak tasarlanmıştır. X-Force, tehditlerin ve bu tehditlerin istismar etmeye çalıştığı altta yatan yazılım güvenlik açıklarının proaktif olarak incelenmesine adanmış, tüm dünyada tanınan bir güvenlik araştırması kuruluşudur.

PAM, modüler genişletilebilir çerçevesi ile sürekli olarak karşı karşıya olduğunuz en zorlu güvenlik tehditlerini önlemek için gelişir ve ek nokta çözümleri satın alma gereksinimini ortadan kaldırır. Dünyaca ünlü IBM X-Force araştırma ve geliştirme ekibi tarafından desteklenen PAM, sizi en son tehditlerin bir adım önünde tutmak için düzenli ve otomatik olarak yeni güvenlik bilgilerini alır. Diğer çözümler sadece bağımsız koruma imzalarını izinsiz yetki kazanma programları ile eşleştirmeye çalışır. Bu süreç, gelişmekte olan tehditlerin durdurulması için çok yavaştır ve yanlış pozitiflerin ve negatiflerin oranlarının artmasına neden olur.

IBM İletişim Kuralı Analizi Modüler Teknolojisi

IBM İletişim Kuralı Analizi Modüler Teknoloji	**Ne Yapar:**
Virtual Patch	Güvenlik açıklarını bir yazılım yamasından bağımsız olarak istismara karşı korur ve yeni tehditler için yamaların test edilmesi gereksinimini ortadan kaldıran güvenliği sağlar. Kritik sistemlere yine de yama uygulanmalıdır, ancak artık yama yönetimi için kendi test edilmiş süreçlerinizi yürütebilirsiniz. Yama yönetimi süreciniz en iyi uygulamalara uygun değilse, IBM, uç noktası yönetimini ağı, sunucuları ve istemcileri kapsayan bütünsel bir güvenlik yaklaşımına bütünleştirmenize yardımcı olabilir.
İstemci Tarafı Uygulama Koruması	Microsoft Office dosyaları, Adobe PDF dosyaları, çoklu ortam dosyaları ve Web tarayıcıları gibi her gün kullanılan uygulamaları hedefleyen saldırılara karşı son kullanıcıları korur.
Web Uygulaması Koruması	Web sunucularını, SQL Injection, XSS (Siteler arası komut dosyası oluşturma), PHP dosyası ekleyicileri, CRSF (Siteler arası talep sahteciliği) gibi gelişmiş uygulama düzeyi saldırılarına karşı korur.
Tehdit Belirleme ve Önleme	Belirli bir izinsiz yetki kazanma programına veya güvenlik açığına değil, her türlü tehdit sınıfına karşı algılama ve önleme sağlar.
Veri Güvenliği	Veri bilinci için, şifrelenmemiş kişisel olarak tanımlanabilir bilgileri ve diğer gizli bilgileri izler ve tanımlar. Ayrıca, herhangi bir potansiyel riskin mevcut olup olmadığını belirlemek için ağ üzerinden veri akışını keşfetme yeteneği sağlar.
Uygulama Denetimi	ActiveX parmak izleri, Eşler Arası, Anında İleti Sistemi ve tünelden gönderme gibi ağ üzerindeki tanımlanmış segmentler içerisindeki yetkisiz uygulamaların ve risklerin denetimini yönetir.

PAM, aşağıdaki ağ tehdidi sınıflarını izleme, belirleme veya önleme becerisine sahiptir:

Tehdit Sınıfları	İzleme	Belirleme	Önleme
Uygulama Saldırıları	√	√	√
Saldırı gizleme	√	√	√
Arabellek taşması saldırıları	√	√	√
Siteler arası komut dosyası saldırıları	√	√	√
Veri sızıntısı	√	√	√
Veritabanı saldırıları	√	√	√
DoS ve DDoS saldırıları	√	√	√
Zararlı yazılımları karşıdan yükleme	√	√	√
Şirket içinden kaynaklanan tehditler	√	√	√
Anında ileti sistemi	√	√	√
Kötü niyetli belge tipleri	√	√	√
Kötü niyetli ortam dosyaları	√	√	√
İşletim sistemi saldırıları	√	√	√
Eşler arası	√	√	√
İletişim kuralı tünelleme	√	√	√
SQL injection saldırıları	√	√	√
Web tarayıcısı saldırıları	√	√	√
Web sunucusu saldırıları	√	√	√

PAM, bu saldırı sınıflarının ele alınması için eşzamanlı olarak çalışan çok sayıda izinsiz giriş önleme teknolojisi kullanır. Bunlar arasında:

- *Kapı tahsisi*
- *Kapı izleme*
- *İletişim kuralı analizi*
- *İletişim kuralı tünelleme*
- *Kalıp eşleştirme*
- *İçerik Analizi*
- *Injection Mantığı Motoru*
- *Kabuk Kodu Buluşsal Yöntemleri*
- *RFC uyumluluğu denetimi*
- *TCP yeniden birleştirme*
- *Akış birleştirme*

IBM İletişim Kuralı Analiz Modülü tarafından durdurulan başlıca ağ tehditleri

İnternet tehditleri gelişmeye devam ederken, eski saldırı yöntemleri de kullanılmaya devam edilmektedir ve pek çok saldırgan, tespit sistemlerini atlatmak için bilinen izinsiz giriş yöntemlerini geliştirmeye çalışmaktadır. IBM İletişim Kuralı Analiz Modülü, aşağıdaki listede bulunan İnternet tehditlerini durdurmaya adanmıştır:

İnternet Saldırısı Tipleri	Tehlikeli Olmasının Nedeni	Durduran PAM Modülü
Arka Kapılar	Geleneksel oturum açma doğrulamasını atlayan sistem giriş noktaları sağlar.	Tehdit Belirleme ve Önleme
Botnetler	Genellikle istenmeyen posta ve/veya kötü niyetli yazılım yaymak amacıyla, bir denetleyicinin yönlendirmesi ile görevlerini yerine getiren ele geçirilmiş bilgisayarlardır.	Tehdit Belirleme ve Önleme
İstemci Tarafı Saldırıları	Kişisel bilgisayarlarda çalışan işletim sistemini veya uygulamaları etkileyen izinsiz yetki kazanma programlarıdır. İzinsiz yetki kazanma programları, e-posta istemcilerini, Web tarayıcılarını, belge görüntüleyicilerini ve çoklu ortam uygulamalarını hedef alabilir.	İstemci Tarafı Uygulama Koruması
Siteler arası komut dosyası oluşturma	Genellikle bilgi çalma amaçlı olarak, bir kullanıcının bilgisayarında yürütme gerçekleştirebilen, görünüşte uygun bir bağlantıya kötü niyetli kod yerleştirmek için kullanılan Web tabanlı izinsiz yetki kazanma programıdır.	Web Uygulaması Koruması
Dağıtılmış Hizmet Engelleme (DDoS)	Hedef sistemi devre dışı bırakmak için tek hedefe çok sayıda ileti ile saldıran bir dizi ele geçirilmiş sistemden yararlanır	Tehdit Belirleme ve Önleme

İnternet Saldırısı Tipleri	Tehlikeli Olmasının Nedeni	Durduran PAM Modülü
Şirket içinden kaynaklanan tehditler	Dahili kullanıcılar, bir ağa virüs, solucan ve Truva Atları bulaştırabilir veya özel verileri çalmaya çalışabilir	Tehdit Belirleme ve Önleme
Anında İleti Sistemi	Ağa Truva Atları, virüsler ve diğer kötü niyetli yazılımların bulaştırılması için kullanılabilir.	Uygulama Denetimi
Kötü niyetli içerik	Kötü niyetli çoklu ortam ve belgelerde yerleşik kabuk kodu saldırganları.	İstemci Tarafı Uygulama Koruması
Kötü niyetli e-posta	Kullanıcıları kötü niyetli Web sitelerini ziyaret etmeye yönlendiren ve ardından potansiyel olarak ağa kötü niyetli yazılım yerleştirebilecek casus yazılımlar ve e-dolandırıcılık girişimleri için ortak bir taşıyıcı.	İstemci Tarafı Uygulama Koruması
Eşler arası (P2P) ağlar	Hizmet engelleme saldırıları ve verileri bozmak için tasarlanmış Truva Atları ve virüsler içeren dosyaların aktarımını sağlar.	Uygulama Denetimi
İletişim kuralı tünelleme	Genellikle daha yüksek bir iletişim kuralı düzeyi içerisine kötü niyetli yazılım yerleştirir ve düşük seviyeli iletişim kurallarının engellenmiş olabileceği ağ segmentlerine geçmesine olanak sağlar.	Uygulama Denetimi
Keşif	Kaba kuvvet, sayım, parola tahmini ve kapı taramaları gibi bir grup tehdittir.	Tehdit Belirleme ve Önleme
Rootkitler	Bilgisayar korsanlarına sistem yöneticisi düzeyi ayrıcalıkları veya bir ağ ya da sisteme kök erişimi sağlayan bir grup program veya araçtır.	Tehdit Belirleme ve Önleme
İstenmeyen Posta	Genellikle İnternet üzerinden toplu iletiler halinde gönderilen istenmeyen e-postalardır.	İstemci Tarafı Uygulama Koruması
Mızrak Hedefli E-dolandırıcılık	Gizli bilgilerin çalınması amacıyla yüksek değerli hedeflere yönelik, dikkatle hazırlanmış bir saldırıdır.	Veri Güvenliği
SQL injection	Bir Web uygulamasını veritabanına erişim sağlaması için aldatmak amacıyla uygulamanın dinamik mantık katmanı aracılığıyla hedeflenen komutlara kötü niyetli SQL kodu ekler.	Web Uygulaması Koruması
Truva Atları	Görünürde zararsız olan programlama veya verilerin içerisine tehlikeli kod ekler.	Tehdit Belirleme ve Önleme
Solucanlar	Kendisini bir e-posta eki veya bir ağ iletisinin parçası olarak yeniden göndererek kendi kendine eşlenen virüstür.	Tehdit Belirleme ve Önleme
Sıfırıncı Gün Saldırıları	Yazılım satıcıları bir yama sağlayamadan önce, henüz açıklanmamış güvenlik açıklarını istismar etmeye çalışan tehditlerdir.	Virtual Patch

IBM İletişim Kuralı Analiz Modülü içerisindeki çok katmanlı önleme teknolojileri

PAM, hepsi de İnternet tehditlerini önlemek için uyum içerisinde çalışan çok sayıda tehdit önleme teknolojisinin gücünü birleştirir. PAM, aşağıdaki saldırı önleme yöntemlerini kullanır:

Saldırı Önleme Yöntemler	Anlamı	Destekleyen PAM Modülü
Tarayıcı İstismarı Önleme	JavaScript™ gizleme kullanarak Web tarayıcılarına yönelik saldırıları önler.	İstemci Tarafı Uygulama Koruması
İçerik Analizi	Önceden tanımlanmış ve özel imzalarla ağınızda bulunan şifrelenmemiş verileri inceler ve bloke eder. Bu teknoloji, bileşik veri kümesi arama incelemeleri oluşturma ve Microsoft® Office belgeleri, PDF'ler, Zip dosyaları ve 10'dan fazla iletişim kuralı dahil olmak üzere bileşik belgeleri inceleme becerisi sağlar.	Veri Güvenliği
Akış Birleştirme	Sadece bağımsız paketleri değil, tüm ağ bağlantısını analiz ederek bir açık bağlantıdan yararlanarak iletişim akışına katılmış olabilecek kötü niyetli trafiği engeller. Akış birleştirme, ileri düzey tehditleri önlemek için trafiği daha yüksek düzeyde analiz ederek TCP yeniden birleştirmeyi tamamlar.	Tehdit Belirleme ve Önleme
Injection Mantığı Motoru	SQL injection ve kabuk komutu ekleme gibi kötü niyetli injection girişimlerini buluşsal olarak tanımlar. İmza güncellemeleri olmaksızın mevcut ve gelecekteki güvenlik açıklarını kapsar.	Web Uygulaması Koruması
Kapı Tahsisi	İzinsiz giriş önleme hizmetleri, belirli bir TCP/IP kapısında belirli bir tür trafiğin oluşacağını varsayamaz. Aksi halde, trafik tipinin varsayılan kapıya uyması ve geçmesine izin verilmesi durumunda saldırganlar erişim imkanına sahip olabilir. IBM Security İzinsiz Giriş Önleme Sistemi ürünleri, trafiğin yönlendirildiği kapıya bakılmaksızın tüm trafiği inceler.	Virtual Patch
Kapı İzleme	Sadece başlangıçta bağlantının kurulması için kullanılan kapının kullanılmasının sağlanması için iletişim oturumlarını takip eder. Bu şekilde, orijinal kimlik bilgileri ile açık bir kapıya ulaşan saldırganların bir başka açık kapıya bağlanarak fark edilmeksizin veri aktarımı gerçekleştirmesi önlenir.	Virtual Patch
İletişim Kuralı Analizi	Benimsenen normlara uygun olmayan olağandışı davranışlara karşı ağ trafiğini inceler ve OSI modeli Katman 2'ye kadar iletişim kurallarının kodlarını çözebilir. İletişim kuralı analizi, IBM Security İzinsiz Giriş Önleme Sistemi ürünlerinin anormal davranışları imzalara bağımlı olmaksızın belirlemesine olanak sağlar.	Virtual Patch

Saldırı Önleme Yöntemler	Anlamı	Destekleyen PAM Modülü
İletişim kuralı tünelleme	Zaman zaman kapı tahsisi ile birlikte kullanılan IBM Security İzinsiz Giriş Önleme Sistemi ürünleri, daha düşük düzey iletişim kurallarının engellenmiş olabileceği ağ segmentlerine geçişine izin verilebilecek daha yüksek düzey iletişim kurallarına yerleşik kötü niyetli ve/veya patentli verileri bulmak için iletişim kuralı tünellemeyi belirler ve önler. İletişim kuralı tünelleme, saldırganların güvenlik duvarlarını atlayarak sorgulanmaksızın ağ erişimi elde etmesini önler ve hem içerideki kullanıcıların, hem de saldırganların bir kuruluş içerisinden veri aktarmak için tüneller oluşturmasını ve kullanmasını engeller.	Uygulama Denetimi
RFC uyumluluğu denetimi	Trafiği ana bilgisayarlar, uygulamalar ve ağ kümesi arasındaki ağ iletişimlerine yönelik RFC standartları ile karşılaştırır. Trafik standarda uyumlu değilse, IBM Security İzinsiz Giriş Önleme Sistemi ürünleri tarafından engellenir.	Uygulama Denetimi
Kabuk Kodu Buluşsal Yöntemleri	Belirli bir saldırı imzasını veya kalıbını eşleştirmek yerine davranışları doğrultusunda kötü niyetli kodu tanımlar ve durdurur. Buluşsal yöntemler, geleneksel izinsiz giriş önleme çözümlerini atlamak için imzalarının küçük kısımlarını değiştirerek gelişen tehditleri önler.	Tehdit Belirleme ve Önleme
Durum bilgili kalıp eşleştirme	Trafiğin sadece gerçekten bir saldırı oluşabilecek belirli kısımlarında saldırı kalıplarını belirlemek için gelişmiş algoritmalar kullanarak yanlış pozitiflerin sayısını önemli ölçüde azaltır. IBM Security İzinsiz Giriş Önleme Sistemi ürünleri, buluşsal yöntemlerle birlikte durum bilgili kalıp eşleştirme kullanarak tespit edilmemek için kalıplarını değiştirerek gelişen tehditleri önler.	Tehdit Belirleme ve Önleme
TCP yeniden birleştirme	Ağ paketlerini yeniden birleştirir ve potansiyel tehditlere karşı inceler.	Virtual Patch

IBM İletişim Kuralı Analiz Modülünün Avantajları

IBM Security İzinsiz Giriş Önleme Sistemi teknolojileri kapsamındaki IBM İletişim Kuralı Analiz Modülü, güvenlik açıklarının ve saldırı yöntemlerinin özelliklerine ilişkin sürekli araştırmaların sonucudur. Eski izinsiz yetki kazanma programları tamamen ortadan kalkmasa da tehditler gelişmeye devam etmektedir ve IBM de PAM motorunu, hem yeni, hem de eski her türlü tehdit sınıfını engellemek üzere tasarlanmış teknolojilerle güçlendirmektedir.

Daha ayrıntılı bilgi için

IBM Security Solutions ve önleyici koruma ile ilgili daha ayrıntılı bilgi edinmek için lütfen IBM Satış temsilcinizle veya IBM Çözüm Ortağınızla iletişim kurun veya aşağıdaki Web sitesini ziyaret edin:
ibm.com/tivoli/solutions/threat-mitigation.

IBM Tivoli yazılımı hakkında

IBM Tivoli® yazılımı, maliyetlerin düşürülmesine yardımcı olurken aynı zamanda sürekli değişen iş gereksinimlerinin karşılanması ve hem esnek hem de hızlı yanıt veren BT hizmeti yönetimi sağlanması için işletmelerin BT kaynaklarını, görevlerini ve süreçlerini etkin ve verimli bir şekilde yönetmesine yardımcı olur. Tivoli portföyü, güvenlik, uygunluk, depolama, performans, kullanılabilirlik, yapılandırma, işletim ve BT yaşam çevrimi yönetimi yazılımları içerir ve dünya çapında IBM hizmetleri, desteği ve araştırmaları tarafından desteklenir.

Ek olarak, IBM Global Financing tarafından sağlanan finansman çözümleri, etkin nakit yönetimine, teknolojinin eskimesine karşı korumaya, geliştirilmiş toplam sahip olma maliyetine ve yatırım getirisine olanak sağlayabilir. Ayrıca, Küresel Varlık Geri Kazanım Hizmetlerimiz, yeni ve enerji verimliliği daha yüksek çözümlerle çevreye ilişkin endişelerin giderilmesine yardımcı olur. IBM Global Financing ile ilgili daha ayrıntılı bilgi için:
ibm.com/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Amerika Birleşik Devletlerinde hazırlanmıştır. Mayıs 2010

WGD03001-USEN-00